C L I F F O R D

C H A N C E

REPORT OF INVESTIGATION ON SWEDBANK AB (publ)

23 MARCH 2020

CLIFFORD CHANCE US LLP

2001 K STREET NW
WASHINGTON, DC 20006-1001
TEL +1 202 912 5000
FAX +1 202 912 6000

31 WEST 52ND STREET
NEW YORK, NY 10019-6131
TEL +1 212 878 8000
FAX +1 212 878 8375

C L I F F O R D

C H A N C E

TABLE OF CONTENTS

I. INTRODUCTION

A. Background to the Report

Swedbank AB (publ) ("**Swedbank,**" or "**the Bank**"), a Stockholm-headquartered bank that is publicly traded on NASDAQ Stockholm (SWED), operates in four home markets: Sweden and the three Baltic markets of Estonia, Latvia and Lithuania. The Bank has three primary business lines: Large Corporates and Institutions ("**LC&I**"), which handles large corporations and financial institutions; Swedish Banking, which handles private customers and companies in Sweden; and Baltic Banking, which covers Swedbank's business in the three Baltic states. Baltic Banking operates through three main subsidiaries: Swedbank AS (Estonia) ("**Swedbank Estonia**"), Swedbank AS (Latvia) ("**Swedbank Latvia**"), and Swedbank AB (Lithuania) ("**Swedbank Lithuania**") (collectively, the "**Baltic Subsidiaries**").[1] Swedbank also maintains several international branches, including in New York USA. One of the oldest financial institutions in Sweden, Swedbank through its predecessor entities has been in existence for 200 years.

In late 2018, media reports raised questions regarding Swedbank's exposure to money laundering scandals involving the Baltic region and Estonia in particular. At the time, Swedbank publicly maintained that it had limited exposure to such risks because Swedbank was a low-risk bank focused primarily on domestic retail customers, and because Swedbank had anti-money laundering ("**AML**") procedures in place to ensure that it acted forcefully in response to suspicious activity.

On 20 February 2019, the Swedish public television network program *Uppdrag granskning*, broadcast on Sveriges Television ("**SVT**") began a series of broadcasts alleging that customers of Swedbank's Baltic Subsidiaries had engaged in suspicious transactions indicative of money laundering. Subsequently, the Swedish Financial Supervisory Authority ("**SFSA**") and Estonian Financial Supervisory Authority ("**EFSA**") announced investigations into the allegations.

Following the first SVT program, Swedbank engaged Clifford Chance to conduct an investigation (the "**Investigation**") into the allegations that had been made and more broadly into Swedbank's historical exposure to money laundering risk. Taking a risk-based approach, Clifford Chance's Investigation has focused primarily but not exclusively on Swedbank's Baltic Banking business in the Baltic Subsidiaries from January 2007 through March 2019 (the "**Investigation Period**"), as well as Swedbank AB's involvement in that business, and related activity in Sweden. As Clifford Chance has conducted its Investigation, Swedbank also has been cooperating with ongoing government investigations in Sweden, the Baltics and the United States.

Clifford Chance has provided regular reports on the methodology and progress of the Investigation to the Swedbank Board of Directors (the "**Board**") and has prepared this report for the Board setting forth the factual findings of the Investigation (the "**Report**"). The findings in this Report are Clifford Chance's objective conclusions. The Bank has not influenced the course of the Investigation or Clifford Chance's factual conclusions, and has cooperated fully in the Investigation.

B. Scope of the Report

Clifford Chance designed the Investigation to identify historical shortcomings in Swedbank's AML compliance processes, as well as exposure to money laundering risk and potential violations of US sanctions. The Investigation encompasses Swedbank, including its global network of branches and wholly-owned subsidiaries, and includes customers, transactions and activities from throughout the Investigation Period. With forensic support from FTI Consulting ("**FTI**"), the Investigation has analyzed over 30 billion transactions, approximately half of which are from the Baltic Subsidiaries.

[1] A more comprehensive list of key terms used in this Report can be found at Appendix A.

This Report sets forth the results of the Investigation. Following an Executive Summary, the Report begins with a brief review of Swedbank's history and a detailed description of how the Investigation was conducted. The Report then describes the AML legal framework that applied to Swedbank and the Baltic Subsidiaries during the Investigation Period, and the governance structure of Swedbank and its Baltic Subsidiaries during the Investigation Period. This is then followed by a chronological narrative of Swedbank's and the Baltic Subsidiaries' historical exposure to AML and sanctions risk, including a discussion of certain high risk non-resident ("**HRNR**") customers of the Baltic Subsidiaries. The Report next sets forth Clifford Chance's findings regarding Swedbank's exposure to high risk customers and potentially suspicious transactions, its apparent sanctions violations, its AML control functions and governance, its public disclosures, and employee accountability. The Report concludes with a description of ongoing remediation efforts.

More specifically, the Report includes:

- a brief summary of the relevant AML legal framework under which Swedbank and the Baltic Subsidiaries operated during the Investigation Period, with a discussion of how these legal and regulatory standards evolved over time;
- an overview of the governance structures and escalation procedures and practices at Swedbank and the Baltic Subsidiaries during the Investigation Period;
- an explanation of the respective roles of Swedbank's three lines of defense (including the functions of Group Security & Investigations ("**GSI**"), Group Compliance and Group Internal Audit ("**GIA**"));
- the history of the development of the non-resident customer portfolio in the Baltic Subsidiaries and the adequacy of the controls implemented by Swedbank and the Baltic Subsidiaries to manage the risk thereof;
- an overview of Swedbank's and the Baltic Subsidiaries' response to previously identified problems relating to AML and sanctions risk (including with respect to specific customer groups that presented heightened risk in these areas), prior internal investigations or reviews conducted by Swedbank regarding such problems, and Swedbank's response to the findings from these reviews;
- an assessment of historical deficiencies in AML- and sanctions-related policies, procedures and processes at Swedbank and the Baltic Subsidiaries;
- a description of the process for identifying customers of Swedbank's Baltic Subsidiaries that present heightened risk for money laundering, and a review of those customers' transactions within a five-year lookback period to identify transactions carrying certain indicia of money laundering risk;
- a description of Swedbank's key past public disclosures regarding its exposure to AML risk in the Baltic Subsidiaries;
- an assessment of Swedbank's communications with regulators regarding AML issues;
- an assessment of the conduct of Chief Executive Officers ("**CEOs**"), and Boards of Directors of Swedbank with respect to the issues identified;
- an assessment of exposure to US sanctions risk in the Baltic Subsidiaries during a five-year lookback period; and
- prior and ongoing remediation efforts at Swedbank and its Baltic Subsidiaries.

In conducting the Investigation, Clifford Chance has adopted a risk-based approach, focusing on the business areas and time periods in which the most significant issues have been identified.

Executive Summary

Clifford Chance designed the Investigation to identify historical deficiencies in Swedbank's AML compliance systems and controls during the Investigation Period. The Investigation focused on the areas of Swedbank and the Baltic Subsidiaries that, based on the available information, evinced the highest historical AML-related risk. In this regard, the scope and focus of the Investigation was informed by the media allegations regarding Swedbank, the pending investigations by Swedish, Baltic and US authorities, Swedbank's own prior internal reviews that had identified historical issues, and, on an iterative basis, information identified through Clifford Chance's analysis of internal documents and communications, customer and transaction records, and interviews of current and former employees at every level of the institution and across each of its four home markets.

Methodology

The Investigation was broad and intensive, and considered billions of transaction records, approximately 160 million customer records, over 38 terabytes of electronic and scanned hard copy data from Swedbank's internal files, including over 20 million documents gathered from email servers, employee laptops and mobile devices, shared server files, KYC materials, internal audit reports, and Board and key committee minutes and supporting materials. This data was reviewed against targeted search terms, which were adjusted as we learned more as the Investigation progressed. The Investigation involved the collection and review of relevant documents in multiple languages, including Swedish, Estonian, Latvian, Lithuanian and Russian.

Clifford Chance conducted nearly 100 interviews of 81 individuals, including current and former employees, managers and senior executives, current and former Board members, and an external counsel. Throughout the Investigation, Swedbank took steps to retain all potentially relevant data and documents and facilitated Clifford Chance's unfettered access to documents, data and personnel.

In addition, steps were taken, on the advice of local counsel, to ensure compliance with applicable privacy, bank secrecy, employment and other relevant legal regimes. While the manner in which certain facts and findings are discussed in this Report has been impacted by applicable Swedish, Estonian, Latvian and Lithuanian privacy and bank secrecy laws and regulations, in our view, the Report provides a clear picture of what happened, how it happened, and the accountability of those involved.

AML Controls

Over the course of the Investigation Period, AML regulations have evolved, as have their interpretation and application by international banks operating in Europe. Industry standards have also evolved, based on common practices, official guidance and past enforcement actions, with regulatory expectations increasing over time. It is important to understand the facts discussed herein against this backdrop rather than solely through today's lens and with the benefit of hindsight.

As is set forth in detail in this Report, based on the available information, Clifford Chance did not conclude that Swedbank engaged in money laundering or processed customer transactions that constituted the proceeds of crime. Among other things, this would require definitive knowledge of a customer's source of funds, which was not available. However, the Investigation did reveal that Swedbank, throughout the Investigation Period and to varying degrees across LC&I, Swedish Banking and Baltic Banking, had inadequate systems and controls to ensure proper management of the AML and economic sanctions risk of its customer base, which, therefore, historically exposed Swedbank and the Baltic Subsidiaries to significant AML and sanctions risk.

This risk appeared most prevalent in the Baltic Subsidiaries, primarily at Swedbank Estonia, and principally arose from the HRNR business. From before 2007 until a decision to de-risk the HRNR business in 2016, Swedbank Estonia and Swedbank Latvia actively pursued these high risk customers as a business strategy. Swedbank Estonia also accepted certain customers that had been off-boarded by another bank in Estonia in 2015 that had decided to exit the HRNR business based on excessive money laundering risk.

Although Swedbank Estonia created a special committee to review the on-boarding and maintenance of HRNR customers, the Investigation has identified that this committee approved high risk customers without having complete documentation regarding the ultimate beneficial owners ("**UBOs**"), proof of source of funds or explanation of the legitimate business purpose of the customers, and did not address red flags that arose from the information that was provided. Some of the companies had complex and opaque ownership structures involving off-shore entities organized in low tax jurisdictions, as well as ownership through foreign trusts and similar vehicles for which the UBOs were difficult to verify. Swedbank Estonia also accepted customers despite awareness amongst employees, including relationship managers ("**RM**s"), that the listed beneficial owners were not the actual UBOs, and in situations in which the prospective customer refused to provide verifiable beneficial ownership information.

In addition, at Swedbank Estonia, employees involved in the HRNR business kept certain information regarding the UBOs for some customers outside of Swedbank's regular customer databases and retained the information in hard copy in a safe or locked drawer to assuage the customer's concern that the true UBOs may become known to third parties. Swedbank Estonia employees also accepted customer corporate structures knowing that they were designed to conceal the true UBOs from home country tax authorities. Lastly, Swedbank Estonia employees also repeatedly overlooked or disregarded indications of potentially suspicious transactions. Some of these practices were also identified in the other Baltic Subsidiaries. The AML deficiencies were not limited to the Baltic Subsidiaries, as certain of the high risk customers that banked primarily in the Baltics also were permitted to open and to maintain accounts with Swedbank LC&I and Swedish Banking.

AML Forensic Analysis

The Investigation analyzed forensically the external payment transactional activity of Baltic Banking customers that met the Baltic Subsidiaries' definition of HRNR customer, namely customers that were non-resident legal entities registered outside of the EU and Norway but also including customers registered in Malta, Cyprus, the UK or Luxembourg, which customers Swedbank had rated as high risk at some point during the Investigation Period. This definition, as applied to the full customer base of the Baltic Subsidiaries, could include entities that today would not be considered to have high AML risk, but could exclude other customers who did present high AML risk. To avoid excluding such customers from the review, the Investigation also considered additional categories of customers, such as (a) customers identified in the course of the Investigation as presenting AML risk, (b) customers that had done business through Swedbank with counterparties at certain high risk Baltic banks identified by government authorities or in the media as being involved in money laundering schemes and (c) customers with strong links to certain foreign jurisdictions, either through residency or ownership.

FTI collected transaction data for this aggregate group of customers ("**AML Risk Identified Customers**") for the period from March 2014 through March 2019, and ran 21 algorithmic detection scenarios designed to identify potentially suspicious transactions. Inclusion in the group of AML Risk Identified Customers is not necessarily indicative of suspicious behavior or improper conduct. Rather, these parameters were

designed to capture the portion of the Baltic Subsidiaries' customer population that warranted further review. In addition, the fact that an external payment to or from one of these customers hit against one or more of the detection algorithms does not mean that the payment should have been considered suspicious at the time, let alone is it evidence that a customer engaged in money laundering or other financial crime. Rather the detection algorithms are designed to identify transactions with risk indicators similar to those that a transaction monitoring system would flag for further review. To provide further context, industry wide, typically less than 10% of hits against detection algorithms result in a report of a suspicious transaction to an appropriate financial intelligence unit ("**FIU**"). In other words, the false positive rate often exceeds 90%.

In presenting the results of this analysis, Clifford Chance has focused on external transactions that alerted on three or more detection scenarios.

For Swedbank Estonia, during the five-year period from March 2014 through March 2019, this exercise identified payments that totaled approximately €9.9 billion that were received into these customers' accounts, and a total of approximately €11.4 billion that were sent by these customers from their accounts.

For Swedbank Latvia, during the five-year period from March 2014 through March 2019, this exercise identified payments that totaled approximately €4.8 billion that were received into these customers' accounts, and a total of approximately €4.5 billion that were sent by these customers from their accounts.

For Swedbank Lithuania, during the five-year period from March 2014 through March 2019, this exercise identified payments that totaled approximately €3.2 billion that were received into these customers' accounts and a total of approximately €3.0 billion that were sent by these customers from their accounts.

Thus, across all three Baltic Subsidiaries the total value of external payments that alerted on three or more detection scenarios during the five-year period from March 2014 through March 2019 was approximately €17.8 billion of incoming and €18.9 billion of outgoing payments.

Significantly, the value of transactions meeting these criteria decreased materially on an annual basis over the period from 2014 through 2019 for Swedbank Estonia and Swedbank Latvia. For example, at Swedbank Estonia, incoming payments decreased from a high mark of approximately 9.5% of the total incoming payments of all customers for Swedbank Estonia over the last three quarters of 2014, to approximately 1.1% of the total incoming payments in Q1 2019. Similarly, at Swedbank Latvia, incoming payments decreased from a high mark of 6.8% of the total incoming payments of all customers for Swedbank Latvia in 2015, to 0.9% of the total incoming payments in Q1 2019. At Swedbank Lithuania, the overall relevant transaction activity was lower than at Swedbank Estonia and Swedbank Latvia, but increased to a high of approximately 2.8% of the total incoming payments for all customers of Swedbank Lithuania in 2018.

US Sanctions Forensic Analysis

The Investigation also included an assessment of potential non-compliance by the Baltic Subsidiaries or their customers with the sanctions regulations of the US Treasury Department's Office of Foreign Assets Control ("**OFAC**"). In particular, based on data collected and processed by FTI, Clifford Chance reviewed USD Society for Worldwide Interbank Financial Telecommunications ("**SWIFT**") network payments processed by the Baltic Subsidiaries during the five-year period from March 22, 2014 through March 22, 2019 to identify whether any such payments may not have complied with OFAC blocking sanctions or country embargos, which we then characterized as "**Subject Transactions**." As part of this process, Clifford Chance also reviewed available customer data to identify any OFAC-sanctioned customers of the Baltic Subsidiaries

and to ensure the inclusion of their USD SWIFT payments in the OFAC transaction review.

For the five-year period under review, covering approximately 26.6 million transaction messages and 1.8 million USD payments, Clifford Chance identified 582 Subject Transactions, totaling approximately $4.76 million, processed by the Baltic Subsidiaries.

Within this total, by Baltic Subsidiary, Clifford Chance determined that:

- Swedbank Estonia customers used an online banking platform to initiate 19 outgoing Subject Transactions, totaling approximately $100,000, which appeared to involve persons in Iran, Cuba or Crimea. We also identified 35 apparent incoming Iran-related Subject Transactions, totalling approximately $222,000.
- Swedbank Latvia customers used an online banking platform to initiate 522 outgoing Subject Transactions, totaling approximately $4.43 million, of which 507 such outgoing Subject Transactions between 30 December 2014 and 30 December 2016, amounting to approximately $4.26 million, involved three shipping customers domiciled in offshore jurisdictions that had accounts at Swedbank Latvia but whose owner appeared to operate these companies from Crimea. The remaining 15 outgoing Subject Transactions from accounts at Swedbank Latvia appeared to involve non-sanctioned customers who were temporarily located in Crimea or Iran or payments by non-sanctioned customers to counterparties in Crimea. We also identified one incoming Subject Transaction for $5,970 to an individual customer of Swedbank Latvia who had a residency address in Crimea.
- Swedbank Lithuania customers used an online banking platform to initiate five outgoing Subject Transactions, totaling approximately $2,400 that appeared to involve persons in Crimea.

None of these Subject Transactions involved any OFAC-listed persons, and nearly all of them, by volume and value, occurred prior to 2017, the year that the Baltic Subsidiaries implemented an automated payment screening solution.

Governance

Since 2016, Swedbank initiated enhancements to its compliance control and risk management systems in the Baltic Subsidiaries. However, these efforts were impeded by a number of governance failings. For example, Swedbank senior management historically had failed to establish clear lines of AML-related responsibilities, particularly as between the business (the first line of defense) and Compliance (the second line of defense), or to ensure methods of challenge by the second line over the AML-related functions appointed to the first line of defense. In addition, throughout the Investigation Period, the Swedbank CEOs appeared to lack an adequate appreciation for the severe risk posed to the institution by the HRNR business in Baltic Banking, given the consistently ineffective AML controls. This lack of appreciation for the degree of risk was evidenced by the Bank's failure to adopt a Group-level AML risk appetite statement until 2017, or to take steps to ensure consistency of approach to risk rating customers across business lines.

The Investigation also found that because senior management failed to appreciate the degree of legal and reputational risk to Swedbank, it did not always engage with the Board in a manner consistent with the importance of these issues. For example, throughout the Investigation Period GIA repeatedly identified and reported serious AML control deficiencies which were raised to the Audit Committee of the Board and often summarized to the full Board, particularly during the period from 2016 through early 2019. The messaging on balance by the CEO and other senior executives to the Board during this period was that while there were problems, they were under control.

Similarly, during this period, the Group Compliance function internally and with the assistance of outside experts such as the law firm Erling Grimstad AS ("**Grimstad AS**"), had identified serious AML control deficiencies and potentially serious legal risk to Swedbank arising from those deficiencies. In some cases, the more serious findings were not escalated in a timely manner to the Board, shared with GIA, or shared with the management of the relevant Baltic subsidiary.

In addition, Clifford Chance reviewed and considered requests from regulators received by Swedbank and its Baltic Subsidiaries regarding AML-related topics and Swedbank's responses to those requests, to assess Swedbank's transparency when dealing with its regulators regarding such matters. The Investigation found that, in certain instances, Swedbank did not always take an actively transparent posture with regulators regarding AML-related issues, de-emphasized negative information and occasionally employed a narrow or literal reading of certain requests.

Public Disclosures

Clifford Chance considered the completeness and accuracy of Swedbank's public disclosures concerning AML compliance and related issues, in view of the facts established in the Investigation. Specifically, Clifford Chance reviewed public statements made by Swedbank and its executives from January 2014 through March 2019, including for example, interim and annual reports issued by Swedbank and associated materials, other statements and presentations in communications with investors, analysts, and the financial community, corporate debt offering documents and media appearances and publications. When considered in light of the facts developed in the Investigation, certain statements made during October 2018 and February 2019 by Swedbank and its executives concerning Swedbank's historical AML compliance, then current AML compliance, and exposure to certain types of AML risk, were inaccurate or presented without sufficient context.

Accountability

The Investigation also considered which individuals the facts indicated were responsible over time for the existence and perpetuation of the deficiencies in AML and sanctions controls, and why these deficiencies that were identified by GIA, Compliance and other functions, as well as to some extent by Swedbank's external auditors, nonetheless continued without material improvement for many years. In assessing responsibility, the Investigation determined that the three former CEOs who served during the Investigation Period, the Board and certain employees all contributed to a greater or lesser degree to Swedbank's failure to recognize and manage the significant legal and reputational risk to Swedbank posed by its HRNR portfolio in the Baltic Subsidiaries.

As to the CEOs, the Investigation found that the CEO who served from 2009 through 2016 failed to focus on AML deficiencies in the Baltic Subsidiaries during this time despite recurring GIA reports indicating such deficiencies, and notwithstanding an SFSA inspection that found significant AML deficiencies in LC&I and Swedish Banking. With respect to the CEO who served from 2016 through 2019, the Investigation concluded that the CEO's tenure included significant steps to de-risk the HRNR business in the Baltic Subsidiaries and to launch internal investigations of potential AML exposure in response to media reports of money laundering scandals, regulator requests and other indicators. However, the CEO did not direct sufficient resources, attention, or urgency to the remediation of the issues identified, and did not ensure that information regarding these issues was shared between relevant Swedbank control functions or with the Management Boards of the relevant Baltic Subsidiaries. Nor did this CEO ensure that the Board was adequately educated or apprised of the significant legal and reputational risk that these AML deficiencies, in light of the historical high risk customer base in the Baltic Subsidiaries, presented to Swedbank.

As to the Board, the Investigation determined that while the Board was not apprised of the full extent of the legal and reputational risk posed by the AML issues in the Baltics, the Board was informed through regular GIA reports of recurring problems in AML controls, including in the Baltic Subsidiaries. Interviews of Board members indicated that the Board generally understood, based on statements from Swedbank's management, that these matters were under control. Although the minutes of the Audit Committee do reflect relevant discussions of these issues, the full Board record does not reflect significant challenge by the Board to management on the AML issues that were presented to them.

The Investigation also identified a number of employees whose actions and/or inaction caused or contributed to the perpetuation of the AML problems in the Baltic Subsidiaries. These employees ranged from senior managers at Swedbank and the Baltic Subsidiaries, to relationship managers who serviced some of the most problematic HRNR clients, and included members of the customer approval committee in Swedbank Estonia who approved account openings despite apparent red flags. Clifford Chance shared facts regarding these employees with Swedbank over the course of the Investigation, and Swedbank consequently ended the employment of a number of then-current employees.

Remediation

Since the Investigation began in early 2019, Swedbank has appointed a new CEO and a mostly new management team, including a new Chief Compliance Officer ("**CCO**") and CEO of Swedbank Estonia, and has taken other employment actions dictated in large part by findings in the Investigation. Moreover, Swedbank has a new Board Chair, and the Board now is comprised of mostly new members.

Under this new leadership team, Swedbank has focused on transforming its approach to AML and counter-terrorist financing ("**CTF**") and sanctions policies and procedures, creating new roles, appointing new personnel, increasing resources, revising and strengthening policies and procedures and taking steps to continue the process of de-risking its customer portfolio including in the Baltic Subsidiaries.

As part of these ongoing de-risking and remediation efforts, and with input from Clifford Chance, Swedbank and its Baltic Subsidiaries have (a) embarked on a much more comprehensive approach and remediation plan to address and to strengthen the AML/CTF and sanctions frameworks; (b) undertaken a review of Swedbank's corporate governance; (c) engaged external consultants to assist in remediation efforts; (d) increased AML/CTF resources; and (e) continued to off-board customers who do not meet Swedbank's risk appetite.

In addition, Swedbank is planning to engage a consultant to assess the current state of Swedbank's AML/CTF policies, procedures, systems and controls, including their implementation. The consultant will identify any existing gaps against regulatory requirements and industry best practices, help Swedbank address those gaps and conduct assessments to ensure that gaps have been fixed.

II. HISTORY OF SWEDBANK

Swedbank is rooted in a savings-bank tradition that is closely aligned with the development of cooperative agricultural banking. Sweden's first savings bank — Swedbank's predecessor — was founded in Gothenburg in 1820. The savings-bank concept spread rapidly throughout the country, with tailored banking products to encourage saving among the general public. Over the next century, the rise of agriculture and growing urban migration spurred the development of agricultural cooperative banks, with Sweden's first agricultural bank established in 1915. Agricultural banks were economic associations owned by their members, in shares proportionate to the size of the member's farm. The main tasks of the agricultural banks were to provide operational credit to smaller farms and to encourage saving.

The middle of the twentieth century saw the beginning of a period characterized by substantial governmental control of banking operations. The savings banks were also becoming modernized. In the 1940s and 1950s, centralization of the savings banks and cooperative banks contributed to the growth of Sparbankernas Bank (the "**Savings Banks' Bank**"), which was established as the central bank for the various savings banks, and Föreningsbankernas Bank (the "**Union Banks' Bank**"), formed by a merger of the agricultural banks. Consolidations of these entities and their successors over the years led to the creation of FöreningsSparbanken AB in 1997, which changed its name to Swedbank AB in 2006.

Swedbank originated in the savings bank movement, and it continues to respect the fundamental savings bank ideology. It aims to cultivate strong links with the local community and to promote a stable banking system. In addition, Swedbank's largest owners are the savings bank foundations, whose principal task is to advance the savings bank concept and to conduct operations that promote growth in consumer saving. Swedbank is now a major bank playing an important role in the communities it serves and is a fundamental part of the financial fabric in Sweden and the Baltics:

- Swedbank Group serves more than 7.3 million private customers and 620,000 corporate customers;
- Swedbank Group's total revenue (income) in 2018 was approximately $4.4 billion; and
- Swedbank Group today employs nearly 15,000 employees world-wide.

Swedbank's presence in the Baltic market stems from its acquisition of Hansabank, which began in 1998 and was completed in 2005:

1991: Hansabank began operating in Estonia.

1995: Hansabank opened in Latvia.

1996: Hansabank opened in Lithuania and established Hansabank Group, with operations in all three Baltic countries.

1998: Swedbank (then known as FöreningsSparbanken) acquired more than 50% of Hansabank's shares through a share issuance.

2005: In March 2005, Hansabank completed its acquisition of Moscow-based OAO Kvest bank in Russia. Later that year, Swedbank purchased the outstanding equity in Hansabank, making it a wholly-owned Swedbank subsidiary.

2007: Swedbank expanded to Ukraine by acquiring the Ukrainian bank TAS-Kommerzbank, which becomes OJSC Swedbank.

2008: Hansabank changed its name to Swedbank.

2011: The Baltic Subsidiaries are reorganized so that each of the Estonian, Latvian, and Lithuanian subsidiaries become directly owned by Swedbank AB. Before the change, Swedbank Estonia was the corporate parent of the Latvian and Lithuanian subsidiaries.

2013: In April, Swedbank announced that it was discontinuing operations at its Russian subsidiary, OAO Swedbank, selling its Ukrainian subsidiary, OJSC Swedbank, and would focus on its home markets.

At present, the Baltic Subsidiaries account for nearly one-fifth of Swedbank's profits and more than 40% of its customers and employees:

- Baltic Subsidiaries service approximately 3.3 million private customers and 285,000 corporate customers;
- Swedbank Estonia employs approximately 2,500 individuals across 32 branches;
- Swedbank Lithuania employs approximately 2,380 individuals across 58 branches; and
- Swedbank Latvia employs approximately 1,700 individuals across 32 branches.

Swedbank and the Baltic Subsidiaries have significant market share and are of systemic importance to the banking sectors in Sweden and the Baltics, serving large portions of the population in each of their home markets:

Sweden		Estonia		Latvia		Lithuania	
Population	10,1 m	Population	1,3 m	Population	1,9 m	Population	2,8 m
Private c.	4,0 m	Private c.	0,9 m	Private c.	0,9 m	Private c.	1,5 m
Business c.	270 000	Business c.	132 000	Business c.	91 000	Business c.	69 000
Offices	180	Offices	30	Offices	32	offices	58
ATM*		ATM	387	ATM	367	ATM	407
Cards	4 m	Cards	1,1 m	Cards	1,0 m	Cards	1,7 m
Employees	7701	Employees	2756	Employees	1674	Employees	2341

Source: https://www.swedbank.ee/static/pdf/about/presentatsioon_ENG.pdf

Outside of its home markets, Swedbank maintains a network of branches in the following countries: China (Shanghai), Denmark (Copenhagen), Finland (Helsinki), Luxembourg, Norway (Oslo) and the United States (New York). Other than its Baltic Subsidiaries, Swedbank also has wholly-owned subsidiaries in Sweden, Luxembourg, Norway and the United States.

III. LOCAL LAW IMPACT ON SCOPE OF REPORT

The scope of information disclosed in this Report is necessarily impacted by applicable law governing Swedbank's operations in Sweden, Estonia, Latvia and Lithuania. In particular, the information permitted to be disclosed is governed by Regulation (EU) 679/2016 (General Data Protection Regulation) (the **"GDPR"**) and the bank secrecy laws in Sweden,[2] Estonia,[3] Latvia,[4] and Lithuania.[5]

Each of the four jurisdictions addressed in this Report—Sweden, Estonia, Latvia, and Lithuania—is subject to the GDPR, which requires Swedbank to protect personal data and prevents the disclosure of information that identifies a natural person, either alone or in combination with other information, without legal basis, such as a legitimate business purpose. The bank secrecy laws prohibit the disclosure of information identifying or relating to specific banking customers, whether a natural person or entity, including any confirmation that a natural person or entity is or was, or is not or was not, a customer of Swedbank and any related information, such as account numbers, transactions, account balances and financial status. Failure to comply with these GDPR or bank secrecy requirements can carry serious penalties.

As a consequence, this Report does not contain identifying information such as names of customers or employees or account numbers, with the exception of using titles of certain senior executives. To the extent possible, the Report does not disclose any other information that could serve to identify a customer, employee or other natural person where such disclosure is unjustified. Furthermore, the Report also presents aggregated information regarding customers and transactions.

[2] The Swedish Banking and Financing Act 2004:297, Chapter 1 Section 10 (Bank Secrecy).
[3] Credit Institutions Act, § 88 (Information subject to banking secrecy).
[4] Credit Institutions Law of Latvia, Articles 61-64 (Relationships between Credit Institutions and Customers).
[5] Republic of Lithuania Law on Banks, Article 55 (Secret of a Bank).

IV. OVERVIEW OF AML INVESTIGATION AND METHODOLOGY

A. Investigation Methodology

The following describes the steps taken by Clifford Chance and FTI to identify, preserve and collect the potentially relevant Swedbank data. At all times, Clifford Chance and FTI received the full support and cooperation of Swedbank personnel.

B. Identification of Data Sources

At the outset, Clifford Chance and FTI conducted a wide-ranging scoping exercise to understand Swedbank's IT architecture and to identify repositories of structured and unstructured electronic data and sources of hardcopy documents potentially relevant to the Investigation, including archives and back-up repositories.[6] Critical to the exercise was a thorough understanding of the organizational structure of Swedbank and its branches, subsidiaries and affiliates in order to: (a) understand Swedbank's senior management and reporting architecture, and (b) identify the functional areas within Swedbank where potentially relevant employees might work, including employees in compliance or customer relationship management. The scoping exercise encompassed data related to Swedbank's three business lines: Baltic Banking, Swedish Banking and LC&I.[7]

Clifford Chance and FTI mapped the locations of data relating to each of the following categories:

1. Organizational Structure: documents and data reflecting the organizational structure of Swedbank and its branches, subsidiaries and affiliates;
2. Customers: information relating to current and historical customers (both natural persons and legal entities), including on-boarding and off-boarding dates, customer account information and identification of relationship managers;
3. KYC & CDD Materials: Know Your Customer ("**KYC**") and Customer Due Diligence ("**CDD**") materials, including customer identification information, account opening documents and internal bank documents reflecting customer reviews, customer risk ratings and decisions to exit customers;
4. Transactions: transaction data, including payments, loans and credit card activity involving customer accounts, as well as SWIFT data and transaction screening and monitoring data reflecting the activity of current and historical customers;
5. SWIFT Messages: structured data tables containing the full content of all messages on the SWIFT network sent and received by each Baltic Subsidiary, as well as text format messages extracted from Swedbank's report archiving system covering Swedish Banking and LC&I;
6. Current and Former Employees: live email mailboxes and email archives, employee network user shares and any network shared folders to which employees were granted access, user-generated SharePoint data, locally stored laptop data, certain mobile device records and any other records that reflect the responsibilities and conduct of current and former employees relevant to the Investigation;
7. Policies and Procedures: current and historical policies and procedures on AML compliance and related internal controls, including policies and procedures related to customer on-boarding, customer risk rating, and customer screening and monitoring;

[6] For purposes of this Report, "structured data" refers to data that is organized in clearly-defined fixed fields within a database, so that its elements can be made addressable for more effective processing and analysis, such as data tables or spreadsheets. The term "unstructured data" refers to data that is not organized in a pre-defined manner, such as email correspondence or Microsoft Word documents.

[7] Organizationally, LC&I encompasses Swedbank's international branches, including its New York Branch.

8. Meeting Minutes and Materials: meeting minutes and underlying materials reflecting: (a) relevant issues considered before Boards, Councils and relevant risk, compliance and audit committees across Baltic Banking, Swedish Banking and LC&I, and (b) those responsible for the oversight of customer relationships, including HRNR relationships; and
9. Prior Reports: documents and data regarding Swedbank's current or historical internal investigations, reviews and internal audits (collectively, "**Prior Reports**").

C. Data Retention

From the start of the Investigation, Clifford Chance requested that Swedbank take steps to ensure that all available potentially relevant data encompassing the Investigation Period was preserved. To accomplish this, Clifford Chance prepared and the Bank circulated data retention notices to preserve hard copy materials and data stored in relevant IT systems and applications, as well as any employee-generated data, including email data. This process continued on a rolling basis throughout the Investigation as additional systems and employees were identified.

Clifford Chance focused the preservation efforts on both structured and unstructured data, identifying source systems and applications, as well as repositories where data is transferred for longer-term storage. Clifford Chance did not limit retention efforts to only those systems and applications that had been confirmed for collection, but also circulated notices to all systems and applications which, based on available information, were potentially relevant to the Investigation.

As of the date of this Report, Clifford Chance prepared and the Bank circulated: (a) 426 data retention notices to employees identified as responsible for the day-to-day management and oversight of potentially relevant IT systems and applications; and (b) 703 document retention notices individually to potentially relevant employees.

D. Further Preservation of Unstructured Data

Clifford Chance and FTI also identified certain features of Swedbank's systems that had the potential to impact the preservation of unstructured data generated by employees ("**User Data**") and took additional steps to understand those features and fully preserve the User Data. In addition, Clifford Chance and FTI arranged for the retention and potential collection of laptops and mobile devices from key employees who have left Swedbank since the Investigation began.

E. Data Collection

In coordination with Clifford Chance, FTI designed and implemented forensically sound methods of extracting, processing and uploading to review platforms the data identified during the scoping discussions described above using established, standardized and tested processes. Data broadly fell into the following nine categories: (a) organizational structure; (b) customers; (c) KYC/CDD; (d) transactions; (e) SWIFT messages; (f) current and former employees; (g) policies and procedures; (h) meeting minutes and materials; and (i) Prior Reports. FTI's collection methods were intended to collect comprehensively and systematically the data and documents that could be relevant to the Investigation, which would then undergo further review and analysis.

For all unstructured data collections, prior to the start of any data collection activity, Clifford Chance and FTI prepared and followed a series of protocols for collecting and handling data from each of the identified sources. These protocols embodied rigorous, industry-standard procedures aligned with the Association of Chief Police Officers Good Practice Guidelines for Computer and Mobile Phone Based Evidence. The

protocols required an end-to-end chain of custody, using a unique cryptographic hash value ("**SHA256**") to safeguard the integrity of the data at every phase of collection and handling. The objectives of collection included maintaining confidentiality and security, verifying data completeness, applying validation controls to prevent data alteration, and preserving metadata, timestamps and folder structures.

For all such collections, FTI created two copies for redundancy: Target and Backup. Each evidence item generated was assigned a unique reference number for tracking throughout its lifetime. FTI also extracted and recorded available information about the attributes of the data and its composition, based on the source. FTI encrypted all collected data using industry-standard encryption and strong, pseudo-random passwords controlled exclusively by nominated personnel within FTI.

FTI reconstructed Swedbank's structured data in Microsoft SQL Server and Oracle analysis databases, loading relevant customer and transaction data to its proprietary platform, CUDARE ("**CUDARE**"), and all unstructured data to the e-discovery platform Relativity ("**Relativity**"). Both platforms were set up for review on a restricted, isolated network at a specialized project site (the "**Review Center**").

1. Organizational Structure

In parallel with scoping discussions, Clifford Chance coordinated *ad hoc* collections of data showing Swedbank's current and historical ownership interests during the Investigation Period, including its acquisition of the Baltic Subsidiaries. On an *ad hoc* basis, Clifford Chance also collected data and organizational charts on the current and historical structure and leadership of the in-scope locations, focusing in particular on the Baltic Subsidiaries.

Clifford Chance supplemented its data on Swedbank's historical ownership and organizational structure with forensic collections of employee data (described in detail below), which Clifford Chance used to develop a detailed overview of Swedbank's operational structure and to identify current and former employees occupying roles relevant to the Investigation. This information also assisted in prioritizing locations for review (based on size, type of customers and potential risk factors) and, as described below, employees for data collection.

2. Customer Data

FTI extracted structured customer data records from Swedbank's structured customer data systems, including Swedbank's core databases and data warehouses, covering current and historical customer relationships resident at Baltic Banking, Swedish Banking and LC&I.

For Baltic Banking, structured customer data is stored in databases for each of the three subsidiaries, in a set of primary, archive, log and reference tables that represent customer information captured by Swedbank dating back before the Investigation Period. FTI extracted hundreds of millions of distinct customer points from the databases, covering relationships across Estonia, Latvia and Lithuania for analysis.

All structured customer data collections captured all current and historical customers within the Investigation Period for each of the jurisdictions, which provided the data universe in which Clifford Chance and FTI conducted the searches described further below to identify the customers relevant to the AML risk analysis.

3. KYC/CDD Materials

For certain current and historical customers of interest to the Investigation—based on prior and pending inquiries from external parties, media reports about exposure to money laundering risks, possible links to Russian oligarchs[8] or politically exposed persons ("**PEPs**") and other similar sources—Clifford Chance collected KYC/CDD materials, including information about decisions to on-board and off-board these customers. These materials were uploaded to Relativity at the Review Center.

a. Baltic Banking

For Baltic Banking, Clifford Chance and FTI conducted site visits to identify historical repositories of KYC data. Based on these discussions, Clifford Chance and FTI identified that Baltic Banking historically has maintained KYC materials in three repositories: (a) in Baltic Banking's databases and linked document repositories, accessible through a front-end customer service and bank operations performance portal, and a back office application used primarily to manage loan financing; (b) in paper archives at third-party storage providers in each of the Baltic States (Estonia, Latvia and Lithuania); and (c) in shared folders on the Baltic Banking network. For collection and review, Clifford Chance and FTI prioritized KYC data accessible through the front-end portal and paper archives at off-site storage.

To collect KYC data through the front-end portal, FTI provided detailed collection instructions— pursuant to secure data extraction, audit logging and transfer processes governing unstructured data—to dedicated Swedbank personnel at each of the three Baltic Subsidiaries and coordinated closely on each of the collection steps. Upon receiving a collection request related to a specific customer, Swedbank personnel identified and extracted the customer materials via the front-end portal, completed audit documentation of the identified content, organized the materials by customer and transferred the exported materials to a secure network location for FTI to access.

Where necessary, Clifford Chance and FTI also performed additional review of the back office application to identify documents not accessible through the front-end portal. Any such material was subject to the same collection instructions.

To collect KYC data held in hardcopy archives, FTI provided detailed collection instructions – pursuant to secure data extraction, audit logging and transfer processes governing unstructured data – to dedicated Swedbank personnel at each of the three Baltic Subsidiaries and coordinated closely on each of the collection steps. Upon receiving a request for a specific customer, Swedbank personnel liaised with the hardcopy archive provider to request the collection and electronic scan of associated hardcopy documents. Swedbank personnel then organized the scans by customer and loaded them to a secure network location for FTI to retrieve on a rolling basis. This process was repeated as new customers of interest were identified.

For all collections, upon receiving notice of a complete collection from Swedbank personnel, FTI performed completeness checks against the received materials using Swedbank generated file-counts. FTI processed and uploaded collected materials to Relativity on a rolling basis. For each customer, FTI grouped the data collected and, with the structured customer data collection, developed a set of materials relevant to reviewing a customer's relationship with Swedbank.

[8] Applied to the region encompassing Russia, Ukraine and CIS countries, the term "oligarch" broadly refers to private sector persons in control of sufficient economic resources to influence national politics. The US Treasury Department defines "Russian oligarch" to include "Russian individuals with an estimated net worth of $1 billion or more." US Department of the Treasury, Treasury Releases CAATSA Reports, Including on Senior Foreign Political Figures and Oligarchs in the Russian Federation, 29 January 2018, https://home.treasury.gov/news/press-releases/sm0271 (last accessed 17 March 2020).

b. LC&I

Clifford Chance and FTI observed that the Bank historically maintained KYC materials for LC&I customers in three repositories: (a) LC&I's client relationship management solution; (b) its system for on-boarding new LC&I customers (which also records offboarding and compliance-related information); and (c) shared folders in LC&I's network share environment.

Adhering to the same completeness and certification principles applied to KYC data from Baltic Banking, Clifford Chance and FTI collected materials for LC&I customers of interest.

4. Transaction Data

FTI extracted structured transaction and transaction monitoring data from relevant structured data systems, including Swedbank's core databases, data warehouses, SWIFT and Single Euro Payments Area ("**SEPA**") repositories and screening and monitoring systems. The collected data covered transaction activity for current and former customers. For each customer, transaction data provides details regarding account activity—including funds transferred into and out of the account, currency, end-of-day-balances and type of transaction—which are relevant to the Investigation analysis. As with the structured customer data collection, the collection of transaction data was designed to be overly inclusive to ensure collection of all potentially relevant data.

5. SWIFT Data

Baltic Banking sends and receives SWIFT messages through the SWIFT Alliance Access ("**SAA**") tunnel. All SWIFT messages that go through the SAA tunnel are copied and recorded simultaneously into the Baltic Banking databases with message header information and field details parsed. FTI extracted 65.5 million SWIFT messages, both archived and current, from 1 January 2007 through 1 August 2019. Of this population, 26.6 million messages fell within the OFAC review period from 22 March 2014 through 22 March 2019 (the "**Sanctions Review Period**").

6. Employee-Generated Data

a. General Approach to Employee Data Collections

To identify employees of interest to the Investigation for the collection of documents and for interviews, Clifford Chance adopted an iterative and fact-based approach. Clifford Chance and FTI contacted Swedbank's Human Resources ("**HR**") division to gather background information on any relevant employee, including verification of the employee's employment, name changes, multiple email addresses or gaps in employment. The information enabled Clifford Chance and FTI to conduct a comprehensive collection and anticipate any gaps in time that may be explained by gaps in employment.

b. Centralized Sources of Employee Data

With respect to all centralized digital sources of employee data (*i.e.*, email and network share hosted data and SharePoint), FTI closely coordinated with and received the complete support of IT personnel at Swedbank in mapping each data source (including underlying technology lifespans) and creating processes for the forensically sound, repeatable extraction and transfer of data in line with the applicable information security requirements.

(i) Email: Live & Archive

FTI initiated email collections by submitting a request tracker to Swedbank personnel dedicated to supporting the Investigation. The tracker contained key identifiers for

personnel to apply to the identified email environments, including name, employee ID and email addresses. To ensure a comprehensive collection, each request queried the live environment and potential archives, regardless of the employee's working location or employment status. FTI ran verification checks to verify and confirm a complete, unaltered collection.

(ii) Swedbank Network Shares (Individual User and Group): Baltic Banking

Clifford Chance and FTI selected two snapshot points in time as sources of network share data for collection: (a) February 2019, immediately prior to the start of the Investigation; and (b) August 2019, to provide, as necessary, the data required to address any delta for the remainder of the Investigation Period.

Clifford Chance and FTI prioritized employee-generated data in the user share (*i.e.*, employee network folder) environment for all current Baltic Banking custodians, as well as former Baltic Banking custodians for whom data remained available.

Using employee ID(s) received from Swedbank HR, FTI searched the directory listings to identify file paths associated with custodians and initiated user share collections by submitting a request tracker containing the paths to dedicated Swedbank personnel. The tracker contained paths pertaining to user shares identified during searches. Swedbank IT then executed a forensically sound collection, which FTI validated upon receipt before processing and uploading the data to Relativity for review.

(iii) Swedbank Network Shares (Individual User and Group): Swedish Banking and LC&I

As described above, Clifford Chance and FTI selected two snapshot points in time as sources of network share data for collection: (a) February 2019, immediately prior to the start of the Investigation; and (b) August 2019, to provide, as necessary, a delta for the remainder of the Investigation Period.

Prioritizing employee-generated user share data linked to custodians, FTI initiated collections by submitting a request tracker containing the resolved paths to dedicated Swedbank personnel. The tracker contained paths pertaining to user shares identified by Swedbank personnel. Swedbank IT then executed a forensically sound collection, which FTI validated upon receipt before processing and uploading the data to Relativity for review.

(iv) SharePoint

FTI coordinated with Swedbank IT personnel to obtain SharePoint site listings containing data fields that included, where available, site address, name, description, owner, commission date and monthly views for live and archive sites dating back to 2016, the point at which site listings were automated. Clifford Chance performed a review of these listings, identifying and marking potentially relevant sites for collection.

FTI initiated SharePoint collections by submitting a request tracker containing the identified sites from the Clifford Chance review to dedicated Swedbank IT personnel, who then executed a forensically sound collection of the nominated data to an encrypted container for transfer to FTI. FTI then verified the collection prior to processing and uploading to Relativity.

c. Data Held by Employees

As to data held by a custodian and locally stored on his or her laptop or mobile device, Clifford Chance and FTI received the full support of Swedbank personnel in establishing collection processes, notifying custodians, addressing questions from custodians and scheduling the collections.

To perform laptop collections, FTI traveled to the custodian's location to meet with the custodian and address any questions. Upon handing the laptop to FTI, the employee signed a form to ensure chain of custody. FTI then obtained a complete image of the laptop, certified completeness and transferred custody of the laptop back to the employee.

To perform mobile device collections, FTI similarly obtained a complete image but coordinated with Swedbank and Clifford Chance to extract only chats and messages for review, thus excluding non-business personal data such as application data and photos.

d. Data Collection Metrics

Clifford Chance identified and collected documents from 148 employees—91 current and 57 former employees—and one non-employee as custodians. The 148 employees include senior management, corporate and private banking, GIA, GSI and risk and compliance personnel from the following Swedbank locations:

- Sweden: 44[9]
- Nordic or Other International Branches: 4
- Estonia: 66
- Latvia: 16
- Lithuania: 18

From these employees, FTI has extracted 3,929 GB consisting of more than 20 million individual records (such as a single email or a single Microsoft Word document) from email mailboxes and archives, user share data, laptops and mobile devices.

From SharePoint, Clifford Chance and FTI have to-date extracted an additional 88 GB consisting of more than 220,000 individual employee-generated records.

FTI has processed and uploaded all of the data to Relativity.

7. Policies & Procedures

From discussions with Swedbank personnel, Clifford Chance identified and then collected copies of Swedbank's current and historical AML and sanctions compliance materials covering the Investigation Period, including policies and procedures implemented across Swedbank, across all Baltic Subsidiaries and at individual Baltic Subsidiaries.

Clifford Chance targeted policies and procedures that, among other areas, instructed client relationship managers on KYC/CDD responsibilities, outlined methodologies on customer risk-rating, instructed compliance personnel on the handling of suspicious customers and transactions, and allocated oversight and decision-making responsibilities for customer on-boarding, maintenance, and off-boarding across senior employees and bodies.

Clifford Chance gathered additional information about policies and procedures, including their drafting history, from employee data.

[9] Including any Baltic Banking or LC&I employee based in Sweden.

8. Meeting Minutes & Materials

Clifford Chance and FTI undertook collections of meeting minutes and materials prepared for meetings, for the following bodies:

- Swedbank AB Board of Directors;
- Audit Committee of the Board of Directors;
- Group Executive Committee ("**GEC**");
- Group Risk and Compliance Committee ("**GRCC**");
- KYC Decision Making Committee for LC&I ("**DMC**");
- Supervisory Boards (Council) of Directors for each of the Baltic Subsidiaries;
- Management Boards for each of the Baltic Subsidiaries;
- Baltic Banking Management ("**BBM**");
- Business Area Baltic Banking Risk and Compliance Committee ("**BARCC**");
- Swedbank Estonia's High Risk Customer Acceptance Committee (and its predecessor, the Client Committee); and
- KYC Committees for each of the Baltic Subsidiaries.

Based on discussions with relevant Swedbank personnel, Clifford Chance and FTI identified relevant repositories of this information across multiple systems and applications, including group share folders on the network share environment, recording the locations and folder paths. FTI then mapped the file paths and submitted a request to Swedbank IT to perform a forensically sound extraction and to delivery to FTI.

Clifford Chance also gathered additional data related to meeting minutes and underlying materials from employee data.

9. Prior Reports

Clifford Chance collected approximately 2,200 Prior Reports and related documents, which detailed the origins, methodology and findings of Prior Reports, investigations and internal audits related to historical AML compliance, as carried out by personnel from GSI, Compliance and GIA or from external consultants.

F. Data Review

Clifford Chance and FTI amassed over 38 TB of data for use in the Investigation. In broad strokes, the review of that data has taken the following course:

As to structured data: (a) Clifford Chance and FTI first compiled a list of relevant search terms from a number of internal and external sources; (b) FTI then ran the list of search terms against the structured customer and transaction data to identify relevant customers; and (c) finally, FTI analyzed transactions of these customers during the period from March 2014 through March 2019 (the "**AML Review Period**") using certain algorithms designed to flag for review transactions that may raise a risk of money laundering or other financial crime.

In this regard, the fact that a payment hits against one or more of such detection algorithms does not mean that the payment should have at the time been considered suspicious. Rather, the detection algorithms are designed to identify the types of transactions that a well-functioning transaction monitoring system would flag for further review. To provide further context, publicly available sources indicate that typical false positive rates of hits using automated detection algorithms against detection scenarios to transactions for which a report is made to an appropriate FIU industry-wide are above 90%.

As to unstructured data, the review has involved: (a) the review and analysis of KYC materials; and (b) the use of search terms to extract relevant employee data, followed by the review of that data by a multi-lingual review team to address documents in Swedish, Estonian, Latvian, Lithuanian, Russian, Ukrainian and other languages (collectively, the "**Operating Languages**"), assisted over time by a machine-learned process of continuous active learning review.

These review processes for structured and unstructured data are detailed further below.

1. Structured Data Sources – Baltic Banking

a. The AML Risk Identified Customers

Clifford Chance and FTI identified a universe of customers of interest to the Investigation, the AML Risk Identified Customers, for further analysis. These include:

(1) HRNR customers as defined by Swedbank's own criteria. Clifford Chance and FTI created the population of HRNR Customers through the application of Swedbank's defined criteria for such customers: non-resident legal entities registered outside the EU countries or Norway, or that were resident in Malta, Cyprus, the United Kingdom or Luxembourg. In practice, registration and residency countries for these customers are typically the same. The residency of customers was established by reviewing the residency country in the structured customer data. Clifford Chance and FTI reviewed Swedbank's methodology for identifying HRNR customers and noted that the portfolio only included customers identified as high risk by Swedbank's internal risk ratings. Therefore, Clifford Chance and FTI only included as HRNR customers any non-resident legal entities listed as resident in one of the applicable countries in the structured data at any time, and was categorized as high risk by Swedbank at any time. Clifford Chance determined that financial institutions were not handled by the relationship management team or the High-Risk Customer Acceptance Committee (the "**HRCAC**") that managed the HRNR portfolio, and much of the transaction activity attributable to financial institutions that would have otherwise been included in this category, were attributable to major multinational banks that did not match the risk profile of the HRNR portfolio's core customer base. Clifford Chance and FTI have thus excluded financial institutions from the HRNR customer population.

(2) Additional legal entity customers residing in the same jurisdictions set out in the Bank's HRNR defined criteria but without reference to risk ratings. Whereas the HRNR customers were identified by reference to residency country, Clifford Chance and FTI identified these customers more broadly by assessing the registration country, residency country and tax residency country.

(3) Additional legal entity customers resident in certain EU countries deemed by FTI to present a relatively higher risk of money laundering, namely Bulgaria, Czech Republic, Ireland and Romania. These customers were also identified by assessing the registration country, residency country and tax residency country.

(4) Legal entity customers that were owned by persons resident outside the EU countries or Norway, or that were resident in Malta, Cyprus, the United Kingdom, Luxembourg, Bulgaria, Czech Republic, Ireland or Romania. To identify these customers, FTI and Clifford Chance reviewed structured customer data for relationships indicating "*beneficial owner*," "*shareholder*," or "*owner-user*" designations in the structured data, as these relationships indicate ownership or control. These owners were also identified by assessing the registration country, residency country and tax residency country. If these attributes were not evident, FTI looked to the citizenship country of the owner. For all Estonian e-residents, FTI also evaluated the citizenship country of the owner.

(5) Non-resident individual customers that had at least €250,000 in external transactions in the AML Review Period. To identify these customers, FTI and Clifford Chance considered residents outside the EU countries or Norway, or those who were resident in Malta, Cyprus, the United Kingdom, Luxembourg, Bulgaria, Czech Republic, Ireland or Romania. These customers were also identified by assessing the registration country, residency country and tax residency country. If these attributes were not evident, FTI looked to the citizenship country of the customer. For all Estonian e-residents, FTI also evaluated the citizenship country of the customer.

(6) Transactions of customers with counterparties at six high risk financial institutions, including those referred to in the Report as CPB-1,[10] CPB-2, CPB-3, CPB-4 and CPB-5.[11] Each of these high risk financial institutions had been implicated in one or more money laundering scandals such as the Russian Laundromat. FTI and Clifford Chance identified these transactions by searching the transaction data for the Bank Identifier Code ("**BIC**") associated with one of the high risk financial institutions.

(7) Customers identified by using search terms. Search terms were designed to capture customers in the following categories: (a) customers identified as linked to proxy networks with reputational risk issues, the Russian Laundromat, the Azerbaijani Laundromat or with connections to certain oligarchs or PEPs; (b) customers with connections to the Panama Papers and Mossack Fonseca (or "**MF**"); (c) customers that corresponded to entities subject to Magnitsky-related allegations by Hermitage Capital Management ("**HCM**");[12] and (d) customer groups, entities or persons identified through the Investigation.

To identify this last set of customers, Clifford Chance and FTI developed search terms from a number of sources, topics and categories of information located in repositories such as internal and external reports, media reports and other public or paid for databases. These included:

- customer names extracted from the Bank's Prior Reports concerning AML-related investigations or reviews;

  Clifford Chance and FTI reviewed Swedbank's Prior Reports concerning AML-related investigations or reviews and identified individuals and entities named in those reports. The review focused in particular on customers that had specific recommendations for off-boarding, due diligence, monitoring or reporting, as well as other customers that were identified in the reports because of AML-related issues. Where possible, FTI supplemented the search terms by obtaining and reviewing the source data underlying the Prior Reports.

- entities or individuals identified in Magnitsky-related complaints filed by HCM against Swedbank and Nordea;

  One of Swedbank's prior internal Prior Reports relates to the complaints filed by HCM against Swedbank or Nordea. In reviewing these complaints and performing its own search against structured customer data in 2018 (Nordea) and 2019 (Swedbank), Swedbank identified relevant customers.

[10] Transactions with CPB-1 were only considered until the end of Q1 2016, as that is the period of highest risk.

[11] The financial institutions are discussed in further detail in Section VII.A, infra.

[12] In 2007, Russian subsidiaries of the investment fund Hermitage Capital Management Limited ("HCM") were allegedly raided by Russian police and used by state officials as vehicles for stealing $230,000,000 in tax money from the Russian treasury in a fraudulent tax refund. A lawyer for HCM, Sergei Magnitsky, uncovered the scheme and, after reporting it to authorities, was incriminated for the same tax fraud. Magnitsky eventually died in prison from alleged mistreatment. These events gave rise to the Russia and Moldova Jackson-Vanik Repeal and Sergei Magnitsky Rule of Law Accountability Act of 2012 (the **"Magnitsky Act"**) by which those Russian officials believed to be involved in the death of Magnitsky were barred from entering the United States or using its banking system. The stolen funds associated with the Magnitsky scheme were allegedly laundered through banks and offshore companies in different jurisdictions, including the Baltic states, Ukraine, Cyprus, the United Kingdom, the British Virgin Islands and Moldova.

- persons and entities identified in the course of the employee data review and employee interviews; and

  During the course of the employee data review and employee interviews, Clifford Chance and FTI identified various individuals and entities as sources of AML risk. FTI searched for and identified customer relationships regarding these individuals and entities.

- International Consortium of Investigative Journalists ("**ICIJ**") Panama Papers database.

  Clifford Chance and FTI collected data from the ICIJ website. Following the release of the Panama Papers, ICIJ created a graph database available on its website containing parties identified from released data and information about the relationships among them. ICIJ rendered the data underlying the Panama Papers Database available in five files on its website: "*Entity*," "*Officer*," "*Intermediary*," "*Address*," and "*Edges*" (showing the relationships among the preceding four files). The "*Entity*" file contains the names of 213,634 companies identified in the Panama Papers Database as having been formed with the assistance of MF. FTI relied upon this list of companies in constructing the search terms for identifying customers that were formed with the assistance of MF.

In addition, Clifford Chance and FTI conducted separate research to identify the directors, officers, beneficial owners, parents, affiliates and subsidiaries of groups and institutions identified through the above-referenced process that were also then used as search terms across the structured customer database to identify additional customers to include in the analysis. To identify these related parties, Clifford Chance and FTI conducted a series of searches using the following sources:

- D&B Hoovers Corporate Family Reports;
- Orbis Company Reports;
- S&P Capital IQ Reports;
- Lexis Company Reports;
- Bankers Almanac;
- Arachnys;
- Publicly available websites pertaining to relevant entities;
- Published financial statements (where available);
- Local foreign corporate registries (in relevant jurisdictions);
- Spark-Interfax (for entities registered in Russia, Ukraine, Kazakhstan, Belarus and other former Soviet republics);
- The online database of the ICIJ;
- Open Corporates;
- Local media reports;
- Reports and unstructured data published by the Organized Crime and Corruption Reporting Project ("**OCCRP**"); and
- Other publicly available web-based sources such as LinkedIn.

FTI conducted the following steps to execute the detailed search and review over structured customer data:

- First, to enable an effective and comprehensive search, FTI isolated all customer-identifying name information housed in the structured customer data. These database columns included surnames, forenames and middle names, full names, international names, card names, name-containing address lines and any historical variant on these names for all customers without date limitation. Additionally, FTI isolated a field observed to contain BIC information for Swedbank customers.
- FTI then performed normalization procedures on the names by mapping foreign letters to a Latin alphabet, removing non-alphanumeric characters and eliminating meaningless white space. FTI created a distinct listing of normalized customer names to eliminate unnecessary re-processing of the same name. Where multiple customer IDs were associated with a single name, FTI maintained this mapping. FTI similarly normalized search terms to facilitate like-for-like comparisons with the customer names.
- FTI then executed forensic searches using the search terms over the structured customer data to identify relevant customers. In addition to true hits FTI identified related parties in the structured customer data. For example, if Entity A was included in the search term list and the structured customer data indicated that Entity A has an ownership interest in Entity B, then the relationship with Entity B was identified as a relevant customer relationship.
- FTI ran the entity search terms against the population of entity customers. Because FTI identified the existence of legal entity customers with names corresponding to the names of sole-proprietor natural persons, FTI ran the natural person search terms against the entire customer population to avoid any risk of applying natural person search terms too narrowly.
- FTI deployed search strategies designed to fit the form and volume of data being analyzed. These strategies included the use of established string similarity algorithms (such as Jaro-Winkler) deployed in execution packages designed to control processor usage and optimize for computer resources, report search progress (for large, long-run data sets), to manage input and output file formats and to log settings around search parameters. In other instances, such as in searching for MF related names, FTI adapted these tools to fit single-word or "*token*" based searches rather than full names. FTI has separately used recognized third-party search tools to validate results and for efficiency when working with particularly large data sets.
- The Jaro-Winkler similarity algorithm reports on a scale of zero to one to represent the extent to which a search term and a customer name are the same. FTI set a threshold on this scale below which a human reviewer would be unlikely to consider the term and customer name as a possible match. As part of its testing, FTI evaluated possible term/customer matches at the boundary of this threshold on a sample basis by close human review to validate the soundness of the value.
- Next, FTI personnel conducted a bulk human review of potential matches. Examining automated matching output on a line by line basis, FTI reviewers identified customer names that could reasonably be eliminated as not matching to the search term. FTI rigorously tracked all names and terms with IDs and recorded all decisions to ensure consistency and audit trail.
- Potential matches that had not been excluded following the initial manual review were then uploaded onto a proprietary customer data review platform (CUDARE) adapted by FTI for the Investigation. Enriched with machine-identified matching results, CUDARE enabled case-by-case human analysis of information from the structured customer data alongside reference data for the search terms. CUDARE

facilitated, as needed, requests for additional information tailored to the case under review to determine whether the Swedbank customer was a true match to the search term. The case-by-case review compared the objective reference information, such as registration number, contained in the structured customer data to the relevant information for the target persons or entities identified through public research in determining whether the customer was a true match to the search term.

- Comparison of this objective reference information in conjunction with the name enabled reviewers to categorize each match as "*false positive*," "*true positive*," or "*inconclusive*." FTI deployed a team of reviewers largely comprised of forensic accountants and financial services or compliance consultants to process cases, and worked according to a set of guidelines agreed upon with Clifford Chance and designed to provide a fail-safe (*i.e.*, possible matches would not be excluded without supportable rationale) and a consistent set of decisions across the reviewer population.
- Inconclusive findings triggered escalated review, which on occasion resulted in the collection of additional customer data from the Bank.
- FTI performed 100% peer review of each batch review and decision, on top of which additional quality control processes including sampling and targeted reviews were performed. The CUDARE tool maintains a full audit trail of all review decisions.

b. Identifying In-Scope Transactions for AML Risk Identified Customers

(i) Overview of methodology for application of detection scenarios

Clifford Chance and FTI reviewed all transactions for the AML Risk Identified Customers during the AML Review Period where the AML Risk Identified Customer acted as a Swedbank customer.

The review sought to identify activity that could be considered as potentially high risk in the context of the Investigation and included the following steps:

- design and apply algorithms to isolate transactions reflecting high-risk activity, such as transactions exceeding risk-weighted thresholds, round-trip transactions, repeated transactions, large round-amount transactions, transactions indicative of structuring practices and transactions involving high-risk jurisdictions; and
- aggregate the data to identify additional notable patterns and further understand the magnitude, nature and timing of high-risk activity, including by customer, transaction type, currency, geography and year.

(ii) Identification of transactions using detection algorithms

FTI took the following steps to identify Baltic Banking transactions during the AML Review Period involving an AML Risk Identified Customer that hit against one or more of FTI's detection scenarios.

The algorithms were designed to pick up certain red flags and circumstances indicative of money laundering, using certain customer data, transactional data and payment data. To develop the algorithms, FTI started with its standard library of algorithms and tailored them to incorporate FTI's and Clifford Chance's review of Swedbank's Prior Reports, documents and transactions relevant to the customer identification exercise, interviews with Swedbank personnel and FTI's and Clifford Chance's understanding of the nature of historic activity during the AML Review Period. FTI developed and implemented the following detection scenarios to identify activity such as that related to corruption, bribery, obfuscating source of funds, capital flight and unknown beneficiaries:

- Large Cash Deposits
  - Identifies customers who have deposited above the detection threshold on a single day.
- Atypical Cash Activity
  - Identifies deviations in cash activity across seasonally-adjusted monthly periods.
- Structuring
  - Identifies groups of transactions within a fixed period of time that are individually below reporting thresholds but aggregate near to or in excess of the threshold.
- Customers with Accounts that Rapidly Open and Close
  - Identifies customers whose accounts are open for 90 or fewer days.
- Customers Transacting with Bank Employees
  - Identifies customers conducting transactions with Swedbank employees.
- Transactions with Potential Shell Entities
  - Identifies transactions where the counterparty is a potential shell entity and which are to, from or through jurisdictions known to have laws favoring entity formation with little to no information and/or are known tax shelters.
- Atypical Account Deviations
  - Compares deviations in a customer's activity across seasonally-adjusted monthly periods.
- Transactions through High-Risk Jurisdictions
  - Identifies transactions to, from or through jurisdictions which are recognized as: (i) having limited regulation or controls prohibiting money laundering and/or terrorist financing, (ii) a shell jurisdiction, (iii) having high levels of corruption, (iv) known for financial secrecy, and/or (v) are sanctioned by the United States and/or the EU.
- Transactions through an Atypical Number of Countries
  - Identifies transactions involving more than three countries.
- Large Round Dollar Transactions
  - Identifies transactions that are round and unusually large.
- Parties Transacting Multiple Times on the Same Day
  - Identifies parties transacting with each other on the same day two or more times.
- Large Movements of Funds Coming into and out of an Account on a Single Day
  - Identifies days where a large sum of funds enters an account and that same amount (or within 10% of that amount) is transferred out on the same day.
- Circular Transactions
  - Identifies transactions that are sent out by a customer and received back by that same customer but via an intermediary party.
- Recycled Transaction Descriptions
  - Identifies transaction descriptions that appear across more than one customer within a month.

- Payments between One Originator and Multiple Beneficiaries
  - Identifies transactions from one originator to multiple beneficiaries on the same day.
- Payments between Multiple Originators and One Beneficiary
  - Identifies transactions from multiple originators to one beneficiary on the same day.
- Transactions through Closed Accounts
  - Identifies transactions through closed, blocked and/or dormant accounts.
- Repeated Transaction Amounts, between the Same Parties, within Seven Days
  - Identifies transactions between the same parties that occur in the same amount and more than one time within a seven-day window.
- Bidirectional Transactions
  - Identifies transactions where funds are flowing back and forth between two parties and where the value being moved is within 10% of the originally identified amount.
- Customer Account Closures where Funds are Transferred to Another Bank Customer
  - Identifies transactions that appear to be closing one customer's account and where the counterparty is another bank customer.
- Keywords
  - Identifies transactions that reference keywords that are indicative of money laundering, terrorist financing, weapons proliferation, bribery and/or fraud.

These scenarios are intended to isolate potentially suspicious patterns from what would be considered typical banking activity for individual and corporate customers. As such, these scenarios often alert on legitimate activity which can be parsed out by a focused investigation into the activity and/or continuous monitoring of the customer and its counterparties over time. In subsequent investigative steps, the vast majority (numerically) of the transactions these scenarios alert upon would be readily reconciled to legitimate business activity and excluded from further review, leaving for further investigation a much smaller number of transactions to identify actual suspicious activity.

The fact that a payment hits against the automated detection algorithms does not mean that the payment would have been considered suspicious at the time, let alone is it definitive proof that a customer engaged in money laundering or other financial crime. A typical process for a bank investigating alerts in the context of transaction monitoring would involve members of a compliance team contemporaneously considering the payment against the customer's expected activity. This process could also include seeking additional information regarding the payment (from the customer or other financial institutions involved in the transaction) to determine whether there is reason to file a suspicious activity report ("**SAR**").

In the context of automated detection algorithms in general, while false positive rates for financial institutions are not publicized by regulatory agencies, industry organizations (e.g., the Association of Certified Anti-Money Laundering Specialists) or financial institutions themselves, research from publicly available sources indicates that typical false positive rates are above 90%.

The automated detection algorithms were then applied against the transaction data. The main source for the Baltic transactions is the Baltic ledger data. The ledger maintains details of transactional activity in a customer's account, which is sufficiently

rich in most cases to populate account statements, and further includes most of the basic transactional information required by the Detection Scenarios. Ledger data includes information such as: customer and account numbers, transaction date, amount, currency, beneficiary account, name, counterparty bank and payment narrative. While the ledger data includes details about payment activity to and from a customer account, it does not include full payment details such as intermediary parties, certain messages passed between parties and additional country information like tax obligations and location of beneficial owners. As such, the transaction review concurrently referenced additional structured data sources, such as customer account profiles and change logs, as well as incoming and outgoing foreign and domestic payment details. FTI performed a full forensic extraction of transaction data, ensuring data loaded into its analysis environment was a faithful copy of the information in the Bank's system of record. Additionally, distinct sources of incoming and outgoing foreign payments and domestic payments were reconciled to ledger transaction records related to external payments for AML Risk Identified Customers. All discrepancies identified were either *de minimi*s in value or were resolved through investigation with Swedbank.

FTI reconciled ledger and foreign payments tables so that records of cancelled and otherwise incomplete payments identified in the latter were not included in the analysis of actual customer activity. Information such as counterparty BIC, which is more consistently populated in the upstream payments tables than the ledger data, was an essential source in identifying relevant transactions when considering, for example, activity with high risk banks.

FTI ran the detection scenarios using risk-weighted thresholds and parameter settings such as those imposed by regulatory bodies for reporting and disclosure purposes and industry standard thresholds for identifying atypical activity.

While Clifford Chance and FTI have applied the automated detection algorithms to the in-scope transactions, Clifford Chance and FTI have not conducted an analysis on a transaction-by-transaction basis to determine whether individual transactions triggered an obligation to file a report to the appropriate FIU under the applicable regulations. Mindful of the high likelihood of false positive alerts on legitimate business activity, Clifford Chance and FTI have indicated where transactional activity alerts on multiple detection scenarios and is therefore relatively more likely to indicate possible financial crime.

2. Unstructured Data Sources

Collections by Clifford Chance and FTI of unstructured data captured information in a range of languages, including the Operating Languages. To conduct the initial, first-level review of the collected data and assist Clifford Chance with further analysis, Clifford Chance assembled a team of contract attorneys fluent in the Operating Languages.

Clifford Chance trained, supervised and conducted quality assurance reviews of the work performed by the review team members.

a. KYC/CDD Materials

The multilingual review team conducted a first-level review of nearly 40,000 KYC/CDD documents related to Baltic Banking and LC&I customers.

b. Employee Data

FTI collected and processed the employee data for review on a rolling basis as Clifford Chance identified new custodians. Employee data collected from Swedish Banking, LC&I or the Baltic Subsidiaries was uploaded to Relativity.

To target data with a greater likelihood of potential relevance to the Investigation, Clifford Chance designed, and FTI applied, approximately 1,450 search terms and search term strings (the "**Search Term Set**"). In addition to general search terms broadly designed to capture relevant data, Clifford Chance designed terms from additional sources, including:

- the Prior Reports;
- discussions with Swedbank personnel;
- media reports;
- jurisdictions identified by Clifford Chance and FTI, based on industry standards, as presenting higher money laundering risk such as off-shore low tax jurisdictions; and
- on a rolling basis, findings of the employee data review.

To increase review efficiency, FTI provided Clifford Chance with hit metrics to evaluate the performance of terms in the Search Term Set and either refined or set aside terms that were underperforming (*i.e.*, a term that returned a high percentage of non-relevant documents relative to the percentage of highly relevant documents).

Clifford Chance also consulted the multilingual review team to identify variations of key terms in the Operating Languages, including both Cyrillic and Latin versions of Russian and Ukrainian, resulting in approximately 700 additional search terms.

On a rolling basis as new data was uploaded, FTI applied the search terms to the universe of collected employee data to create a search term responsive population.

In addition to the review by the multilingual review team, a second-level review team consisting of Clifford Chance attorneys reviewed documents tagged by the multilingual review team as potentially relevant or highly relevant. In addition to tagging, the second-level review team also analyzed and drafted summaries of documents to facilitate further analysis and discussion within Clifford Chance.

G. Employee Interviews

Clifford Chance identified potential interviewees from a number of different sources, including:

- Prior Reports;
- the review of employee data for relevance to the Investigation (*e.g.*, pertaining to AML, sanctions compliance or disclosure issues);
- reporting lines (official and *de facto*), especially with regard to those in compliance roles with managerial or oversight responsibilities;
- results of other interviews; and
- recommendations from current employees or board members.

Interviewees were identified on a rolling basis as new information was gathered and additional data was reviewed.

After identifying potential interviewees, the Clifford Chance team initiated two parallel workstreams as part of interview planning: (a) preparation of interview materials; and (b) bank authorization.

In the course of its Investigation, Clifford Chance interviewed a total of 81 individuals, including the following:

- 37 current and former employees of Swedbank AB; and
- 30 current and former employees of Baltic Banking, including:
  - 19 current and former employees of Swedbank Estonia;
  - five current and former employees of Swedbank Latvia; and
  - six current and former employees of Swedbank Lithuania; and
- 12 current and former Swedbank AB Board members, one member of the Supervisory Councils of the Baltic Subsidiaries, and one external counsel.

Certain individuals were interviewed multiple times, resulting in a total of nearly 100 interviews. Such interviews, along with a significant number of scoping and background discussions with numerous Bank employees across a variety of positions, assisted Clifford Chance and FTI in focusing on key document locations and document types.

H. Public Statements Review

Clifford Chance reviewed public statements made by Swedbank and certain executives during the period of January 2014 through March 2019 (the "**Public Statements Review Period**"). The statements Clifford Chance reviewed were contained within interim and annual reports issued by Swedbank (and materials associated with the reporting of results), other statements and presentations made in communications with investors, analysts and the financial community, materials used in connection with the offer of certain corporate debt securities issued by Swedbank and statements made in media appearances and publications.

Clifford Chance reviewed publicly available materials published by Swedbank during the Public Statements Review Period related to Swedbank AB as a listed issuer of securities.[13] Clifford Chance also reviewed written materials prepared by Swedbank in connection with Swedbank's US dollar Senior Unsecured Bonds ("**USD Bonds**") offered to qualified US institutional buyers under Securities and Exchange Commission ("**SEC**") Rule 144A ("**Rule 144A**") promulgated under the Securities Act of 1933 ("**Securities Act**"). Specifically, Clifford Chance reviewed the following categories of documents during the Public Statements Review Period to identify relevant disclosures by Swedbank and statements by Swedbank executives concerning areas that relate to the AML-related matters that are the subject of the Investigation:

(i) annual and sustainability reports.

(ii) interim reports (quarterly).

(iii) annual/quarterly risk management and capital adequacy reports.

(iv) quarterly report telephone conference transcriptions.

(v) quarterly results presentations;

(vi) quarterly investor presentations;

(vii) quarterly fact books;

(viii) roadshow presentations;

(ix) press releases;

(x) USD Bonds (Rule 144A/Reg. S) Base Prospectuses; and

(xi) select media appearances and publications.

[13] The substantial majority of the materials reviewed are located on the Investor Relations webpage located at Swedbank.com/investor-relations.html.

Clifford Chance conducted interviews with current and former employees for the purposes of understanding: (i) Swedbank's securities offerings; (ii) Swedbank's processes for creating, reviewing, and validating public disclosures made by Swedbank; and (iii) Swedbank's ongoing communications with the public, investors, securities research analysts, and financial media. Clifford Chance conducted 21 interviews of current and former employees who Clifford Chance deemed relevant to its Investigation of Swedbank's public statements, including members of the following departments: Group Investor Relations, Group Communications, Group Compliance, Group Treasury and Group Executive. Clifford Chance also conducted targeted searches of Employee Data using search techniques reasonably designed to locate materials relevant to the public statements component of its Investigation.

I. Sanctions Review

Based on review of internal reports and other materials, the Investigation identified that Swedbank historically had gaps in sanctions-related controls, including that the Baltic Subsidiaries did not systematically filter SWIFT payments or screen customer data against sanctions lists until 2017. On that basis, and in conjunction with Swedbank's broad internal investigation of historical AML issues, the Board instructed Clifford Chance to conduct a transaction review to determine whether Swedbank may have processed transactions involving OFAC sanctions targets that failed to comply with an applicable sanctions prohibition (the "**Transaction Review**"). On a risk basis, the Transaction Review has prioritized the Baltic Subsidiaries. We describe below the process and results of the Transaction Review, preceded by an introduction to OFAC sanctions.

1. Introduction to OFAC Sanctions

OFAC is responsible for the administration of a variety of statutes, Executive Orders and their respective regulations imposing economic sanctions to further the foreign policy and national security objectives of the United States. OFAC works with various federal and state regulatory agencies, as well as foreign governments, to pursue sanctions compliance. Generally, US economic sanctions seek to deprive targets of the use of their assets and/or to deny them the benefits of trade and commerce with the United States.

The relevant statutes upon which OFAC bases its authority include, among others, the Trading with the Enemy Act, applicable to economic sanctions against Cuba, and the International Emergency Economic Powers Act ("**IEEPA**"), under which the United States has imposed sanctions on, *e.g*., Iran, North Korea and Syria. OFAC also has imposed sanctions on OFAC-designated terrorists, human rights abusers, international narcotics traffickers, transnational criminal organizations and proliferators of nuclear, biological and chemical weapons. With respect to certain countries, OFAC sanctions apply only to dealings with certain designated government officials and/or other specific targets; for others, the prohibitions apply comprehensively to dealings with, or within, that country and its government. Persons and entities specifically targeted for blocking sanctions appear on OFAC's list of Specially Designated Nationals ("**SDN**s"). Under OFAC's "*50 Percent Rule*," blocking sanctions also apply to entities owned, directly or indirectly, 50% or more by SDNs.

OFAC has not imposed any country-wide sanctions on Russia, but has imposed sanctions on the territory of Crimea and, thereby, all persons located within Crimea. OFAC also has designated a wide range of Russian government officials, business persons, government-owned companies and other entities based in Russia as SDNs, among other measures introduced by the United States since 2014 in response to Russian government actions that the United States has attempted to punish or deter through so-called targeted sanctions.

OFAC requires compliance with the above-referenced sanctions not only by US persons but all persons globally, including non-US-based financial institutions, in

respect of any transaction activity that involves US territory, US persons, the US financial system or other US jurisdictional elements. Under its expansive theories of jurisdiction, OFAC has imposed penalties for sanctions violations against many of Europe's leading financial institutions. OFAC's Enforcement Guidelines distinguish "*egregious*" from non-egregious violations and contemplate the imposition of higher penalties in response to the former relative to the latter.

2. Framework for the Transaction Review of the Baltic Subsidiaries

Based on data collected and processed by FTI, Clifford Chance reviewed USD SWIFT payments processed by the Baltic Subsidiaries during the five-year Sanctions Review Period, from 22 March 2014 through 22 March 2019, to identify whether any such payments ("**In-Scope Transactions**") may not have complied with OFAC blocking sanctions or country embargos ("**Subject Transactions**").

Section IV.E. above describes FTI's data extraction process, including the extraction of the data for the Transaction Review. By applying OFAC-related Search Terms (defined at Section IV.E.4., *infra*) to the In-Scope Transactions (the "**Filtering Exercise**"), FTI identified a population of potentially-relevant transactions for legal analysis by Clifford Chance.

To supplement the Filtering Exercise, Clifford Chance also conducted an OFAC-specific customer review to identify Subject Transactions that the Filtering Exercise otherwise might not have detected (the "**Customer Review**"). For this purpose, Clifford Chance designed the Customer Review to identify customers of the In-Scope Locations that (i) engaged in USD SWIFT payment activity during the Sanctions Review Period, and (ii) based on the available information, were potentially the subject of OFAC sanctions due to:

- OFAC having listed either the customer or 50% or more of its direct or indirect owners as SDNs during the Sanctions Review Period;
- ownership by, or other affiliation of the customer with, the Governments of Cuba, Iran, North Korea, Sudan or Syria during any portion of the Sanctions Review Period that OFAC had imposed blocking sanctions on those governments;
- residency or domicile in Crimea, Cuba, Iran, North Korea, Sudan or Syria ("**Embargoed Countries**") during any portion of the Sanctions Review Period that country-wide OFAC sanctions applied to these Embargoed Countries; or
- beneficial ownership during the Sanctions Review Period by residents of Embargoed Countries.[14]

(collectively, "**OFAC-Restricted Customers**")

Clifford Chance then incorporated the results of the Customer Review into the Filtering Exercise and the broader process of identifying potential Subject Transactions. Our methodology thereby enabled us, based on the available information, to identify Subject Transactions of OFAC-Restricted Customers even if a standard OFAC filter of the US correspondent bank, when applied to SWIFT payment data, would not have detected the potential applicability of OFAC sanctions to those transactions.

3. The Customer Review

To identify potential OFAC-Restricted Customers at the Baltic Subsidiaries, Clifford Chance and FTI used the same OFAC-related Search Terms developed for purposes of the Filtering Exercise. FTI applied the OFAC-related Search Terms to the structured customer data fields of the Baltic Subsidiaries that contained the names and addresses of the customers, as well as, where available, the names and addresses of the direct shareholders, beneficial owners, account signatories and power of attorney holders

[14] OFAC sanctions do not automatically apply to a company domiciled outside an Embargoed Country based on ownership by non-blocked residents of an Embargoed Country. However, US dollar payments of such companies are at higher risk of involving the Embargoed Country and thus merit a transaction-specific review to determine if OFAC sanctions applied to them.

(collectively, "**Key Persons**").[15] FTI then reviewed the search results to identify any "*true*" hits, using FTI's purpose-built FINTRETO review tool. Among the customers that produced true hits, and therefore potentially were OFAC-Restricted Customers, FTI determined that only 49 of them had sent or received any In-Scope Transactions.

Clifford Chance reviewed the KYC unstructured information collected by the Baltic Subsidiaries (the "**KYC Data**") for these 49 customers and, based on the available information, identified 17 to which OFAC sanctions appear to have applied during at least a portion of the Sanctions Review Period. OFAC's so-called primary sanctions do not prohibit non-US banks, such as the Baltic Subsidiaries, from maintaining such customer relationships, but rather prohibit transactions by or for such customers that involve a US element, such as US persons or the US financial system.

The tables below provide a description of these 17 customers:

Apparent OFAC-Sanctioned Customers of Swedbank Estonia
One SDN under the OFAC sanctions against Transaction Criminal Organizations[16]
One SDN under the Russia/Ukraine-related sanctions[17]
One individual who appeared to reside in Crimea during a relevant time period
Two individuals who appeared to reside in Iran during a relevant time period
Apparent OFAC-Sanctioned Customers of Swedbank Latvia
One non-SDN company wholly-owned by an SDN under the Russia/Ukraine-related sanctions[18]
Five individuals who appeared to reside in Crimea during a relevant time period
One individual who appeared to reside in Iran during a relevant time period
Two individuals who appeared to reside in Syria during a relevant time period
Apparent OFAC-Sanctioned Customers of Swedbank Lithuania
Two individuals who appeared to reside in Crimea during a relevant time period
One individual who appeared to reside in Iran during a relevant time period

As part of the Transaction Review, we have reviewed the In-Scope Transactions for all 17 of these customers and included our assessment of them in our below summary of the Transaction Review results for the Baltic Subsidiaries.

Of the 32 customers within the population of 49 that did not appear, based on the KYC Data, to have been the subject of OFAC sanctions, we determined that 16 potentially fell within our definition of OFAC-Restricted Customer because they were corporations domiciled in a non-sanctioned jurisdiction ("**Third-Country Companies**") with at least one owner who, although not the subject of any blocking sanctions, potentially appeared to reside in an Embargoed Country during at least some portion of the Sanctions Review Period. For these 16, we reviewed their In-Scope Transactions

[15] In this regard, as discussed in the Report, historically there were issues with the completeness and accuracy of the customer data collected by the Baltic Subsidiaries or contained in the structured customer databases. To the extent that the Investigation identified additional information such as actual beneficial owners that may be relevant to the OFAC analysis, such information has been considered.

[16] Clifford Chance has confirmed that Swedbank Estonia established its account relationship with this customer prior to OFAC's designation of the customer as an SDN.

[17] Clifford Chance has confirmed that Swedbank Estonia established its account relationship with this customer prior to OFAC's designation of the customer as an SDN.

[18] Clifford Chance has confirmed that Swedbank Latvia established its account relationship with this customer prior to OFAC's designation of its owner as an SDN.

to determine whether they appeared to have involved an Embargoed Country, as opposed to business of the Third-Country Company with no apparent connection to an Embargoed Country (*e.g.*, a payment for legal services provided to the Third-Country Company in the third country). As part of this analysis, FTI reviewed, with input from the Baltic Subsidiaries, whether the Third-Country Companies remitted any USD payments in connection with the In-Scope Transactions through an online banking platform from an internet protocol ("**IP**") address in an Embargoed Country, in which case the Transaction Review would have included that finding in the assessment of whether the transaction appeared to involve business with the Embargoed Country. FTI identified only one USD payment remitted by a Third-Country Company from an IP address in an Embargoed Country.[19]

4. The Filtering Exercise

To conduct the Filtering Exercise, Clifford Chance instructed FTI to use the following search terms (the "**OFAC-related Search Terms**"):

i. historical entries over the course of the Sanctions Review Period from OFAC's SDN list, but, per OFAC guidance, using OFAC's so-called "*weak aliases*" only for evaluating hits on an SDN name or hard alias;

ii. the country/territory names for the Embargoed Countries and each of their five largest cities (by population), as well as several major ports/airports in the Embargoed Countries; and

iii. names and BICs for banks in the Embargoed Countries, even if not on the SDN list.

Clifford Chance instructed FTI to prepare the OFAC-related Search Terms list and apply that list to (a) USD-denominated SWIFT MT 1, 2, 4, 5 and 7 series messages, as well as MT900s and MT910s and (b) MT x9x series messages, including MTx9x messages without a currency denomination, sent or received by the Baltic Subsidiaries during the Sanctions Review Period ("**In-Scope Messages**").[20] FTI applied the OFAC-related Search Terms to the In-Scope Messages and conducted a multi-level review of the resulting hits using FTI's FINTRETO review tool to identify the true hits. FTI then prepared transaction groups comprised of (a) the In-Scope Messages that contained a true hit and (b) other SWIFT messages that FTI could link to them on an iterative basis through common reference numbers in the messages ("**Transaction Groups**"). Next, FTI identified the Transaction Groups that included at least one USD-denominated payment and uploaded them to CUDARE, FTI's purpose-built review platform, for legal review by Clifford Chance (the "**Legal Review**"). Separately, as discussed above, FTI extracted the In-Scope Messages of the OFAC-Restricted Customers identified during the Customer Review and created the associated Transaction Groups for upload to FTI's CUDARE platform and inclusion in the Legal Review.

5. Online Payments Analysis

During the Sanctions Review Period, customers of the Baltic Subsidiaries generally had access to e-banking services through which they could access an online banking platform and remit SWIFT payments, potentially without manual involvement of Swedbank employees in the entry of the payment instruction or transmission of the payment. The Baltic Subsidiaries at the time did not impose any system controls on the IP address locations from which customers with e-banking privileges could remit USD payments Swiftover the online platform. Clifford Chance asked the Baltic Subsidiaries to retrieve the relevant stored data through which FTI could identify whether any

[19] This payment, for $1,615, was remitted by a Third Country Company from its account at Swedbank Estonia. The payment went to a helicopter parts and supply company in the United States. To send the payment, the owner of the company accessed the online banking platform from Iran, the owner's apparent country of residence. Because the payment was sent from the account of a non-Iranian, non-sanctioned company, and not an account of the owner, and the payment did not appear to involve Iran, we did not classify it as a Subject Transaction.

[20] SWIFT has provided an explanation of the SWIFT network and the various SWIFT message types on its website at: https://www.swift.com/our-solutions/global-financial-messaging.

customers had executed USD payments over an online platform during the Sanctions Review Period from IP addresses in an Embargoed Country. FTI provided the list of such customers to Clifford Chance, together with the In-Scope Transactions that FTI determined that they had sent during the Sanctions Review Period from IP addresses in an Embargoed Country. In total, 84 customers (including seven OFAC-Restricted Customers) remitted 733 USD payments, totaling approximately $14.1 million, from IP addresses in an Embargoed Country during the Sanctions Review Period.[21] Clifford Chance included these payments in the Legal Review, as well as additional payments for three of these customers that appeared to operate from Crimea as well as having an owner that entered payment instructions from a Crimean IP address.

6. Legal Review of Relevant Transactions

The Legal Review involved an assessment of the Transaction Groups uploaded to CUDARE to determine whether they: (i) involved both an OFAC-sanctioned element and the US financial system or other "*US Elements*"[22] (the "**Relevant Transactions**"); and *if so* (ii) appeared to have violated applicable OFAC sanctions and thus were Subject Transactions; and *if so* (iii) involved other characteristics of potential relevance to the Legal Analysis of the Subject Transactions.

Clifford Chance used a team of US-based attorneys (collectively, the "**Legal Review Team**"), working from the Review Center, to conduct the Legal Review. To assist their analysis, the Legal Review Team used a range of publicly available and proprietary databases, as well as relevant information obtained from the Baltic Subsidiaries. In particular, for transactions involving OFAC-Restricted Customers of the Baltic Subsidiaries, Clifford Chance reviewed the relevant KYC Data as part of the transaction analysis.[23]

The Legal Review included an assessment of whether the Relevant Transactions may not have violated any OFAC sanctions; *i.e.*, for reasons such as the apparent blocking or rejection by the Baltic Subsidiaries or a counterparty bank of the payment, or an apparently applicable OFAC general or specific license. If, instead, the Relevant Transaction appeared to involve an apparent OFAC breach, the Legal Review Team classified it as a Subject Transaction based on the weight of available evidence.

The Legal Review Team also conducted a resubmission analysis to determine whether the Baltic Subsidiaries or their customers may have resubmitted, after the removal of the OFAC-sanctioned element, any payment instructions that were rejected or blocked by either the Baltic Subsidiaries or a counterparty bank for apparent OFAC-related reasons. The resubmission analysis involved the following four-step process:

- *First,* the Legal Review Team identified Relevant Transactions sent by the Baltic Subsidiaries that were blocked or rejected either by the Baltic Subsidiaries or a counterparty bank (*e.g.*, a US correspondent bank) for apparent OFAC-related reasons.
- *Next*, Clifford Chance instructed FTI to identify all USD SWIFT payment messages sent by the same customer or from the same account within three months after the rejected or blocked payment.

[21] For any such payments remitted by individual customers, we classified them as Subject Transactions unless they appeared to qualify under an OFAC general license or exemption, such as for personal remittances or expenses ordinarily incident to travel. For payments remitted from the accounts of companies domiciled in a non-sanctioned jurisdiction, such as the payment discussed at note 19 supra, we also considered whether the payment appeared to involve the Embargoed Country.

[22] "US Elements" include: (a) the US financial system; (b) US territory; (c) all persons physically located in the United States; (d) US citizens and permanent residents, regardless of their physical location; (e) all entities domiciled in the United States, including their non-US branches (e.g., London branch of a US-headquartered bank); (f) exports of US-origin goods; and (g) under OFAC's sanctions on Cuba and Iran, non-US entities that are US owned or controlled (e.g., non-US subsidiaries of US corporations).

[23] The Legal Review did not identify any trade-related Relevant Transactions that appeared potentially to involve an OFAC-sanctioned element.

- *Next*, the Legal Review Team reviewed all such payments to identify potential resubmissions of the blocked or rejected payment with the OFAC-sensitive information removed, apparently in order to enable the processing of a Subject Transaction without detection by the OFAC controls of the Baltic Subsidiaries or the counterparty bank.
- *Finally*, based on data obtained from the Baltic Subsidiaries, the Legal Review Team assessed whether the relevant customers had resubmitted any such payments through an online banking platform without manual involvement of the Baltic Subsidiaries in the resubmission and, therefore, apparently without the knowledge or authorization of the Baltic Subsidiaries.

V. APPLICABLE AML LEGAL FRAMEWORK

In this section, we provide an overview of the relevant AML legal framework under which Swedbank and the Baltic Subsidiaries operated during the Investigation Period.

A. EU Money Laundering and Terrorist Financing Regime

Each of Swedbank and the Baltic Subsidiaries are required, and have at all times during the Investigation Period been required, to comply with applicable local legislation implementing the EU's harmonized framework for the prevention, detection and investigation of money laundering and terrorist financing. The EU has adopted various Directives which set out the compliance framework for banks and certain other financial institutions ("**obliged entities**") within the EU with respect to AML and CTF compliance. The EU's rules are established in line with internationally recognized standards adopted by the Financial Action Task Force ("**FATF**") and are intended to complement the substantive criminal offenses of money laundering and terrorist financing that form part of domestic legislation in all EU member states.

In the period from 2007 through 2019, the EU adopted three Directives in this area, which built on the existing AML laws in place since the early 1990s, as follows:

First Money Laundering Directive (91/308/EEC) **("1MLD")**	Second Money Laundering Directive (2001/97/EC) **("2MLD")**	Third Money Laundering Directive (2005/60/EC) **("3MLD")**	Fourth Money Laundering Directive ((EU) 2015/849) **("4MLD")**	Fifth Money Laundering Directive ((EU) 2018/843) **("5MLD")**
Came into force on **10 June 1991**	Came into force on **28 Dec. 2001**	Came into force on **15 Dec. 2005**	Came into force on **26 June 2017**	Came into force on **9 July 2018**
Implementation in national law required by **1 Jan. 1993**	Implementation in national law required by **15 June 2003**	Implementation in national law required by **15 Dec. 2007**	Implementation in national law required by **26 June 2017**	Implementation in national law required by **10 Jan. 2020**

We provide below a summary of the key requirements of these Directives as they developed over time.

1. 1MLD and 2MLD

The EU's 1MLD (which was based on then applicable FATF recommendations) established the foundations of the current EU money laundering prevention framework applicable to obliged entities. It imposed various obligations on EU member states to require obliged entities to:

- establish the identity of their customers;
- report suspicious transactions;
- maintain records of client identity and transactions;
- establish adequate internal procedures to prevent operations related to money laundering; and
- train relevant employees on recognizing and addressing operations which may be related to money laundering.

The EU's 2MLD, which came into force in 2001, extended the range of persons falling within the definition of obliged entities and expanded the range of underlying crimes (or "**predicate offenses**") for which the proceeds were covered by the regime.

2. 3MLD

The EU's 3MLD extended and enhanced the EU's AML framework. It imposed obligations on EU member states to require obliged entities (which by then included Swedbank and the Baltic Subsidiaries) to establish and maintain appropriate and proportionate risk-based policies, procedures and controls to prevent and detect potential money laundering and terrorist financing.

These controls included detailed requirements for conducting customer due diligence whenever a business relationship was established or an occasional transaction (of €15,000 or more in value) was carried out, or when suspicion of money laundering arose. Required customer due diligence comprised:

- the identification of customers and verification of the customers' identity on the basis of documents, data or information obtained from a reliable and independent source, subject to limited exceptions;
- the identification, where applicable, of beneficial owners (owners of more than 25% or otherwise exercising control) and the taking of adequate measures, on a risk-sensitive basis, to verify their identity, in order for the obliged entity to be satisfied that it knows who the beneficial owner is, including, as regards legal persons, for trusts and similar legal arrangements, taking risk-based and adequate measures to understand the ownership and control structure of the customer;
- obtaining information on the purpose and intended nature of the business relationship; and
- conducting ongoing monitoring of the business relationship, including scrutiny of transactions undertaken throughout the course of that relationship to ensure that they are consistent with the institution's or person's knowledge of the customer, the business and the risk profile.

3MLD required obliged entities to apply customer due diligence and to conduct ongoing monitoring on a risk-sensitive basis. In certain circumstances, "*enhanced due diligence*" ("**EDD**") was required. This included any situation that, by its nature, could present a higher risk of money laundering or terrorist financing. Enhanced due diligence was also specifically required in each of the following scenarios:

- cross-border correspondent banking relationships with respondent institutions from third countries (*i.e.*, non-European Economic Area countries);
- transactions or business relationships with PEPs (essentially, any person outside of the EU member state concerned who has a prominent public function and who is, therefore, vulnerable to corruption by virtue of this position, together with family members and other connected persons); or
- where the customer was not physically present for identification purposes.

3MLD prescribed the minimum enhanced due diligence required in these circumstances, including, for relationships with a PEP, a requirement to obtain senior management approval of the relationship and ensure that adequate measures were taken to establish the source of wealth and source of funds in the proposed business relationship.

3MLD also included obligations with respect to policies, procedures, training and record keeping. Specifically, 3MLD required obliged entities to establish adequate and appropriate policies and procedures for customer due diligence, reporting, record keeping, internal control, risk assessment, risk management, compliance management and communication, in order to forestall and prevent operations related to money laundering or terrorist financing. 3MLD also required obliged entities to keep records of information and documents obtained during customer due diligence and transactions

for a period of at least five years and imposed rules regarding reliance on third parties for performing customer due diligence.

Finally, 3MLD required obliged entities to pay special attention to any activity which they regarded as particularly likely, by its nature, to be related to money laundering or terrorist financing—especially complex or unusually large transactions and all unusual patterns of transactions with no apparent economic or visible lawful purpose—and to file suspicious activity reports in accordance with local legislation to the relevant FIU.

3. 4MLD

The 4MLD replaced 3MLD on 26 June 2017. As with its predecessor, 4MLD imposed obligations applicable to Swedbank and the Baltic Subsidiaries (subject to local implementation). One of the main purposes of 4MLD was to bring the EU legal framework in line with the updated FATF recommendations by enhancing the existing risk-based approach to customer due diligence and monitoring. 4MLD provided that EU member states must require obliged entities to identify and assess the risks of money laundering and terrorist financing, taking into account risk factors such as those relating to customers, countries or geographic areas, products, services, transactions or delivery channels.

In addition to including a more thorough emphasis on employing a risk-based approach, the key changes brought by 4MLD included:

- a requirement that risk assessments, which may be reviewed by the FIU[24] in each member state, be documented and kept up-to-date;
- a requirement that domestic individuals holding prominent positions should also be classified as PEPs and subject to enhanced due diligence;
- that an exemption to performing customer due diligence ("*simplified due diligence*") would no longer apply automatically for specific customers and instead needed to be considered on a risk-sensitive basis; and
- reduction of the threshold for the requirement to carry out customer due diligence for high value cash transactions to €10,000 and above.

4. 5MLD

The EU's 5MLD amended 4MLD on 9 July 2018. 5MLD required EU member states to transpose its provisions into domestic law by 10 January 2020, the date on which it formally amended 4MLD.

B. Local Implementation

Set out in **Appendix E** are tables prepared by local counsel in each of Sweden and the Baltics, which describe the implementation of the above-referenced EU Directives into local legislation.

C. Guidance

Various international bodies have issued guidance applicable to financial institutions regarding compliance with the obligations set out above under the EU AML framework, including the FATF and the Basel Committee on Banking Supervision ("**BCBS**").

FATF is an international, intergovernmental body dedicated to combatting money laundering and terrorist financing, of which the EU is a member. FATF works to align

[24] Member states are required to have an FIU to which reports of suspicions of money laundering are made. The Swedish FIU is the Finanspolisen Rikskriminalpolisen ("FIPO"). The Estonian FIU is the Rahapesu andmebüroo unit within the Police and Border Guard Board. The Latvian FIU is the Finanšu izlūkošanas dienests ("FID"). The Lithuanian FIU is the Finansiniu Nusikaltimus Tyrimo Tarnyba.

international AML and CTF standards for use by financial services and other firms. FATF sets out its approach to AML and CTF in its published *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: FATF Recommendations*, which are reflected in the EU Directives referenced above, and issues guidance materials on best practice and other papers that are designed to assist with the interpretation of, and compliance with, the standards.

The BCBS is the primary global standard setter for the prudential regulation of banks and provides a forum for regular cooperation on banking supervisory matters. Among other matters, since 2014, the BCBS has issued the guidance *Sound management of risks related to money laundering and financing of terrorism*, which describes how banks should include risks related to money laundering and terrorist financing within their overall risk management framework. This guidance includes cross-references to FATF standards, in order to help banks comply with national requirements based on those standards.

Set out in **Appendix F** is a summary overview of key provisions of the principally relevant FATF guidance.

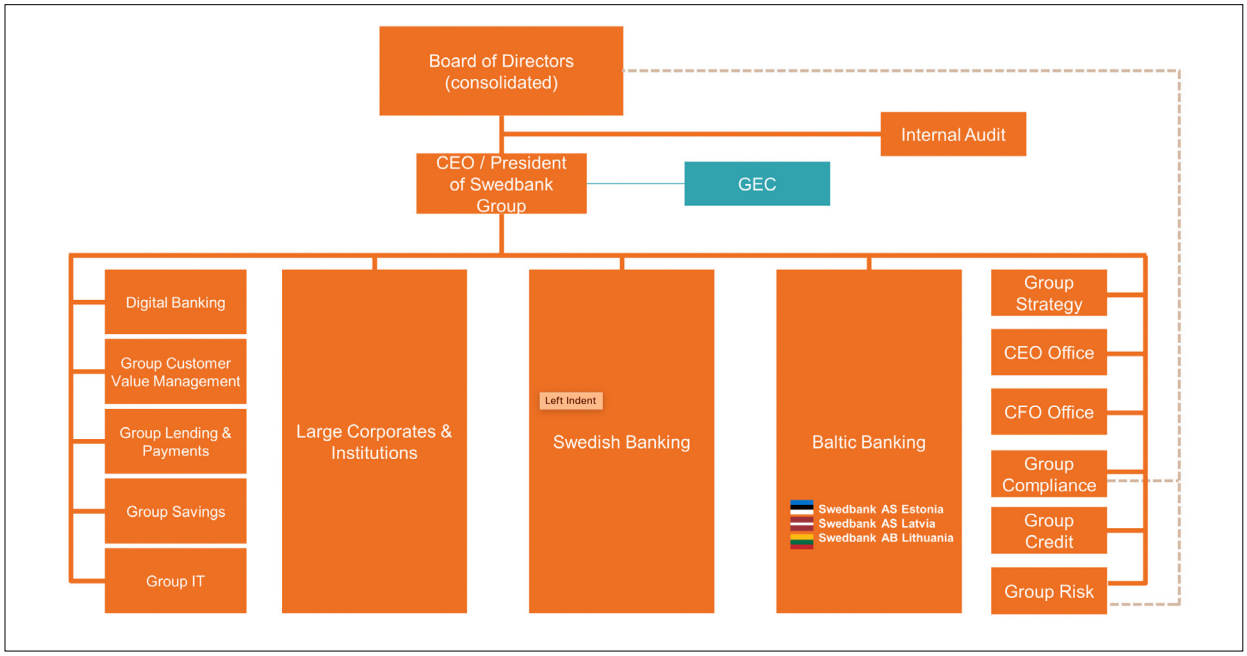
VI. SWEDBANK'S GOVERNANCE STRUCTURE [25]

As explained earlier, Swedbank operates in four home markets—Sweden, Estonia, Latvia and Lithuania—and also maintains branches in several other countries. In the Baltics, Swedbank operates through its three primary wholly-owned Baltic Subsidiaries: Swedbank Estonia, Swedbank Latvia and Swedbank Lithuania.

Swedbank's business is organized into three "**Business Areas**": Swedish Banking, LC&I and Baltic Banking. Swedish Banking handles private customers and companies in Sweden; LC&I handles large corporations and financial institutions; and Baltic Banking covers Swedbank's business in the three Baltic States, where Swedbank operates through its Baltic Subsidiaries. The managers of the three Business Areas report directly to Swedbank's CEO.

In addition to the three Business Areas, Swedbank also has a "**Group Functions**" division. Group Functions is the central division within the organization that supports Swedbank's CEO and various business operations in creating consistent routines, ensuring effective governance and monitoring throughout the organization and clarifying Swedbank's vision and strategy. Among the roles of Group Functions is to develop Group-level policies, instructions and internal rules and to supervise their implementation. Group Functions also compiles and reviews reports for the CEO and the Board, and proposes solutions to issues that require immediate action within each Business Area.

The following chart provides an overview of the Swedbank organization:



A. Swedbank AB (publ) Board of Directors and CEO[26]

The Board has overall responsibility for the conduct of banking operations in accordance with current regulations and generally accepted practices. The Board sets basic compliance guidelines through the compliance framework.

[25] This section relies on information and materials collected during the Investigation in addition to Swedbank's publicly available Corporate Governance Reports. See generally Swedbank's corporate governance reports, Swedbank, https://www.swedbank.com/about-swedbank/management-and-corporate-governance/corporate-governance-reports.html (last accessed 19 March 2020). Unless otherwise stated, the information in this Section reflects Swedbank's general governance structure throughout the Investigation Period.

[26] Please consult Appendix B for a full list of current and historical Board Members, and also the CEOs of Swedbank during 2015 through 2019.

The Board has several committees, including the Audit Committee. The Audit Committee helps identify deficiencies in governance, risk management and controls by working with the Bank's External Auditor, the Head of Group Internal Audit (who sits on the Committee) and the GEC. The Audit Committee also helps establish procedures to guarantee valid reporting and compliance (with both laws and internal regulations). The Audit Committee also receives and reviews the External Auditor's report, as well as Group Internal Audit's quarterly reports.

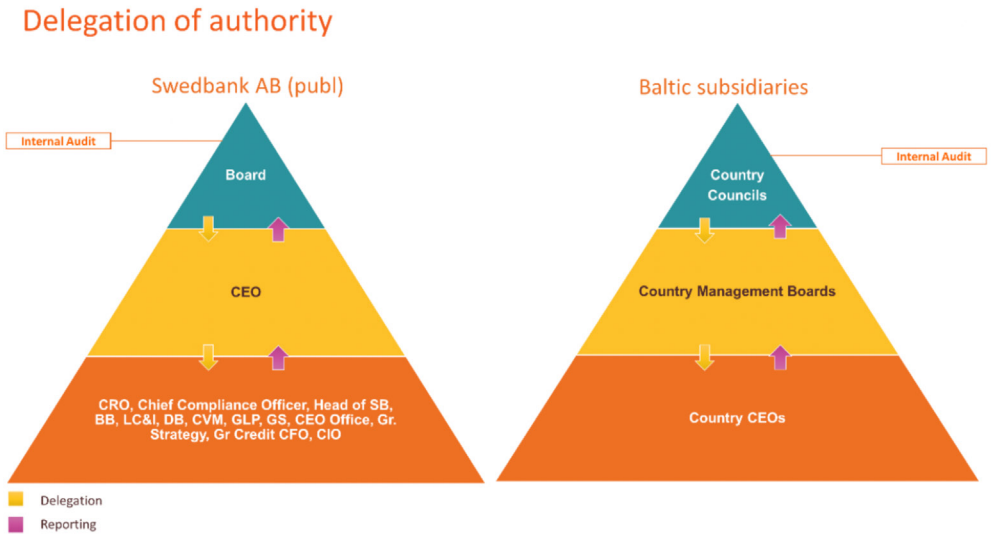
The Bank's CEO reports to the Board and is in charge of managing the Bank's day-to-day operations in accordance with internal and external regulations and within the compliance framework set by the Board. This includes AML/CTF and sanctions compliance.

The CEO may delegate power to executives through issued mandates, but ultimately retains responsibility for all decisions. Various committees support the CEO in fulfilling his responsibility for day-to-day management, including, (among others): the GEC, the GRCC and the Group Customer and Investment Committee. The GRCC supports the CEO in ensuring that routines are in place to identify and define risks relating to business activities and to measure and control risk-taking.

The CEO makes decisions in conjunction with the GEC, whose members generally include the CEO, Chief Financial Officer ("**CFO**"), Chief Risk Officer ("**CRO**"), Chief Credit Officer, Head of the CEO Office, Chief Strategy Officer, Head of Compliance/ Chief Compliance Officer, Head of HR, the Heads of Swedish Banking, Baltic Banking and LC&I and the Heads of Group Savings, Group Lending & Payments, Group IT, Digital Banking, Group Customer Value Management and Strategy Digital Banking.

B. The Baltic Subsidiaries

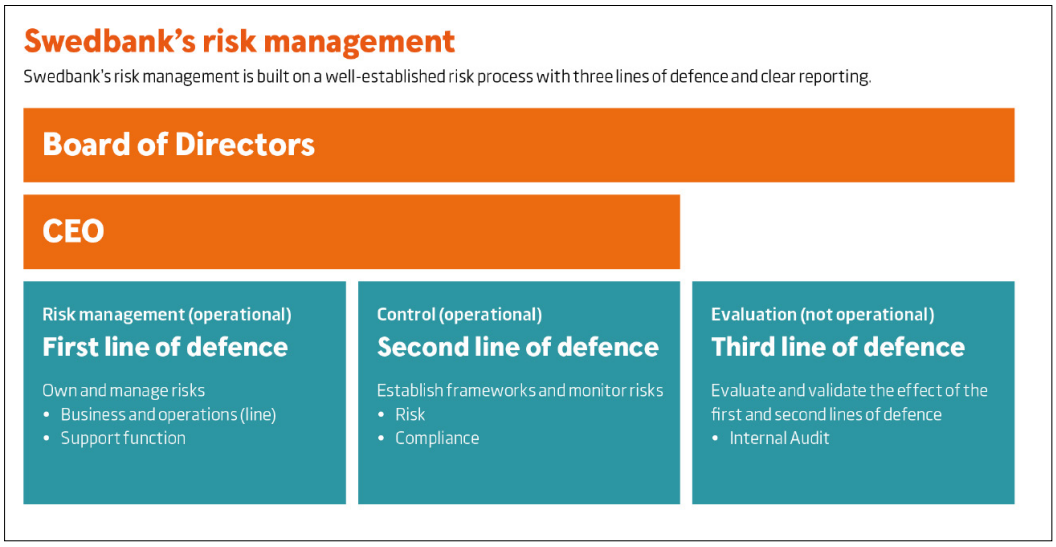
Each of the Baltic Subsidiaries is a separate legal entity from Swedbank that is governed by a Baltic Subsidiary CEO, who is part of the Management Board of the Baltic Subsidiary, which in turn reports to a Supervisory Board (the "**Council**") on at least a quarterly basis. The Council represents Swedbank as the sole shareholder of the Baltic Subsidiaries and includes senior high-level officials of the Swedbank Group (and, as to Swedbank Estonia, two independent board members). Reports to the Council concern strategic business matters and other risks (including AML). Separate reports are presented by Compliance, Risk and Internal Audit. While Swedbank is the sole shareholder of each Baltic Subsidiary, the separate legal structure of each Baltic Subsidiary and its operations in its home market, supervised by financial authorities in that market, must still be respected. Below is a diagram showing the delegation of authority and reporting lines up to February 2019.



Swedbank uses a matrix reporting structure, whereby units within the Baltic Subsidiaries have dual reporting lines to management at the Baltic Subsidiary level and to Group-level management. For example, local Compliance functions in the Baltic Subsidiaries—including each of the Subsidiaries' Compliance personnel—report both to the CEO of the relevant Baltic Subsidiary and to the Compliance function on the Group level.

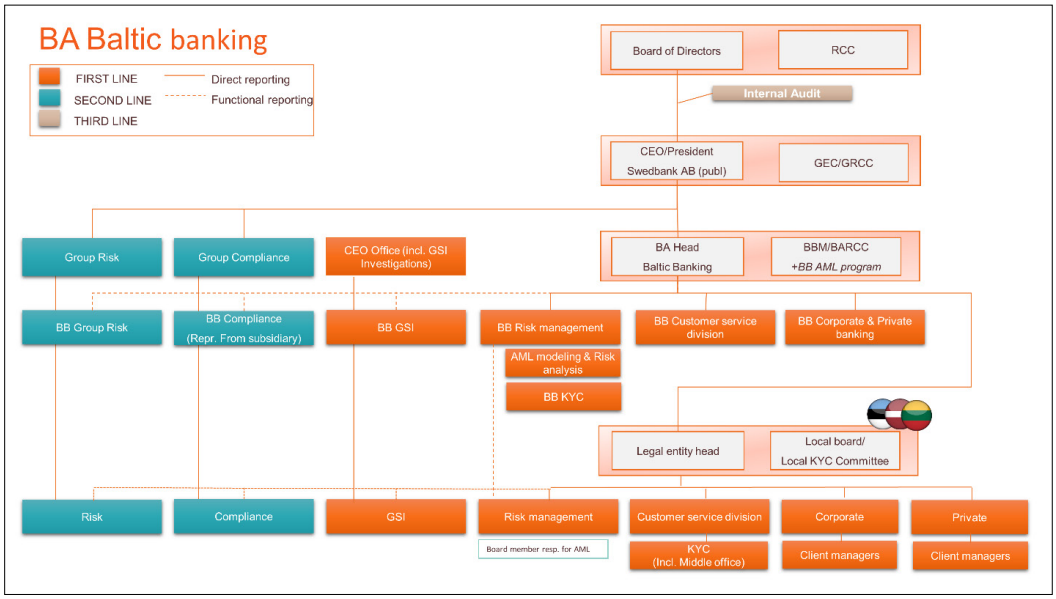
C. Risk Management Structure and the Three Lines of Defense

As shown in the diagram below, Swedbank's AML/CTF infrastructure is built on three lines of defense. This model is intended to: (a) align accountability, oversight and assurance; and (b) provide the Board and the CEO with a clear view of the oversight and management of risks within Swedbank.



The first line of defense, which includes business, operations and the support function, owns and manages risks. The second line of defense, which includes Risk and Compliance functions, establishes the framework and monitors compliance. The third line of defense, which includes GIA, evaluates and validates the effectiveness of the first and second lines of defense.

Baltic Banking similarly follows the three lines of defense, as shown in the chart below from 2019:



1. First Line of Defense: GSI and its Predecessors

The Business Areas maintain Swedbank's first line of defense, which includes collection of customer data, collection of KYC information and EDD on higher-risk customers.

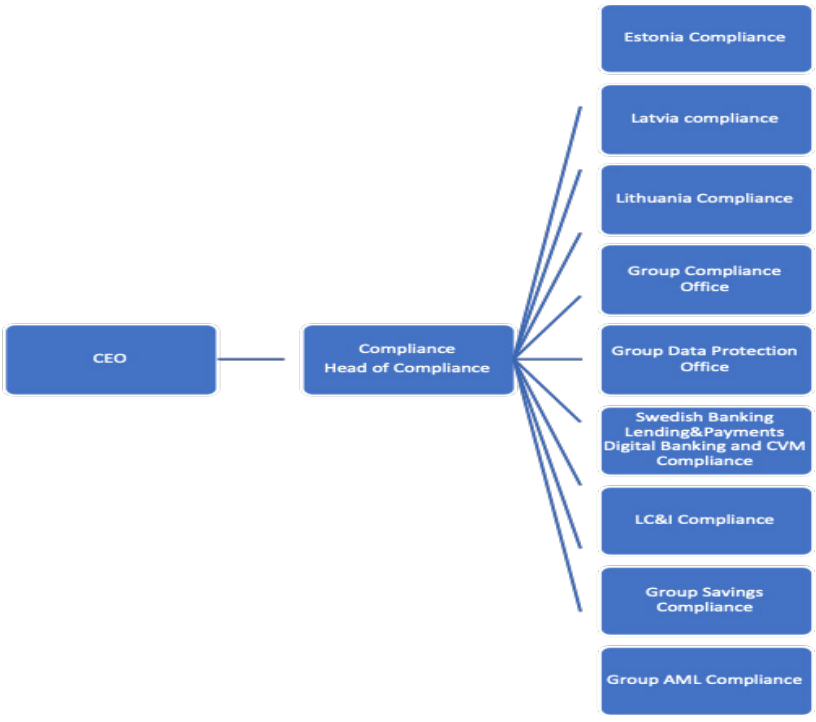
Since 2017, the first line of defense at the Group level has included GSI. Swedbank created GSI in 2017 to align its security network and coordinate its investigation processes, among other reasons. At the Group level, GSI is located in Group Functions and proposes to relevant decision-making bodies the minimum requirements in Group policies and procedures, Group risk assessments, country risk assessments, external benchmarks to secure upcoming new methodology and industry best practice, internal reporting, transaction monitoring, customer-base screening, international-payment screening and FIU reporting. GSI has local investigation units in Sweden, Estonia, Latvia and Lithuania that monitor transactions, conduct sanctions screening and perform other actions.

Prior to the formation of GSI in 2017, these activities were dispersed over different Business Areas and Group Functions across the first and second lines. With GSI's creation, Swedbank transferred some of the Compliance function's responsibilities (*e.g.*, daily transaction monitoring and screening, as well as the general AML framework) to GSI in the first line. Money Laundering and Risk Officers ("**MLROs**") and Financial Sanctions Officers, who had previously been part of the Compliance function, were also transferred to GSI.

2. Second Line of Defense: Compliance Function

The second line of defense establishes the framework for, and monitors compliance by, the first line. At the Group level, Swedbank's second line of defense in relation to AML consists of the Compliance and Risk functions.

The structure of Swedbank's Compliance function has varied, but has generally maintained the following structure since 2013.[27]



[27] For a period of time there was a Head of Baltic Banking Compliance who reported to the Group Head of Compliance.

Swedbank's Group Compliance provides assurance to the CEO and the Board on the state of AML and sanctions compliance by providing advice and support, monitoring and training. The Group Compliance function serves the following objectives: (a) overseeing Swedbank's operation in the CEO Office in relation to AML/CTF and sanctions; (b) supporting compliance at the Business Areas regarding AML/CTF and sanctions; and (c) participating in projects impacting AML/CTF and sanctions. Group Compliance regularly reports to the CEO and to the Board on matters of regulatory compliance. In accordance with a matrix reporting structure, local Compliance functions report to their area management and to Group Compliance.

Swedbank's CCO reports directly to the CEO and, according to the January 2019 CCO Mandate, is responsible, among other items, for:

- proposing, monitoring and following up on the implementation of policies, instructions, best practice, common processes and standards within Compliance to ensure an aligned governance structure across Swedbank;
- liaising with the Head of Group Risk and the Head of GIA to provide assurance to the CEO and the Board that the risk assessments and planning of Group Risk and GIA are aligned and use terminology that facilitates and enhances the overview of all risk types within the Group;
- informing and training on new laws and regulatory developments;
- following up and reporting on matters within Compliance's scope;
- delivering input to resolve matters escalated within the Compliance function;
- assisting the CEO in liaising with supervisory authorities and setting standards on communication, archiving, reporting and follow up with Regulatory Authorities;
- establishing, documenting and implementing processes related to monitoring upcoming compliance regulations for the Group to ensure the business is considering the impact of any changes in law or regulation;
- ensuring (and supporting the CEO in ensuring) that all Group policies, instructions and directives within the CCO's area of responsibility are implemented;
- meeting duties for which the CCO has functional responsibility in accordance with regulations in AML/CTF for Sweden; and
- ensuring that the Group framework regarding suspicious activity and transaction reporting meets industry standards and regulatory requirements and is properly implemented, including by ensuring the appointment of competent MLROs and Data Protection Officers and setting standards for their work.

To place the CEO in a position to escalate matters to the Board, the CCO is required to report matters to the CEO with written support and recommendations. If the matter involves a Baltic Subsidiary, the report also must be made to the Subsidiary's Management Board.

The CCO also provides: (a) quarterly written reports to the CEO and Board; (b) a yearly Group Compliance Plan encompassing key compliance risks and compliance activities for adoption by the Board; (c) a report on significant communications with financial regulators and other regulatory authorities if deemed necessary; and (d) any other reports that may be necessary.

Before GSI was created in 2017, the Group AML Compliance function included AML and financial sanctions, AML investigations and transaction monitoring, MLRO advice and training, monitoring, follow-up and reporting. Group AML Compliance also conducted customer base screening, both for sanctioned entities/individuals and PEPs. As noted above, however, in 2017 Compliance's responsibilities for daily transaction screening and monitoring and the general AML framework (*e.g.*, internal policies and regulations) were transferred to GSI, in the first line of defense. GSI also was assigned responsibility for gathering threat intelligence and trend analysis, providing advice and training, reporting to relevant FIUs and liaising with law enforcement. MLROs, who were responsible for suspicious activity reporting, also became part of GSI.

3. Third Line of Defense: GIA

The third line of defense (*i.e.*, GIA) evaluates and validates the effectiveness of the first and second lines of defense. The scope of GIA—an independent, Group-wide, centralized assurance function commissioned by the Board—encompasses all activities and entities at Swedbank. GIA provides assurance to the Board and the CEO about the effectiveness of controls, risk management and governance processes that mitigate high risk within the Swedbank Group.

The Audit Committee of the Board is responsible for the guidance and evaluation of GIA. The Chief Audit Executive ("**CAE**") is directly responsible to the Board, which has exclusive authority to appoint and dismiss the CAE.

GIA reports each audit engagement to the responsible business unit. The Business Area Risk and Compliance Committee (the "**BARCC**") for each relevant Business Area or Group Function is required to follow up on open findings, including overdue findings. The BARCC helps the relevant Business Area head (*e.g.*, the Head of Baltic Banking) make decisions. The BARCC provides a holistic overview of risk and follow-up actions required to ensure proper and effective risk management.

As of 2019, GIA reports quarterly to the Board and to the Risk and Capital Committee[28] (the "**RCC**"); previously, GIA reported to the Board and the Audit Committee. GIA's quarterly report includes significant audit findings and improvements, as well as follow up on previously reported issues.

[28] The RCC is a committee of the Swedbank Board of Directors and should be distinguished from the GRCC which is a Group-level management committee.

The shift from the Audit Committee to the RCC was intended to allow the Audit Committee to focus on financial reporting. With the shift, the Audit Committee received a yearly Compliance report (based on the CFO's assessment) of the Group's financial report, and the RCC received copies of the yearly Compliance plan, quarterly Compliance reports, the yearly operational risk plan and quarterly operational risk reports from Compliance and Group Operational Risk.

4. The Three Lines of Defense in the Baltic Subsidiaries

As mentioned earlier, Swedbank utilizes a matrix reporting structure, in which units within the Baltic Subsidiaries have dual reporting lines to local management and to Group-level management. Under this matrix reporting structure, since 2012, the CEO of each Baltic Subsidiary reports to the Head of Baltic Banking. (Before 2012, when Swedbank reorganized the corporate structure in the Baltics, Swedbank Latvia and Swedbank Lithuania were subsidiaries of Swedbank Estonia, and their CEOs reported to the Swedbank Estonia CEO, who in turn reported to the Head of Baltic Banking.) The Head of Baltic Banking reports to the Group CEO and has been a member of the GEC since the establishment of Baltic Banking in 2009.

Similarly, the Baltic Subsidiaries have maintained their own three lines of defense that utilize the matrix reporting structure. As part of the second line of defense, Baltic Banking has a unit called Baltic Banking AML Compliance, which manages Baltic AML compliance reporting.

In the third line of defense, the Head of Internal Audit of each Baltic Subsidiary regularly reports to the Council of the respective Subsidiary. Each Subsidiary Council has exclusive authority to appoint and dismiss the Head of Internal Audit of the Subsidiary, and may exercise that authority upon request by the CAE.

In 2016, Baltic Banking made organizational changes relating to KYC. First, Baltic Banking established a KYC Office as the framework owner of the KYC processes, responsible for: (a) development, implementation and maintenance of KYC processes, including customer risk ratings; (b) advisory and training functions; and (c) coordination of AML/CTF risk assessment and analysis. Second, at the Baltic Subsidiary level, a KYC Middle Office was added (reporting to the Subsidiary's branch network), which executed KYC processes for retail customers in a centralized way without the dedicated RM and made decisions on business relations with customers in accordance with given mandates.

D. Development of AML and Sanctions Compliance Policies and Procedures

Swedbank Group's compliance policies and procedures generally consist of four levels (collectively, the "**Group Framework**"):

1. policy, adopted at the Board level;
2. instruction, adopted at the CEO Level;
3. directive, adopted by Swedbank Group Function Heads; and
4. mandates adopted at the CEO Level;
5. supporting materials and other documents, which include, for example, manuals, handbooks, guidelines, and statements.

All Group Subsidiaries, including the Baltic Subsidiaries, are required to adopt their own compliance policies and procedures based on the Group Framework. In adopting such policies and procedures, the Baltic Subsidiaries would typically only deviate from the Group-level requirements if there were an objective reason to do so, such as local law requirements. Any deviations, as well as reasons for such deviations, should be documented by the Subsidiary.

VII. THE INVESTIGATION'S FINDINGS AND CONCLUSIONS

A. Swedbank's and Baltic Subsidiaries' Historical Exposure to Money Laundering and Sanctions Risk and Related Risk Mitigation Efforts

This section summarizes the salient facts developed during the Investigation regarding Swedbank's historical exposure to money laundering and sanctions risk, discusses Swedbank's prior efforts to remediate identified deficiencies, assesses Swedbank's prior public statements relating to AML compliance and considers the accountability of senior management. The Investigation adopted a risk-based approach, focusing on customer groups that posed the greatest risk. Based on the information initially available, these customer relationships primarily existed in the Baltic Subsidiaries, in particular at Swedbank Estonia. Thus, the Investigation focused on examining AML deficiencies in the Baltic Subsidiaries and how those deficiencies affected Swedbank's overall operations.

The facts are presented below as a chronological narrative divided into four parts that reflect, in broad terms, the different phases of Swedbank's non-resident and other related business primarily in the Baltic Subsidiaries. **Part 1** outlines the origins of Swedbank's HRNR business in the Baltics before 2007, Swedbank's acquisition of Hansabank, and the development of this business by the Baltic Subsidiaries (which were renamed Swedbank in 2008) through to 2013. **Part 2** describes the period from approximately 2013 through 2015, commencing with media reports linking Swedbank Estonia to the Magnitsky scheme, and concluding shortly before the release of the Panama Papers. **Part 3** focuses on events around the year 2016, when the Panama Papers leak became public, spurring Swedbank and the Baltic Subsidiaries to de-risk the non-resident customer segment in the Baltic region. Finally, **Part 4** discusses the period from 2017 through to the conclusion of the Investigation Period, during which time Swedbank undertook a number of investigation and remediation efforts in reaction to increased regulator scrutiny and adverse media reports.

1. Pre-2007 through 2013: Development of Swedbank's High Risk Non-Resident Customer Business in the Baltics

Origins of the High Risk Non-Resident Customer Segment in the Baltics

Hansabank, Swedbank's predecessor in the Baltics, began serving non-resident customers in the 1990s. As set forth above (Section II, *supra*), Swedbank fully acquired Hansabank in 2005, and the Baltic Subsidiaries continued to serve non-resident customers after the acquisition. This non-resident customer segment in the Baltic Subsidiaries included corporate non-resident customers, a portion of which Hansabank considered to be "HRNR." A report circulated to senior management of the Baltic Subsidiaries in 2016 explained that the term HRNR referred to a subset of non-resident customers in the Baltics that included non-resident legal entities registered outside the EU countries or Norway, and also those registered in Malta, Cyprus, the United Kingdom or Luxembourg. This report further explained that the majority of the beneficial owners for the corporate non-resident customers in Estonia and Latvia were of Russian and Commonwealth of Independent States ("**CIS**") origin; these Russian and CIS customers favored Hansabank since the 1990s "*[d]ue to geographical proximity, political situation and volatile economic situation in Russia[,] and high standards of banking services in [the] Baltics*."[29] According to this report, these Russian and CIS

[29] All quotations in this Report are drawn from the text of the underlying document or communication, and to the extent not in English, from translations into English of the original source text. To prepare these translations, Clifford Chance interviewed and selected, and Swedbank engaged, a team of professional linguists fluent in a range of non-English languages relevant to the Investigation, such as Swedish, Norwegian, Estonian, Latvian, Lithuanian, Russian, and Ukrainian. The team of linguists prepared translations of documents relied on during interviews and for preparing this Report, and assisted Clifford Chance as needed with on-the-spot analysis of potentially relevant non-English documents.

customers preferred to bank outside their home countries "*to protect their assets and business from potential raids by criminals and/or hostile and corrupt state authorities because the rule of law in [Russia and the CIS] countries is rather weak.*"

Estonia

In the early-2000s, Hansabank Estonia on-boarded a major non-resident customer group linked to Russia, and this customer relationship continued to grow after Hansabank became Swedbank Estonia.[30] The foundation for the relationship was laid in 2002, when an employee of Hansabank Estonia left to work for a commodities trading company ("High Risk Customer 1," or **HRC-1**"). In 2003, this former employee brought the banking business of HRC-1 to Hansabank Estonia. HRC-1 also brought affiliated companies to Hansabank Estonia and later recommended Swedbank Estonia to other customers that had ties to Russia. By 2016, HRC-1 and its affiliates (then numbering approximately 200 entities) (the "**HRC-1 Group**") constituted Swedbank Estonia's largest and most profitable group of HRNR customers. HRC-1's main beneficial owners were three Russian businessmen, two of whom were often referred to in the media as "oligarchs." As early as 2006, however, when there were approximately 250 customer entities in the HRC-1 Group, employees at Swedbank Estonia noted concerns about the opaque nature of these customers' ownership structures.

Latvia

In Latvia, Hansabank[31] also had substantial numbers of Russian and CIS customers that remained customers after the Swedbank acquisition in 2005. A manager within Swedbank Latvia's GSI unit reported that Swedbank Latvia maintained relationships with these customers despite inadequate KYC information. Swedbank Latvia also attributed the growth of its HRNR business to a Latvian "*residence permit program*" that, until 2016, gave foreigners temporary residency permits if they invested in Latvian real estate.

Lithuania

Compared with Swedbank Estonia and Swedbank Latvia, Swedbank Lithuania had fewer non-resident customers and, accordingly, a much smaller HRNR segment. However, Hansabank Lithuania did maintain a relationship with at least one HRNR customer group. From 2002 through 2004, Hansabank Lithuania on-boarded a customer group that included "High Risk Customer 2" ("**HRC-2**"). The UBO of the entities in the HRC-2 customer group (the "**HRC-2 Group**") was a Ukrainian oligarch. KYC files associated with HRC-2, however, listed a Russian citizen as the beneficial owner of HRC-2. Another individual acted as the representative of HRC-2, and was the primary contact for this customer. Swedbank Lithuania appears to have accepted the word of the HRC-2 representative that the declared beneficial owner was the representative's spouse without verifying this information. The RM for HRC-2 during the period from 2011 through 2014 met regularly with the HRC-2 representative, but never met the declared beneficial owner recorded on the KYC forms or verified the ownership interest. Since at least 2012, however, Swedbank Lithuania was aware that the actual UBO of the entities in the HRC-2 Group was a Ukrainian oligarch.

In several cases, HRC-2 Group entities requested large increases in transaction limits (in at least one case up to $50 million per day). In two instances, in 2004 and 2006, Hansabank and Swedbank Lithuania filed reports regarding suspicious transactions involving this customer group. The HRC-2 Group was subsequently associated with other suspicious transactions between 2007 and 2014. These included transactions in 2007 that appeared to lack a legitimate commercial purpose, receipts in 2010 from

[30] Hansabank Estonia is referred to in this Report as Swedbank Estonia following its acquisition by Swedbank in 2005. Hansabank Estonia did not formally change its name to Swedbank Estonia until 2008.

[31] Hansabank Latvia is referred to in this Report as Swedbank Latvia following its acquisition by Swedbank in 2005. Hansabank Latvia did not formally change its name to Swedbank Latvia until 2008.

companies associated with a proxy network, and payments between 2010 and 2013 to offshore companies allegedly linked to payments to associates of a former Ukrainian President.

Swedbank Acquires Hansabank and Prepares for the EU Third AML Directive

In 2005, Swedbank completed its acquisition of Hansabank and its operations in the Baltics. The Baltic Subsidiaries continued to use the Hansabank name until fall 2008, when they adopted the Swedbank name.

In late June 2006, Swedbank GIA issued an audit report to managers within Baltic Banking and Swedish Banking that reviewed AML initiatives in Sweden, Russia and the Baltic Subsidiaries to assess compliance with 3MLD and local requirements. Although GIA found that the money laundering prevention policy and internal instructions were consistent with EU directives, national legislation and other external rules and regulations, GIA expressed serious concerns about the implementation of these policies. For example, GIA noted that there was almost no verification of shareholders/ beneficial owners of offshore companies by the Baltic Subsidiaries, including at Swedbank Estonia, for which GIA found that "*[i]n case of legal persons high-risk non-residents . . . in almost all cases it is not possible to verify the real shareholders of companies and/or beneficial owners*."

This audit report indicated on its cover that it was submitted to the Swedbank CEO. On 21 June 2006, GIA reported high-level findings of its audit to the Audit Committee of the Board. The presentation noted that while Swedbank Estonia received an "*Unsatisfactory*"[32] evaluation with respect to "*[a]ccount opening for legal persons, non-residents*," GIA considered Swedbank Estonia to be "*Well Functioning*" with respect to overall AML compliance. Minutes from the meeting reflect that the Audit Committee concluded that "*the main parts [were] assessed as well functioning,"* but that *"in the local branch the procedures are partly assessed as unsatisfactory*."

Given the implementation of 3MLD, in July 2006 Swedbank Estonia employees recognized that they needed to enhance CDD measures for the HRC-1 Group by 2007. Indeed, Swedbank Estonia employees flagged to a local senior manager in June 2006 that representatives of the HRC-1 Group "*usually refuse[] to submit orderly information about the activity of its offshore companies and their owners*," and that the Group "*lists random people, who have no connections whatsoever to [HRC-1's] shareholders, as ultimate beneficiaries*."

Issues relating to HRC-1 Group were discussed at a Swedbank Estonia Management Board meeting in late November 2006. The meeting minutes reflect that the HRC-1 Group had named a Russian law firm as the UBO, but that the law firm "*can be assumed to act in favor of certain shareholders*." The meeting minutes also indicate that the Management Board decided to "*adopt a harder stance towards*" the HRC-1 Group, and resolved to start closing accounts if the HRC-1 Group would not provide information about the ultimate beneficiaries of its offshore companies.

One month later, in December 2006, a manager in the International Private Banking ("**IPB**") Department at Swedbank Estonia sent a letter to a representative of the HRC-1 Group, explaining that the Management Board had decided it could not accept the law firm as the beneficial owner. The letter requested that the HRC-1 Group provide "*credible*" information about its UBOs, and warned that Swedbank Estonia would begin closing its accounts if this information was not provided.

[32] According to this audit report, GIA's assessment scale at the time was as follows: Excellent, Well-functioning, Functioning, Unsatisfactory.

2007: Growth of the HRC-1 Customer Relationship

In February 2007, in an effort to address this beneficial ownership issue, an HRC-1 Group representative suggested that Swedbank Estonia look into "*possible disclosure of information of beneficial owners of the companies via Dutch private funds*," and requested a telephone call to discuss "*a proposal for 'control.'*" After the telephone call, a tentative arrangement was discussed whereby the HRC-1 Group would deploy Dutch foundations (*Stichtingen*) as shareholders in their ownership structure. In general, a *Stichting* is a Dutch structure which is similar to a trust in that it can obscure a corporation's beneficial ownership. The HRC-1 Group representative requested clarification about the information it needed to provide, and Swedbank Estonia reiterated that it required "*a detailed description of each relevant group, in order to discuss with the bank the management structure [and] method for reporting the ultimate beneficiary*."

On 1 March 2007, the HRC-1 Group provided Swedbank Estonia with "*a general description about what the schema would look like.*" Under the proposal, HRC-1 Group companies would list the Dutch *Stichting* as their beneficial owner, while the *Stichting* would separately identify its UBO(s) to Swedbank Estonia. In April 2007, HRC-1 Group sent Swedbank Estonia the Articles of Incorporation for a *Stichting* that went by the same name as the Russian law firm originally proffered as beneficiary.

On 7 May 2007, a Swedbank Estonia employee internally circulated to business and compliance personnel a draft letter to HRC-1, which conditioned acceptance of the *Stichting* structure on the customer agreeing to notify Swedbank Estonia of any changes in directors, shareholders, or beneficial owners and to provide notarized copies of passports of the beneficial owners and "*correctly executed, properly certified and legalized incorporation documents as well as a declaration of the beneficial owners*." The Investigation has not been able to confirm whether this letter was ultimately sent to HRC-1.

In around June 2007, Swedbank Estonia received a trust declaration signed by the sole director of the first *Stichting* established by HRC-1, declaring that the beneficiaries of the *Stichting* were seven natural persons, including the two Russian oligarchs identified as the HRC-1 Group's UBOs. On 27 June 2007, following a review of the documents and authorization from the AML function, Swedbank Estonia informed the HRC-1 Group that the documents for the *Stichting* had been accepted and that the HRC-1 Group could begin to open new accounts. In July 2007, Swedbank Estonia proceeded to open accounts for a number of companies in the HRC-1 Group with this *Stichting* recorded as the owner. Account opening memoranda reveal that information about the true beneficial owners of the *Stichting* was retained in the separate files of an employee of the IPB Department.

While this arrangement was being finalized, Swedbank Estonia's IPB Department was embarking on a Russia-focused growth strategy substantially based on HRC-1 Group customers. In parallel, the IPB Department represented to senior management that it was improving due diligence and streamlining its portfolio of non-resident business. On 13 June 2007, a senior Private Banking manager at Swedbank Estonia circulated documents to a member of the Board of Hansabank Group (the "**HBG**")[33] that summarized the HBG's non-resident business. In the cover email, the senior manager stated: "*I believe that here in the Baltics we are capable of doing business directed to non-residents. We understand the business and we have the skills and products that allow us to be very competitive. At the same time, our principles and activities in the three [Baltic] countries should be better coordinated.*"

[33] At that time, Swedbank Estonia was the corporate parent of Swedbank Latvia and Swedbank Lithuania, which together made up the HBG.

Attached to the email was a memorandum, which stated that non-residents, especially high-risk non-residents, "*receive special focus in all Baltic countries*," and that responsibility for opening non-resident customer accounts was "*concentrated to special business units where knowledge of off-shore business, including taxation, money-laundering, is the highest*." The memorandum stated that account openings for non-residents were "*approved by [the IPB] Committee that includes representatives from [the] business side, money laundering representatives, [and] lawyers*" and that non-residents were "*being represented by [a] client relationship manager who takes responsibility for following KYC and DD principles*." The memorandum further stated that "*[m]oney laundering is being monitored systematically by money laundering representatives*" and that there was "*[c]onstant training*" and information sharing on a "*pan-Baltic level*."

Summarizing the non-resident business, the memorandum stated that, at that time, Swedbank Estonia had "*497 accounts of corporate non-resident clients*" and had recently blocked "*[a]bout 242 of them.*"

On 18 June 2007, an IPB Department employee circulated to a senior Private Banking manager at Swedbank Estonia and other IPB Department employees a memorandum about the Russia growth strategy, which noted that, with respect to KYC, "*we have compromised with the biggest clients about disclosing their ultimate beneficiaries . . . IPB tries to improve the KYC situation on its own but they miss the support [from the internal investigation department]. The knowledge of risks within the team have improved greatly during the last year*."

The HRC-1 Group's use of the Stichting structure continued to grow and, by August 2007, five Stichtingen were documented in Swedbank Estonia records. On 23 August 2007, HRC-1 Group representatives provided Swedbank Estonia with a series of tables indicating which of the five Stichtingen were to be recorded as the beneficial owner of each HRC-1 Group entity (with some entities owned by two Stichtingen). The HRC-1 Group entities that employed the Stichting structure had either a legal entity or a natural person, or both, as their nominee shareholders and, according to documentation provided by the HRC-1 Group, these nominees assigned their rights in each HRC-1 Group entity to the relevant Stichting or Stichtingen pursuant to a trust declaration. These declarations provided that nominee shareholders of the various HRC-1 Group entities assigned dividends and "all profits and other monies" to the various Stichtingen as beneficiaries. HRC-1 Group representatives provided Swedbank Estonia with trust declarations on a rolling basis through 2007 and into 2008. On 19 November 2008, Swedbank Estonia received trust declarations outlining the purported ultimate beneficiaries of each of the five Stichtingen. The two Russian oligarchs associated with HRC-1 were listed in trust declarations as the beneficial owners of three of the five Stichtingen (the "**Declared *Stichtingen***").

The remaining two Stichtingen (the "**Undeclared *Stichtingen***") did not declare the two Russian oligarchs as beneficial owners. Instead, each of the Undeclared Stichtingen named other persons as beneficial owners, drawn from a rotating group of at least 21 persons, each identified as a Russian citizen in bank records. The Investigation has found that six of these 21 rotating beneficiaries were PEPs at the time, based on World Check and World Compliance databases. A review of the relevant KYC materials has not identified any evidence that Swedbank Estonia applied any EDD, screening or transaction monitoring for the customers nominally owned by these Stichtingen, including those with PEP beneficiaries. Internal correspondence reflects that HRC-1 Group representatives had begun providing documentation on the purported beneficiaries of the Undeclared Stichtingen by May 2008, although there is no indication that RMs for the HRC-1 Group inquired about the link between these ten persons and the two Russian oligarchs until late 2011 (as discussed further below).

Exceptions to the Rule: The Baltic Subsidiaries Issue a Decree Mandating Review of HRNR Customers

Just as the HRC-1 Group customer relationship was expanding through the use of *Stichtingen* structures, HBG issued a decree subjecting the HRNR customer segment at the Baltic Subsidiaries to greater scrutiny. However, the HRC-1 Group (among other customers) was specifically exempted from this HBG-wide decree.

On 13 July 2007, the HBG Board circulated to senior managers a decree titled "*Implementation of enhanced due diligence measures regarding high risk customers of Hansabank Group*" (the "**2007 Decree**" or the "**Decree**"). The Decree was precipitated by the Central Bank of Russia (the "**CBR**") making adverse findings in June 2007 against HBG's subsidiary in Russia (which was rebranded OAO Swedbank in May 2007). These findings prompted the CBR to temporarily restrict OAO Swedbank's operations, based on criticisms relating to non-resident customers, a lack of transaction monitoring or reporting, and concerns that OAO Swedbank was being used for potentially illegal transactions relating to money laundering or terrorist financing. A few months later, OAO Swedbank was able to resume normal operations in Russia after committing to not offering services to offshore customers except for exceptional instances in which the highest KYC standards would be applied and all transactions would be closely monitored (before OAO Swedbank was ultimately closed in April 2013). Although the CBR's findings were focused on the Russian subsidiary, HBG's senior management decided to conduct a broader review of high-risk customers linked to Russia.

In addition to the CBR's findings, in February 2007 Swedbank Estonia received the final findings of an inspection by the EFSA. The EFSA concluded that Swedbank Estonia's senior management was sufficiently focused on AML and that its procedures were consistent with local law requirements, but it also found a lack of oversight over RMs, cases of incomplete, non-existent and potentially forged documentation for customers and their final beneficiaries and an unreasonable delay by Swedbank Estonia in remediating shortcomings in its customer documentation. The report referenced specific customers as examples, including entities in the HRC-1 Group whose documents were, according to the EFSA, not accurate. The EFSA emphasized that lack of customer data or doubts about accuracy of information should be grounds for exiting the relationship.

Also in 2006 and 2007, Swedbank Latvia received reports identifying deficiencies in relation to its non-resident segment, in particular by the Latvian Financial and Capital Market Commission (the "**FCMC**"). In 2006, the FCMC conducted an inspection of Swedbank Latvia's operations, identifying instances in which the bank failed to document, or insufficiently documented, steps aimed at identifying beneficial owners for certain non-resident legal-entity customers.

Against this background, the 2007 Decree mandated that HBG would not take on new customers or continue existing customer relationships "*with companies registered in the low tax territories (offshore areas)*," with the exception of customers that met any of the following criteria:

- "*International companies which use HBG asset management services*;"
- "*International companies and their related legal entities for which HBG is offering Trade Finance and general financing services*;"
- "*International companies and their related legal entities providing shipping services*;" *or*
- "*International companies which are shareholders of Baltic states' resident companies with sizable business activities in the Baltic states.*"

The author of the Decree, an AML employee, explained in a follow-up email that the term "*International Companies*" was meant to refer to "*offshore*" customers. Beyond the four categorical exceptions, the Decree also authorized the Management Board of Swedbank Estonia (which oversaw the HBG and was the corporate parent of Swedbank Latvia and Swedbank Lithuania) to make further exceptions, without addressing the scope of such exceptions. For example, it was not clear whether the Management Board of Swedbank Estonia could make new categorical exceptions or only exempt individual customers on a case-by-case basis.

For existing customers, the Decree instructed all HBG entities providing services to "offshore customers" to conduct an "*additional inspection*" and "*risk assessment*" by 15 August 2007, and either terminate any customer relationships that were not permitted or seek an exception from the Board.

Following the Decree, the Baltic Subsidiaries began assessing their respective customer portfolios and considering questions such as how to define an *"off-shore*" jurisdiction, whether and how to inform partner banks, and the impact of the Decree on units dedicated to non-resident business. On 30 July 2007, Swedbank Lithuania issued an order affirming the Decree.

On 18 September 2007, HBG's AML unit asked for an update on efforts to implement the Decree, including whether the Baltic Subsidiaries had on-boarded any "*offshore customers*" since the Decree and the findings of their inspections of existing customer portfolios. The Baltic Subsidiaries each responded, detailing the number of new accounts opened pursuant to permitted exceptions, the number of accounts closed for non-conforming customers, and exceptions for certain existing high-risk customers, including the HRC-1 Group and the HRC-2 Group.

Swedbank Estonia reported that it had opened accounts for seven customers and closed accounts for 28 customers. Swedbank Estonia further reported that, during September 2007, it would review accounts for "*150-250 relationships*." Swedbank Estonia asserted that the Decree should not apply to, among others, the HRC-1 Group "*even if they are not in our strategic focus*," claiming that they understood the beneficial ownership structure for HRC-1 and that it "*has strong connections with [the] Estonian economy*." The presentation cautioned that terminating such customer relationships would create the risk of a "*[n]otable decrease in deposit volumes and related fees*," causing the beneficial owners of the HRC-1 Group to have "*negative attitudes regarding our Bank*," and leading to "*[u]ncertain consequences for Swedbank in Russia*."

Swedbank Latvia reported that it had opened accounts for seven customers and closed accounts for 37 customers. It also reported that business and risk-management personnel were, in parallel, jointly building a list of more than 30 customers that did not meet the Decree's exceptions but nonetheless "*could be significant for the bank*." Swedbank Latvia reported that the final version of this list would be approved by the Swedbank Latvia Management Board and that the Management Board "*foresees the confirmation of every single customer*."

Contemporaneous exchanges between an AML officer and employees from Swedbank Latvia's Non-Resident Banking Unit—at that time, a unit comprised of about ten full-time employees (including RMs) housed within Private Banking—reflect an effort to build a "short list" of existing customers to present for authorization under the Decree's exception provision. The latest identified version of the "*short list*," dated 25 September 2007, identified 36 customers for review. The Investigation has identified that of these 36 customers, five were closed in 2007, an additional three were closed in 2008 and Swedbank Latvia continued its relationships with the remaining 28 customers until their accounts were closed by the end of 2016.

Swedbank Lithuania reported that it had opened one account for a Cypriot entity and closed accounts for 19 other customers pursuant to the Decree. Swedbank Lithuania further reported that it would continue serving certain customers, including HRC-2 Group companies. With respect to the HRC-2 Group, a Swedbank Lithuania senior executive signed an order on 24 September 2007 (which referenced and enclosed the Decree), authorizing Swedbank Lithuania to continue its relationship with the HRC-2 Group, provided that Swedbank Lithuania "*continu[ed] to monitor their business activities*." The order enclosed a justification prepared by the relevant business unit, which (i) included several risk-mitigation measures, including in-person meetings with RMs, and (ii) referred to a previous Lithuanian FIU report on certain transactions which "*did not find any facts that caused suspicion*." The justification also stated that Swedbank Lithuania "*makes a lot of net income from the client*" and that, when requested, the client submits all necessary information to "*verify the transparency of . . . transaction*s."

A memorandum prepared in October 2007 regarding the implementation of the Decree throughout HBG stated, among other things, that the Decree had thus far led to the termination of 75 customer relationships. However, despite the EFSA's findings earlier that year that HRC-1 Group entities had submitted invalid documentation, the memorandum acknowledged that Swedbank Estonia would exempt the HRC-1 Group from the Decree, noting its "*well-known and in-good-standing owners*" and that the HRC-1 Group had "*approximately 250 different companies*."

The memorandum also stated that a "*new business strategy was created for IPB which should be adopted by [the] Board*," and that the IPB Department was implementing a "*more conservative approach*" since the adoption of the Decree, including a requirement that "*[a]ll new offshore customers must get approval from Client Acceptance Committee*," which also "*include[d] [a] member from [the] AML Dept*."

During the implementation of the Decree, and while Swedbank Estonia was pivoting to a Russia-growth strategy, GIA recognized increased risks from exposure to payment flows in Russia and the Baltics. In November 2007, GIA issued an audit report that recognized a change in risk profile due to Swedbank "*becoming [a] truly international bank*," citing as an example an increased exposure to payments to the Baltics and Russia. GIA recognized that the changing risk profile would require a "*higher level of competencies for all the staff involved in AML issues*" and therefore emphasized the importance of "*qualitive and continuous training of the employees involved in all stages (prevention, monitoring, reporting etc.).*" GIA rated the governance of the AML program implementation project in Swedbank and the Baltic Subsidiaries as "*Functioning*," a grade that, according to the nomenclature used at the time, was second-to-lowest and indicated that *"[i]dentified shortfalls are considered unfavourable and must be dealt with in the near future*." On 22 November 2007, GIA circulated this audit report to the CEO of Swedbank and to senior managers of the Baltic Subsidiaries. GIA reiterated its "*Functioning*" rating in a report presented to Swedbank Lithuania's Audit Committee during a meeting on 11 December 2007 (which was also attended by members of the Audit Committee of the Swedbank Board). The minutes of this meeting do not reflect any discussion of these findings.

Approval of IPB Business Strategy

On 11 January 2008, IPB made a presentation to the Management Board of Swedbank Estonia titled "*International Private Banking Business Strategy 2008-2011*." The presentation advocated using existing *"Private Banking knowledge, service model and products to offer traditional private banking services and long-term relationship management to Russian/CIS customers*." The targeted customers were wealthy Russian nationals, owners of small- or medium-sized businesses, middle managers in large companies, and private individuals willing to invest more than $300,000 of assets with Swedbank Estonia. The strategy set growth targets of 300 new customers in 2008 and 700 new customers in 2009 and proposed "*commissions/bonuses for new customers*." The presentation stated specifically that the HRC-1 Group was

"*included in [the] business plan*." Minutes of the 11 January 2008 meeting confirm that the Swedbank Estonia Management Board approved the strategy and, per the presentation, set a requirement that new IPB customers have a minimum of $300,000 of assets with Swedbank Estonia.

Meanwhile, following the Decree, both Swedbank Estonia and Swedbank Latvia continued to exit customer relationships. A presentation dated 24 April 2008 by the HBG's AML function reported that Swedbank Estonia's efforts to exit customer relationships had, at that point, resulted in relationships being closed with "*321 offshore companies*." A summary report from the AML function at Swedbank Latvia to its Management Board stated that, as of 30 May 2008, the Non-Resident Banking Unit had reduced its portfolio to 231 customers (from 767 prior to the Decree).

On 26 November 2008, a senior IPB manager presented the IPB's new organizational structure to the Management Board of Swedbank Estonia. The presentation reflected a continued focus on the acquisition of non-resident customers and included a slide outlining the role of the "*Service manager II*" within the IPB Department, who would be responsible for "*Russian speaking, non-resident and high risk customers*."

A later version of this presentation from February 2009 colloquially described this position as the "*Service manager/Russian desk*," a term that referred to a Russian-speaking group of employees within Private Banking at Swedbank Estonia who serviced Russian and CIS customers. On 7 April 2009, an AML manager for the Baltic Subsidiaries emailed senior risk management personnel to discuss the "*current AML/CTF risk environment*." The email stated that "*[t]he main users of offshore structures in Baltic Banks are Russian businessmen or businessmen who operate in Russia*" whose "*purpose is to hide company's real owners, the scope of its business or the nature of it for the reason [of] safety, tax optimization (i.e. to avoid double taxation) or conduct or hide tax evasion*." The email continued:

> *To serve Russian business clients who need transaction services we need specialists who have the necessary competences. Without these specialists it is very difficult, probably even impossible, to assess the risks of . . . [a] client and its business. Therefore it is impossible to offer the service the client needs. The existence of this kind of specialists should be the prerequisite of entering this business area. The usual practice in these cases is the formation of so called Russian Desk . . . [a] collective of specialists who knows client[] needs and Russian conditions, business culture and environment well enough. Although Swedbank has this structure, it is located separately in different departments in Latvia and Estonia.*

Also in April 2009, the IPB Department made a presentation to the CEO of Swedbank Estonia on the strategy for HRNR business. The presentation outlined the "*[p]reconditions*" and "*[r]equired actions*" for the expansion of the business, including targeting "*CIS countries' private individuals and their asset holding companies with financial assets at least 65,000 EUR*" and using "*external partners (agents, law [firms] . . .)*" to identify new customers.

Formation of Committees for Non-Resident Business at Swedbank Estonia and Swedbank Latvia

On 1 February 2008, around the same time as the adoption of the IPB Business Strategy, Swedbank Estonia established the HRCAC to evaluate the on-boarding of non-resident customers, and adopted rules to govern that process. The HRCAC was a successor to the IPB "*Client Committee*," which began recording minutes of its proceedings in April 2006.

The rules provided that the HRCAC would be composed of the IPB Head, representatives from Baltic Banking's Anti-financial Crime and Investigation Services ("**AFCIS**") and Swedbank Estonia's Legal Department, with powers granted by the Swedbank Estonia Board to "*assess[] and decid[e] account opening matters for high-risk customers and entering into service agreements*." The rules defined "*high-risk customers*" as "*high-risk non-residents, persons with political influence (PEP) and their affiliates, and other persons . . . the Bank has identified [as being] a hightened [sic] risk and who require an individual decision regarding the creation of a client relationship*."

In practice, the relevant RM would submit a "*High Risk Non-Resident Customer Memo*" to the HRCAC. The HRCAC would then generate a memorandum of its decision to accept or reject the customer. These memoranda typically contained a description of the customer's business (sometimes accompanied by information about beneficial owners or ownership structure), but did not provide an AML risk assessment. The memoranda typically recommended acceptance of the customer, frequently with a requirement that the HRCAC reexamine the customer in four months. Where such a re-examination occurred, the updated High Risk Non-Resident Customer Memo was often identical to the earlier version.

Moreover, the HRCAC was often aware of opaque ownership structures for customers it accepted. For example, with respect to the *Stichtingen* structures used by the HRC-1 Group, the HRCAC received an October 2009 memorandum prepared by a Swedbank Estonia RM, which stated that one of the main entities in the HRC-1 Group was meant to retain the HRC-1 Group's assets *"mainly behind off-shore companies,"* including assets such as real estate in Russia, Turkey, the United States and elsewhere. The memorandum stated that "*[m]ostly the beneficiaries are 5 Dutch foundations (Stichtings), and we have Declarations of Trust for each Stichting that show natural persons as ultimate beneficiaries. The client [HRC-1 Group] owns . . . [about] 190 companies with accounts in Swedbank*."

Meanwhile, Swedbank Latvia had an analogous non-resident committee since approximately October 2006, which was referred to by its full name, the *Nerezidentu apkaposanas komitejas*, its acronym, the "**NAK**," or as the "*NAN Committee*" (referring to the acronym for the Non-Resident Banking Unit at Swedbank Latvia).

Until late 2009, the NAK did not operate under formally adopted procedures, although a draft policy document from October 2008 indicated that the NAK consisted of two primary representatives, one each from the Non-Resident Banking Unit and from Swedbank Latvia's AML function. In addition, a review of various agendas and meeting minutes indicate that others were frequently invited. According to the draft policy, the NAK was responsible for evaluating both prospective and existing non-residents. To set the agenda for NAK meetings, members of Swedbank Latvia's Non-Resident Banking Unit completed and submitted via email customer background forms for review, which included information on the customer's economic activities, whether the customer was affiliated with a PEP, and the compliance risks.

The draft policy further stated that when the two primary NAK members could not agree, the case could be referred to senior management. This was consistent with the recollection of an employee from the AML function who served as a NAK representative and recalled, that in cases of disagreement, a Swedbank Latvia senior manager would make the final decision about whether to on-board a customer. Email correspondence reflects that the NAK frequently brought decisions to a Swedbank Latvia senior manager for approval, even when the two primary representatives agreed or when the AML representative agreed on the condition of additional EDD measures. When interviewed for the Investigation, the AML employee stated that the business unit tended to have greater influence over the final decision than the Compliance function had at that time.

In December 2009, Swedbank Latvia revised its policy on non-resident customers and formalized the NAK's existing procedures. The NAK's essential function remained the same—namely to decide whether to establish or continue relationships with non-residents, accounting for "*the customer's business activity, risks, purposes of opening the account, as well as the desirable range of products and services*" sought by the customer. It continued to consist of two primary representatives, one from each of the Non-Resident Banking Unit, and Swedbank Latvia's newly created customer transaction monitoring and security unit.

Swedbank Lithuania Maintains the HRC-2 Customer Relationship After Identifying Potentially Suspicious Transactions

Following the issuance of the Decree, Swedbank Lithuania continued to service the HRC-2 Group after having identified potentially suspicious transactions. For example, in July 2007, an HRC-2 Group entity entered into a contract to purchase paintings for approximately $7 million, with the payment guaranteed by an individual linked to the HRC-2 Group. Several months later, employees at Swedbank Lithuania noted that a related series of transactions involving the HRC-2 Group appeared suspicious because affiliated entities were defaulting on intra-group guarantees, thereby necessitating intra-group payments. One employee questioned whether the transactions were simply "*selling air*" (*i.e.,* engaging in transactions that lacked a legitimate commercial purpose).

In May 2008, Swedbank Lithuania received an inquiry from a correspondent bank about the series of payments over consecutive days and in similar amounts that had been made by HRC-2. Swedbank Lithuania employees sought additional information from HRC-2 regarding the nature of these transactions so as to respond to the correspondent bank. In an internal email, one employee noted, "*[t]he trouble is that this is a classic way to hide laundering (by dividing the amount into smaller parts). If they had at least chosen a longer period of time or varied the sums a bit, but now it looks really bad😊Of course, this is for AML/Compliance to decide . . .*" Notwithstanding these concerns, Swedbank Lithuania continued to service the HRC-2 Group for over five more years, until 2014.

At the time of these transactions, Swedbank did not have a detailed transaction monitoring policy. Rather, applicable policies referred to monitoring suspicious transactions in the context of CDD reviews. For example, Swedbank Group's 2007 AML/CTF Policy included only a general requirement that the Bank conduct "*ongoing monitoring of the business relationship and transactions to ensure that the transactions are consistent with the knowledge of the customer*" as part of its CDD procedures. From 2010, however, Swedbank's Group-level AML/CTF Directive included separate AML/CTF transaction monitoring requirements that were independent of CDD. In any event, the Investigation did not identify evidence that Swedbank Lithuania employees took steps to ensure, as required by Swedbank's 2007 AML/CTF Policy, that the transactions conducted in July 2007 were consistent with their knowledge of the business activities of the HRC-2 Group.

Development of Customer Risk Rating Policies

In May 2008, Swedbank established a Group-wide policy on AML/CTF ("**2008 Group Directive**") that mandated a risk-based approach "*[b]efore or in conjunction with establishing a Business relationship*." The 2008 Group Directive required that a risk classification be assigned to each business relationship based on an assessment of customer risk, country/geographic risk, product/services risk, and channel risk, aggregating these factors according to four risk levels:

- Low Risk – negligible money laundering risk; simplified due diligence and other risk mitigation measures are applicable.
- Medium Risk – low money laundering risk; standard due diligence and other risk mitigation measures are applicable.

- High Risk – conceivable money laundering risk; EDD and scrutinized risk mitigation measures must be ensured.
- Non-Acceptable Risk – money laundering risk is present and with critical impact; the goal of mitigation measures is to avoid, control or terminate the identified situation (*e.g.*, business relationship).

The 2008 Group Directive also required that the risk assessment of a customer "*consider the potential impact of the risks facing the entire Swedbank Group*."

The Baltic Subsidiaries adopted a risk-rating policy in 2009 that reflected aspects of the 2008 Group Directive, and ranked customers in five risk segments: (1) Low Risk; (2) Medium Risk; (3) Medium-High Risk; (4) High Risk; and (5) Unacceptable Risk (under this policy, the Medium, and Medium-High Risk categories were recognized as correlating with the Medium Risk segment applied at the Group level). These 2008 policies (with various amendments) were not substantially modified until May 2017, when a new Group-wide risk-assessment policy was adopted.

AML Issues in the Baltic Subsidiaries and Elsewhere

Around the time that Swedbank established its 2008 Group Directive, GIA continued to identify deficiencies with respect to AML processes in the Baltic Subsidiaries. On 15 July 2008, GIA issued an audit report that found KYC processes and AML/CTF training were overall "*Functioning*" in the Baltics, but required further enhancements. Among other things, this audit found: (1) a lack of definite criteria for AML training; (2) shortcomings in addressing previous AML audits; and (3) delays in adopting Swedbank's AML/CTF Policy.

Recipients of GIA's final report included senior managers of the Baltic Subsidiaries and Swedish Banking. GIA also presented its findings at a 17 December 2008 meeting of the Swedbank Lithuania Audit Committee, which members of the Audit Committee of the Swedbank Board also attended. The minutes of this meeting do not reflect any specific reaction to the findings.

In 2008, the then-CEO of Swedbank received reports identifying certain AML deficiencies in the Group, including the Baltics. For example, an EFSA on-site inspection report of Swedbank Estonia that listed the Swedbank CEO as "*Chairman of the Supervisory Board*," indicated that while Swedbank Estonia's internal regulations were significantly "*conforming to the requirements; Bank is aware of deficiencies in documentation (E.g., establishing UBO)*." Another report from August 2008 by Group Risk Control regarding transaction monitoring focused the "risk situation" on transaction monitoring deficiencies in Russia and Ukraine, noting that "*Baltic Banking AML transaction monitoring capability [has been] enhanced.*" By early 2009, the minutes from the 22 January 2009 Board of Directors meeting reflected that the CEO "*concluded that [they] believe[e] that the bank has adequate routines on the subject [AML]*," but the minutes do not explain the CEO's basis for this conclusion, and reflect no further questions from the Board on this conclusion.

2009: Dissolution of the IPB Department at Swedbank Estonia

In 2009, after discovering evidence of misconduct by both current and former employees of the IPB Department, Swedbank Estonia dissolved the IPB Department and initiated a review to off-board certain non-resident customers. In April 2009, Swedbank Estonia learned that the Estonian FIU had commenced proceedings against a former non-resident customer of the IPB Department in relation to possible money laundering. As it cooperated with the Estonian FIU's investigation, Swedbank Estonia recognized that it was missing key customer and transaction documentation for the customer and its related companies, prompting Swedbank Estonia to begin its own internal investigation of IPB's handling of the then-former customer.

Swedbank Estonia's investigation revealed that certain employees in the IPB Department had failed to obtain adequate KYC information regarding the customer, and had failed to retain customer documentation. Swedbank Estonia also identified a number of transactions by the customer for which IPB employees had failed to either obtain adequate supporting documentation or follow proper procedures. The report also concluded that, on one occasion, it was "*likely*" that a passport copy validated by an IPB employee was used to create a false identity for an account and card user.

A report prepared as part of Swedbank Estonia's investigation identified systemic failings at the IPB Department that enabled these activities, noting the existence of "*widespread shortcomings in the functioning of the internal control system and . . . the organization of services to high-risk customers, which was ongoing despite repeated attention to the shortcomings identified by . . . management*." While certain employees resigned, and others were dismissed or disciplined as a result of the misconduct, several IPB RMs remained at Swedbank Estonia after the IPB was disbanded.

In 2009, GIA again identified certain deficiencies in AML processes at the Baltic Subsidiaries. In December 2009, GIA issued an audit report analyzing money laundering prevention measures across Swedbank and the Baltic Subsidiaries and rated them overall as "*Well-Functioning*," a rating described as "*[i]dentified shortfalls are considered minor.*" Nevertheless, the audit found that "*[n]on-domestic PEP acceptance procedures differ in each Baltic . . . Country . . . The internal regulations are outdated in Estonia and Lithuania regarding acceptance of PEPs and do not reflect the actual process*." The report further noted that "*[i]nefficient internal control rules and insufficient internal regulations could lead to [non-]compliance with AML law and risk that PEPs are not handled according to [the] Group AML framework*." This report was circulated to senior managers at Swedbank and the Baltic Subsidiaries. On 21 January 2010, GIA presented its Q4 audit findings to the Audit Committee of the Swedbank Board, but the minutes and written materials do not reflect that these findings were included in that presentation. Internal GIA documentation reflects that GIA closed these findings by May 2010.

A year later, a December 2010 GIA report found that the sufficiency and effectiveness of AML controls and monitoring procedures were "*Satisfactory*" in the Baltic Subsidiaries, a rating similarly described as "*[i]dentified shortfalls are considered minor. No [m]ajor weaknesses identified*."[34] GIA did note that AML reporting and coordination at the Baltic Banking level could be more efficient and called for the implementation of guiding principles in LC&I and Ukraine (while noting that these principles had already been implemented at Baltic Banking).

These audit findings were disseminated to senior managers at Swedbank, including within Baltic Banking and LC&I. On 7 February 2011, GIA included its AML findings in a presentation to the Audit Committee of the Swedbank Board. The presentation noted GIA's "Satisfactory" finding but, among other things, also referred to delays in LC&I's implementation of a "*risk based approach and related monitoring routines in the AML area*," which "*expos[ed] the bank to reputation risk and regulatory penalties*." GIA also presented this finding to the full Swedbank Board that same day. Neither the minutes from the 7 February 2011 Board meeting nor the minutes from the Audit Committee meeting reflect any discussion of this finding. GIA's database reflects that it closed this finding on 17 June 2011.

[34] This GIA audit report reflects that in 2010, the grading schema changed to: Optimized (Governance, risk management and controls are assessed as optimized), Satisfactory (Identified shortfalls are considered minor. No major weaknesses identified), Require Improvement (Identified shortfalls are considered unfavorable and must be dealt with in the near future), and Unsatisfactory (Shortfalls are considered serious and must be dealt with immediately).

Continued Growth in Swedbank Estonia's HRNR Portfolio

In April 2010, the Management Board of Swedbank Estonia reviewed an "*action plan*" for its HRNR business. The presentation of this plan distinguished HRNR customers from other customers by reference to criteria that included: (i) "*No book-keeping and financial reporting requirements*;" (ii) "*Final beneficiaries and owners can[]not be often identified directly*;" (iii) "*Contact person for the bank is representative by the Power of Attorney*;" (iv) "*Majority of clients are doing business in Russia*;" and (v) "*Final beneficiaries are in maj[]or part residents of Russia*." The presentation stated that Swedbank Estonia's HRNR segment, as of December 2009, totaled "*653 clients with active accounts*," which accounted for 4% of Swedbank Estonia's total revenue. Within the HRNR segment, HRC-1 accounted for 13% of the total HRNR revenue and 28% of the total deposits.

Another presentation to Swedbank Estonia's Management Board followed in December 2010. This presentation indicated that the HRNR segment had grown to encompass 900 customers, and that the HRC-1 Group accounted for 26% of the total HRNR revenue and 37% of the total HRNR deposits. The presentation also cited a counterparty bank (Counterparty Bank 1, or "**CPB-1**") as a "*competitor*" and indicated that the HRC-1 Group spreads its "*risks*" across the two banks.

Against this background, Swedbank Estonia continued to open accounts for *Stichting*-owned customers linked to the HRC-1 Group. Some of these accounts were later associated with complex transactions that had no apparent commercial purpose. For example, in September 2011, the primary RM for HRC-1 at Swedbank Estonia submitted a request to the HRCAC for an "*extraordinary decision on opening Swedbank accounts for two companies*." The memoranda accompanying the request stated that the two companies were linked by shareholder trust declarations to one of the Undeclared *Stichtingen*, the beneficiaries of which were five Russian nationals. One of the memoranda stated, however, that "*according to the [RM's] assessment*" those beneficiaries were "*not the actual beneficiaries for this company*," and the "*client has promised to disclose the actual beneficiaries . . . to Swedbank as the below transactions are concluded; and they will provide a new Trust Declaration*." The memorandum referred to two Russian oligarchs as the "*actual beneficiaries*" of the Undeclared *Stichtingen*.

The HRCAC was also advised that the request for these accounts related to a complex $100 million loan transaction (based upon a "*loan agreement*" between one of the companies and a Russian bank), with that sum of money to pass between accounts at Swedbank and CPB-1 "*at least two, probably three times*." The request acknowledged that moving such large sums of money between Swedbank and CPB-1 increased the risk of "*an inquiry by the correspondent bank*," which would require Swedbank Estonia and CPB-1 to "*provide the correspondent bank with information regarding the client's larger and more important companies, which the client really wants to avoid*." In an apparent effort to mitigate this risk, the RM for the HRC-1 Group explained to the HRCAC in the email accompanying the request that the reason for opening both accounts was to "*be able to move the money along the whole chain within Swedbank (i.e. we would receive the money to our client's account and it would be followed by intra-bank payments)*." The RM further noted that "*[t]he 'added value' of opening accounts for these two companies: we would get much better information about the client and we'd control the movement of the money . . . between the accounts of the whole chain of owners.*" The HRCAC accepted the request to open these accounts for the two companies in the HRC-1 Group.

The relevant transaction data reflect that, shortly after these emails and memoranda went to the HRCAC, each of the two companies ("**Company 1**" and "**Company 2**") engaged in a series of circular transactions with other Swedbank Estonia customers in the HRC-1 Group. One circular transfer involved a series of payments, each approximately $100 million, beginning with a $100 million payment on 7 September

2011 from a Russian bank to the Swedbank Estonia account of Company 1. The next day, the same sum was transferred by Company 1 to a second HRC-1 Group customer, which paid approximately $100 million back to Company 1 about two weeks later. A few days after that, Company 1 paid $100 million back to the same Russian bank that originated the payment. Between October and November 2011, essentially the same circular transfer, for about the same amounts and involving the same Swedbank Estonia customers, was enacted again.

Company 2 also made circular transfers in September 2011, involving payments of approximately $200 million each. On 8 September 2011, the first payment of approximately $200 million was sent by a third HRC-1 Group customer to an account of Company 2, where it was immediately transferred to another account of Company 2. The next day, the same amount was returned to the first account and paid to the Swedbank Estonia account of HRC-1. A few days later, HRC-1 sent a similar amount to the account of Company 2, and the next day, Company 2 transferred the payment back to the account of the third Swedbank Estonia customer in the HRC-1 Group. On 14 September 2011, HRC-1 sent $5 million to the account of Company 2, and Company 2 sent a little over $5 million to the third HRC-1 Group customer that same day. Therefore, the transaction data reviewed by the Investigation reflects that the third HRC-1 Group customer sent $203 million to HRC-1, which was sent back less than a week later, with an additional payment of approximately $5 million. All of these payments went through the Swedbank Estonia accounts of Company 2.

The Investigation's review of the relevant transaction data did not find evidence that CPB-1 was involved in these circular transfers by Company 1 and Company 2.

In October 2011, the HRC-1 RM requested additional account openings for HRC-1 Group companies owned through the *Stichting* structure. A memorandum to the HRCAC requesting approval for these accounts again explained that the beneficiaries of the *Stichting* were five natural persons who "*are close associates of the shareholders of. . .[the HRC-1 Group]*" but that while the RM "*asked the client to specify the link between [the] natural persons and . . .[the HRC-1 Group's] shareholders or members of the board*," Swedbank Estonia had received "*no such additional information at the moment*." Similar to prior account openings, the RM asserted that the HRCAC should accept the requests because the HRC-1 Group was a "*TOP client*." The HRCAC accepted this account opening request.

Alongside the profitability rationale, the HRCAC was also told that another benefit of approving these new accounts was that they would provide the bank with better information about the internal structure and flow of funds throughout the HRC-1 Group.

Nevertheless, despite assurances that the true beneficiaries of the *Stichtingen* would be provided once new accounts were opened, the RM continued to advise the HRCAC in 2011 and 2012 that the HRC-1 Group had refused to provide documentation linking the stated beneficiaries of the *Stichtingen* to the true beneficial owners of the HRC-1 Group. After one such briefing in December 2011, the HRCAC agreed to a revised process for opening new accounts for HRC-1 Group entities that employed the *Stichting* structure. The HRCAC instructed the HRC-1 RM to maintain a separate addendum to each HRNR customer memorandum that outlined the actual beneficiaries of the accounts, even if the memorandum itself did not, and to store the addendum together with the HRCAC memorandum in the relevant customer database used by employees to access customer information. The HRCAC noted that this procedure would "*ensur[e] that the Bank will have all the information concerning the client*." As discussed *infra*, however, this instruction was not fully implemented, and such information was often omitted from the relevant customer database.

In April 2012, Swedbank Estonia employees acknowledged that they knew little about the beneficiaries of the two Undeclared *Stichtingen* and their relationship to the two

Russian oligarchs who the employees believed ultimately controlled the customer group. These employees also noted that efforts to obtain further information had been unsuccessful and remained unlikely to succeed in the future. In particular, the RM for the HRC-1 Group explained in a memorandum to the HRCAC that "*[t]he main problem has appeared about how to link the beneficiaries . . . to the two major [Stichtingen] shareholders*," and noted that oral and written attempts to obtain such information since late 2011 had been unsuccessful. The RM explained that, at a recent meeting in Moscow on 1 March 2012, the customer representative had informed the RM that the "*natural persons are relatives and affiliates of the two major shareholders ([the two Russian Oligarchs]) and that these two shareholders have appointed them into those Stichtingen by their own direct order*." Despite the customer's assurance that any information can be issued and certified "*upon the agreement of [the two Russian Oligarchs]*," the RM accepted that this was not an "*attainable*" option for Swedbank Estonia "*because of their high status and the strict hierarchy*" of the HRC-1 Group.

In light of this, the HRC-1 Group RM acknowledged in the memorandum to the HRCAC that there was a risk that Swedbank Estonia might "*theoretically receive an [Estonian] FIU prescription*" if it received a request for information covering the Undeclared *Stichtingen*, because it had insufficient information about the corporate structure or major shareholders of the customer group entities. However, the memorandum urged the HRCAC to accept the proffered beneficial owners in light of the HRC-1 Group's historical "*importance and profitability*" and cautioned that "*[i]n the case of not accepting them, there's quite a substantial risk that the client will open accounts with [other banks] and take their main transactions and deposits to those banks*."

The HRCAC ultimately agreed to conditionally accept a continuation of the relationship with the 60 entities owned by the Undeclared *Stichtingen*, and to allow further accounts to be opened through this ownership structure. The minutes of the HRCAC reflect that the committee understood that Swedbank Estonia would likely never receive complete documentation reflecting the ultimate ownership of HRC-1 Group customers linked to the Undeclared *Stichtingen*. Nevertheless, the HRCAC continued to authorize the opening of new accounts, and requested that the RM continue to follow up with the customer about the deficiencies in beneficial ownership information.

In September 2012, the HRCAC again considered the lack of beneficial ownership information for the Undeclared *Stichtingen*. HRCAC meeting minutes indicate that although Swedbank Estonia knew based on "*conversations*" with HRC-1 Group representatives that the documented beneficial owners were "*relatives*" or "*people close*" to the two Russian oligarchs, "*[o]btaining documents verifying the connection of the beneficial owners and getting their CVs is unlikely*." The committee also noted that, based on the documentation possessed by Swedbank Estonia, it could not "*connect the persons with the management structure of the company or with the main shareholders*." Notwithstanding these deficiencies, the HRCAC again agreed to continue the relationship with the entities owned by the Undeclared *Stichtingen* and to accept future account openings. In an apparent compromise, the HRCAC noted that where it was not possible to obtain specific ownership documentation, other "*direct and indirect measures must be used to understand the company's ownership structure and collect additional information on ultimate beneficiaries . . . for example . . . representatives' signed explanations . . . and the representatives' oral testimony*." The HRCAC also directed that such information be recorded and stored in the relevant customer database.

The prevailing Group policies and directives (which were applicable to all of Swedbank, including the Baltic Subsidiaries) required identification and verification of a customer's identity and beneficial ownership, and mandated that a "*[b]usiness relationship shall not be established"* if CDD could not provide clarity on the relationship. The Investigation revealed that these policies were not followed in connection with Swedbank Estonia's opening of accounts for HRC-1 Group entities.

On 22 October 2012, shortly after the HRCAC allowed the continuation of Swedbank Estonia's relationship with HRC-1 Group entities owned through the Undeclared *Stichtingen*, the EFSA asked Swedbank Estonia a number of questions about customers registered in offshore low-tax jurisdictions. These questions were based on a need to assess Swedbank Estonia's "*activity in implementing . . . due diligence measures*" after a recent increase in the value of deposits by such customers.

Swedbank Estonia responded on 12 November 2012 that the increase in deposits of HRNR customers was mainly attributed to the two largest customer groups in this category, one of which was the HRC-1 Group. The response asserted that larger payments in recent months were linked to a restructuring of the HRC-1 Group's ownership. Swedbank Estonia also stated that it understood the nature of the restructuring, that the relevant documentation was available to Swedbank Estonia, and that it monitored the transactions. However, as outlined above, in 2012 Swedbank Estonia generally did not have a full and complete understanding of the beneficial ownership structure of the HRC-1 Group, nor did it adequately respond to potentially suspicious transactions. While the Swedbank Estonia employees involved in preparing the response to the EFSA—including an AML officer and senior managers who participated in the HRCAC—would have been on notice of these deficiencies, most of those employees were not available to be interviewed as part of the Investigation, and the Investigation has not found any evidence that they intended to deliberately mislead the EFSA.

2010-2012: The HRC-1 Customer Relationship Expands to Sweden

According to Swedbank Estonia's internal records, the HRC-1 Group was the most profitable customer group in Swedbank Estonia's Corporate Banking Division in 2010. By 2011, HRC-1's activity was significant enough to strain credit limits at Swedbank Estonia. For example, in July 2011, HRC-1 sought to increase its "*unsecured overdraft*" limit and "*off-balance [Foreign Exchange] limit*" to levels that exceeded the authority of the Swedbank Estonia Credit Committee, thereby requiring approval from members of Swedbank's Group Credit Committee-Executive (the "**GCC-E**"). The GCC-E approved the requested increase, and approved further credit increases for HRC-1 in August 2011, November 2011 and February 2012.

Following these increases in Swedbank Estonia's credit exposure to HRC-1, RMs at LC&I and Swedbank Estonia proposed to the GCC-E that HRC-1's FX limit and utilization be transferred to LC&I, with other day-to-day banking operations remaining with Swedbank Estonia. According to the former Swedbank Estonia CEO, Swedbank Estonia management supported this transfer because these large FX transactions created excessive risk for Swedbank Estonia. As part of the transfer, an LC&I RM was appointed to handle HRC-1's foreign exchange business, with the Swedbank Estonia RM retaining responsibility over the remainder of HRC-1's business. In October 2012, this arrangement was approved by LC&I and the GCC-E.

Both the GCC-E and the Swedbank Estonia Credit Committee were aware that three Russian businessmen (two of whom were oligarchs) were the main beneficial owners of HRC-1, and that the two oligarchs had "*good relationships with the Kremlin*." For example, the October 2012 credit memorandum to the GCC-E that proposed splitting HRC-1's relationship between LC&I and Swedbank Estonia contained organizational charts that identified the oligarchs' ownership interest, and noted that HRC-1's "*ownership structure is fairly complex with a number of holding companies and off-shore accounts*." With respect to the oligarchs' ties to the Kremlin, the credit memorandum's risk analysis concluded that "*unless they suddenly start financing the opposition parties then the political risk should also be covered as well as possible in Russia*."

In August 2012, shortly before this credit memorandum was issued, an LC&I customer analyst asked the Swedbank Estonia RM for financial information on the 100% holding company of HRC-1, a short description of the UBOs and documentation confirming

ownership. The Swedbank Estonia RM responded with financial records for the holding company, a description of the UBOs, share certificates and a trust declaration. One share certificate connected HRC-1 to the 100% holding company and the other share certificate listed a proxy holder as the owner of 50,000 shares of the 100% holding company. The trust declaration reflected that the proxy holder was holding the 50,000 shares for the benefit of one of the UBOs. As a result, while the Swedbank Estonia customer team disclosed to LC&I the ownership interests of the two Russian oligarchs in HRC-1, their ownership was not confirmed through documentation.

Later, an LC&I employee questioned HRC-1's transparency because HRC-1 had only provided financial statements for its 100% holding company for the previous seven months. The LC&I analyst then asked Swedbank Estonia for four years of financial statements but was told that "*historical financials have not been provided to us.*" The Investigation has not found evidence that LC&I employees sought further information before submitting the October 2012 credit memorandum. While the credit memorandum noted that "*KYC has been performed by Large Corporates in Stockholm and PEP control . . . has been performed and approved by Swedbank Relationship Services*," the KYC information appears to have been, for the most part, copied from documents that had been compiled by Swedbank Estonia. According to an LC&I RM who was interviewed for the Investigation, LC&I did not have dedicated KYC analysts at that time.

Swedbank Estonia Segregated Records for the Most "Confidential" Customers

The number of HRC-1 Group entities that utilized the *Stichting* structure, and the specific *Stichting* associated with each entity, varied over time. For example, in February 2009, Swedbank Estonia had open accounts for approximately 153 HRC-1 Group entities linked to *Stichtingen* (of which approximately 72 were associated with the Undeclared *Stichtingen*). By September 2012, there were approximately 115 such accounts (of which approximately 63 were associated with the Undeclared *Stichtingen*). The Investigation also identified that HRC-1 Group entities were occasionally moved from a Declared *Stichting* to an Undeclared *Stichting*. The objective, as stated in a March 2009 memorandum written by the primary RM for the HRC-1 Group to document a meeting with an HRC-1 Group representative, was to ensure that "*a certain part of the group is connected to persons who do not wish to disclose in any way that they are the companies' beneficiaries*." The RM circulated this memorandum to senior managers at Swedbank Estonia.

Documents relating to the *Stichtingen*, as well as other customer records that were deemed highly confidential, were stored apart from regular customer documentation maintained by Swedbank Estonia. In internal documents (including HRCAC memoranda), Swedbank Estonia personnel sometimes listed the relevant *Stichting* as the UBO (with a cross-reference to trust deeds which detailed the natural persons who were beneficiaries), and sometimes expressly listed the natural persons that were purported to be the UBOs.

Email communications between Swedbank Estonia employees also reflect that the beneficial ownership documentation relating to the five *Stichtingen* was often not uploaded to the relevant customer database, but instead stored offline in a safe or locked drawer, first within the IPB Department and later in the Swedbank Estonia AML Department. Despite the HRCAC's instruction in 2012 that information about the ultimate beneficial ownership of the *Stichtingen* be recorded and saved in the relevant customer database, there remained instances in which this did not occur and beneficial ownership information continued to be stored exclusively in the safe. The Investigation reviewed a sample of HRC-1 Group customer information in the relevant customer database, and did not identify any annexes containing beneficial ownership documentation for the sample customers reviewed. For all sample customers, key documentation or information was either missing or had only been uploaded after

significant delay. To date, the Investigation has identified very few instances where annexes containing beneficial ownership information were prepared by the HRC-1 Group RM, all of which were located outside of the relevant customer database.

The practice of storing beneficial ownership documentation outside the relevant customer database was not limited to the HRC-1 Group or to these specific *Stichting* entities, but extended to other customer documentation that was deemed highly confidential. As early as 2008, employees in the IPB Department and AML Department drafted a process document that stated: "*Top-confidential documents, e.g. documents concerning the owners and beneficialy [sic] owners of the company (Declaration of Trust, Nominee Service Agreement, etc.) . . . are preserved in a locked safe in the IPB Department's room."* The CEO of Swedbank Estonia received this document in July 2008 as part of a package of IPB documentation. During an interview conducted as part of the Investigation, a Swedbank Estonia RM recalled that the practice of storing customer documentation relating to beneficial ownership in a safe was not limited to the HRC-1 Group, but rather was a more common practice.

This practice made it difficult for Swedbank Estonia to review the historical HRC-1 Group relationship. For example, in November 2016, the HRC-1 RM at Swedbank Estonia received an inquiry from an employee of Swedbank Estonia's Legal Department requesting documentation on the ownership structure of an HRC-1 Group entity. The RM forwarded the email to a Swedbank Estonia AML officer, noting that the documentation "*is in your safe,*" and copied the Legal Department employee. Addressing the Legal Department employee directly, the RM wrote, "*you should know that the most confidential [HRC-1 Group] documents were (are) stored*" in the safe.

Again, in November 2016, the HRC-1 RM emailed an AML officer at Swedbank Estonia to document that the RM had taken from "*your department safe*" the file for the HRC-1 Group "*containing the information (the statutes, registry extracts and Trust Declarations) on five [Stichtingen]*." The HRC-1 RM also noted that "*internal audit was mainly interested in the Trust Declarations (Connection to natural person) of the first two foundations*." That same day, a Swedbank Estonia RM emailed the Legal Department employee with information on an HRC-1 Group entity, writing that a trust deed for one of the *Stichtingen* "*is not up in [the relevant customer database] yet*." [35]

Concerns with the practice of storing customer documentation outside of the relevant customer database were raised with the Management Board of Swedbank Estonia in December 2016, when a Legal Department employee presented findings on the verification and accuracy of documentation for HRNR customers. Although the presentation did not specifically refer to the HRC-1 Group or interactions with the HRC-1 Group's RM, it did refer to incorrect and poor customer documentation, including "*limited information about ultimate beneficiaries*" and a "*limited*" view of group customer structures, as well as a finding that "*[c]lient documents are hard to find and they are stored in different locations*." The employee's proposals on this finding included ensuring "*employee compliance with regulations*."

The failure to store certain beneficial ownership documentation in the relevant customer database also appeared to create difficulties for Swedbank Estonia when providing information to regulatory agencies. In an email exchange from February 2017, a Swedbank Estonia AML officer referred to "*another case where the FIU got inaccurate information about a beneficiary (colored red in the list)*." The AML officer noted several entities that are "*probably connected*" to High Risk Customer 3 (discussed further below, and described hereafter as "**HRC-3**") had information in the customer database

[35] The Investigation also identified other instances when critical documentation and information related to this HRC-1 Group entity was either missing from the relevant customer database or had only been uploaded after significant delay. For example, an internal memorandum that identified the two Russian oligarchs as the ultimate beneficiaries of one of the main entities in the HRC-1 Group was drafted in July 2015, but not uploaded until 21 April 2017. Prior to that upload, no documentation existed in the database for this customer that identified the Russian oligarchs as beneficial owners. The structured data field for shareholders in the database appears to have been modified to identify the Russian oligarchs in September 2017, while the beneficial ownership field appears to have been modified to identify the Russian oligarchs only in 2019.

that was not "*correct*," in that it did not link the entities to the UBO of HRC-3. The AML officer then referred to "*some kind of deal*" between the KYC and AML personnel at Swedbank Estonia, where some customers would not have data entered into the customer database *"because they want to retain their anonymity or something*." The AML officer instructed that "*[w]e need to quickly identify these people and enter these corrections in the database*."

When asked about this email exchange during an interview for the Investigation, a Swedbank Estonia KYC manager recalled that there were enhanced concerns regarding the confidentiality of Russian oligarchs, and that documents relating to these customers were stored separately. Clifford Chance reviewed documentation related to a sample of the customers cited in the February 2017 email exchange and confirmed that key documents and information were either missing or had only been uploaded after significant delay. For example, for one HRC-3 customer group (the "**HRC-3 Group**") entity, there was no reference in the customer documents to the Russian oligarch identified as the UBO of HRC-3. Instead, documentation from April 2016 referred to another individual as the beneficial owner.[36]

Swedbank Group's 2008 KYC Directive stated that "*KYC information must have a complete and transparent audit trail, i.e. relevant employees and competent authorities must be able to access the information concerning each client and how it has changed over time with short notice*." A similar record keeping requirement was reflected in the 2010 Swedbank Group AML Policy, which applied to "*the Bank, and all Subsidiaries*," and provided that:

> *customer information must be stored in such a form and is [sic] such a way that it is possible, without difficulties, to. . . access the information and reconstruct important steps in the processing of all business relationships and transactions. . . and. . .establish all corrections and other amendments as well as the content of the information before these corrections and amendments were made.*

The storage of customer documentation outside of regular customer-management systems did not comply with these policies, as the practice did not provide an effective audit trail, nor was it possible for employees to readily access important KYC information about customers.

The HRC-1 Group Refers Other Customers to Swedbank Estonia

Swedbank Estonia's relationship with the HRC-1 Group led to customer referrals. For example, in early December 2011, the primary RM for the HRC-1 Group, along with three other Swedbank employees, attended a meeting in Cyprus at the recommendation of the HRC-1 Group to discuss a potential banking relationship with representatives of HRC-3. The RM later drafted a memorandum recommending that Swedbank Estonia do business with HRC-3. The memorandum explained that a Swedbank Estonia customer that was previously owned by HRC-1 had been sold to HRC-3, and that the HRC-3 Group was interested in continuing and enlarging the pre-existing relationship with Swedbank Estonia by opening 20 to 40 accounts for "*the group's non-resident companies' transactions and deposits.*" The memorandum divided these non-resident companies into four categories: "*Holding Companies*," "*Settlement Companies*," "*Wallet [Companies]*," and "*Investment Firms*."

This memorandum identified a Russian individual, often referred to in media reports as an oligarch, as the main beneficial owner of HRC-3, but explained that for some HRC-3 Group companies "*the declared beneficiary . . . is [a] close relative [of the oligarch]*." The exact relationship between the Russian oligarch and the "*close relative*" remained

[36] For a second HRC-3 Group customer, while documents from 2011 and 2012 identified the Russian oligarch as the beneficial owner, subsequent documentation from 2013 and 2016 identified a different person, and then an entity, as the beneficial owner. For a third HRC-3 Group customer, there is no reference in the customer documentation to the Russian oligarch. Instead, the documentation reflects that a different natural person and an entity were the beneficial owners. For each of these aforementioned three customers, the structured data field for beneficial owners in the customer database appears to have been modified to identify the Russian oligarch only in May 2019.

unclear, so the HRCAC directed the RM to substantiate the connection. Before that information was obtained, however, Swedbank Estonia opened the first of many accounts associated with the HRC-3 Group, for a Cyprus-domiciled company whose UBO was the Russian oligarch. The account for this Cyprus company had a daily limit of €50 million. Swedbank Estonia also opened a personal account for the Russian oligarch in April 2011, but it was closed in May 2013, and the Investigation has not identified any activity over the life of this account.

Contemporaneous communications reflect that the RM never obtained written evidence from HRC-3 establishing the connection between the close relative and the oligarch. An email on 31 August 2012 between HRCAC participants reflects that the RM had stated in a memorandum that the declared beneficiary, the close relative, had no connections with the Cyprus-domiciled HRC-3 Group company. Nevertheless, the email exchange indicates that the RM had proposed marking as complete the requirement to establish the nature of the connection between the declared beneficiary and the oligarch since Swedbank Estonia had listed the oligarch as a beneficiary of the company. The minutes of the HRCAC meeting on 29 August 2012 indicate that the requirement to "*determine the association*" between the declared beneficiary and the oligarch was "*fulfilled*." The minutes state, however, that the RM will "*search public sources for additional information*" about the declared beneficiary and ask for a *curriculum vitae* ("**CV**"). In April 2013, the RM sent the declared beneficiary's CV to a member of the HRCAC and asked that the requirement be marked as complete. In May 2013, the HRCAC member sent the RM a log detailing the status of HRCAC tasks which marked the requirement as complete. There is no further mention of the declared beneficiary in subsequent HRCAC meeting minutes.

According to a subsequent investigation report by GSI Estonia, Swedbank Estonia ultimately opened accounts for about 70 entities associated with the HRC-3 Group, including a number of companies described in the KYC files as "*wallet*" companies for HRC-3.

These wallet companies were used for complex circular transactions that often called for exceptions to the daily account limits. For example, on 18 November 2015, the RM for HRC-3 requested management approval via email for raising the daily teleservice limits, explaining that the customer's "*money will make a bigger circle today and will presumably exit to Russia as dividends already tomorrow*." The request described a series of six separate transactions between various HRC-3-affiliated entities. These transactions were to occur the same day, and the value of the entire series of linked transactions was approximately $111 million. The relevant manager approved the temporary increase in the daily limits that same day. There is no indication that the RM for HRC-3 or the relevant manager performed adequate due diligence, as required by then-applicable Group policy and directives, for these transactions. For example, the 2010 Swedbank Directive on AML and CTF (adopted by Swedbank Estonia on 21 December 2010) required due diligence for occasional transactions "*for an amount equivalent to EUR 15 000 or more or when several transactions linked together represents in total EUR 15 000 or more.*"

The use of so-called "*wallet*" companies was not limited to HRC-3. Swedbank Estonia's KYC files for the HRC-1 Group characterize at least 23 companies as "wallets." The purpose of the wallet companies was described variously as holding funds generated from trading, collecting payments from business ventures, or redistributing funds to holding companies.

Continuation of Relationship with HRC-2

Meanwhile, Swedbank Lithuania's management board agreed to continue, and expand, its relationship with the HRC-2 Group. In January 2012, the HRC-2 RM prepared a memorandum to a member of the Swedbank Lithuania management board seeking

approval to continue the relationship with the HRC-2 Group and to open several new accounts for affiliated entities. The appendix to the memorandum indicated that a Ukrainian oligarch owned a controlling stake in the HRC-2 Group, through direct or indirect controlling interests in other affiliates. The memorandum outlined that Swedbank Lithuania had taken steps to mitigate money laundering risk, primarily by meeting with representatives of the customer group in person and by obtaining underlying documentation supporting payment activity. The memorandum also noted that "*[a]s the Bank makes a lot of net income from the client, I suggest allowing to continue working with this client*." A member of the Swedbank Lithuania management board approved the continuation of the customer relationship and the opening of new accounts.

In February 2012, three additional companies related to HRC-2 opened accounts with Swedbank Lithuania, despite not providing full KYC documentation. Notwithstanding the January 2012 memorandum that identified the Ukrainian oligarch's interest in the HRC-2 Group, none of the KYC documents provided to Swedbank Lithuania for these three new companies identified the oligarch as a UBO.

In June 2012, GIA issued an audit report examining governance, risk management and internal controls for money laundering prevention in the Baltic Subsidiaries. The audit attributed the grade "*Requires Improvement*" (described in the report as "*[i]dentified shortfalls are considered unfavourable and must be dealt with in the near future*") to a number of areas, and found that Swedbank Lithuania failed to control the accuracy and completeness of customer information entered into its customer database. Recipients of the audit reports included senior managers of the Baltic Subsidiaries and Baltic Banking.

A parallel audit issued by GIA in July 2012 assessed AML controls within Swedbank. Recipients of the audit report included a senior Group Risk manager and senior managers of Swedbank Business Areas. Overall, GIA concluded that the area "*Require[d] Improvement*," identifying 15 areas requiring improvement, including five "*Unsatisfactory*" findings in AML routines, sanctions list screening, the identification of non-domestic PEPs among Swedbank's institutional customers, and AML training. Other findings addressed deficiencies in governance structure, updates to AML scenarios, transaction monitoring and the handling of alerts. For example, the audit found that "*Group AML has not set a clear enough AML governance structure, including the governance of Subsidiaries. As a result, there is a risk that required AML duties might not be fulfilled in accordance with internal and external regulations which might lead to [SFSA] sanctions.*" GIA's database of historical findings shows that GIA closed this item on 9 January 2013. The report also found that LC&I "*does not have a clear risk based [KYC] procedure*," and as a result "*KYC might be performed incorrectly or not at all in violation of internal or external regulations*." GIA also found that LC&I management had not ensured "*that all relevant employees have done the mandatory AML training.*" GIA closed these items on 28 December 2012 (LC&I's KYC procedures) and on 7 January 2013 (LC&I's AML training). GIA closed all findings identified in this audit by 24 March 2013.

In its Q2 2012 report to the Audit Committee of the Board, GIA listed these audits among its activities for the year. With respect to its audit of "Group AML and Swedbank in Sweden," the report noted that LC&I "*does not have a detailed risk based [KYC] procedure*," that "*KYC roles and responsibilities are not set*" and that "*management has not followed up that all relevant employees have done the mandatory AML training*." The report concluded that, as a result, Swedbank risked a "*violation of internal and external regulations*." Minutes from the Audit Committee's meeting on 17 July 2012 do not reflect any discussion of or reaction to these findings.

For each year of the Investigation Period, Swedbank had an external auditor that prepared and submitted reports to the Audit Committee of the Board. While AML

compliance was not a central issue of these reports, the reports did note AML deficiencies. For example, for the Audit Committee's meeting on 17 July 2012, the external auditor submitted a presentation to the Audit Committee that observed "*Group AML needs to strengthen its governance structure*."

Minutes from a meeting of the Swedbank Board that same day also noted that "*Group AML needs to strengthen its governance structure*," including such "*[i]dentified shortfalls*" as "*outdated instructions as well as job descriptions and compliance plans, unclear AML responsibilities and authority in relation to the Swedish subsidiaries and week [sic] follow-up procedures*." The minutes noted that "*[a]s a result there is a risk that required AML duties might not be fulfilled in accordance with internal and external regulations*." The minutes do not reflect that any action items were discussed to address this risk, and they note simply that "*[a]lthough there are some critical findings by Internal Audit, management takes the matters seriously and deals with the matters with the sense of urgency that is called for.*"

Also in July 2012, Swedbank Lithuania tightened its policy on HRNR customers. Swedbank Lithuania issued a directive not to on-board new customers from high risk offshore jurisdictions, and that exceptions to this policy generally had to be approved by the CEO. If a pre-existing HRNR customer group sought to open additional accounts for companies within the same group, the approval of a senior manager in the Compliance function was deemed sufficient.

In January 2013, a Swedbank Lithuania compliance officer rejected a request to open a new account for an affiliate of the HRC-2 Group. The compliance officer noted that the "*companies from this group do not conduct business in Lithuania, the payments are not made to business partners in Lithuania, hence there is no way to ascertain the economic legitimacy of the transactions carried out*." Nevertheless, the other entities in the HRC-2 Group remained customers of Swedbank Lithuania until March 2014 and the account of one entity remained active until June 2016.

High Risk Customers at Swedbank Latvia

During 2011 through 2012, Swedbank Latvia developed relationships with high risk customer groups linked to offshore jurisdictions. In March 2011, Swedbank Latvia on-boarded a Latvian joint venture (High Risk Customer 5 or "**HRC-5**"). Swedbank Latvia assessed that the minority shareholder in HRC-5 was controlled by three Latvian PEPs; however, its ownership structure was obscured because the PEPs' family members, "*or other related persons*," were listed as beneficial owners.

A Credit Memo prepared by Swedbank Latvia two months after HRC-5's on-boarding acknowledged that the company's operations included "*high political risk*" and that the "*Russian business specifics . . . cannot be fully assessed*," however, the memorandum nevertheless recommended that Swedbank approve a €30 million investment loan for a local development project because it was "*economically reasoned[,] and planned cash flow from realized project suggests sufficient debt servicing ability*." The Credit Memo acknowledged that the 49% shareholder in HRC-5 was "*[i]ndirectly . . . related to local political heavy weights*." The memorandum also noted that another Russian oligarch was the UBO of the Cypriot company that was the majority shareholder of HRC-5. The Credit Memo mentioned that Swedbank Latvia was "*one of [the] main cash management banks*" for the group of companies associated with the 49% shareholder, and that growing the business relationship would position Swedbank Latvia to become "*the home bank (including the financing)*" for this customer group, as well as potentially attracting more business from HRC-5's 51% shareholder. In July 2011, Swedbank approved Swedbank Latvia making the requested loan to HRC-5.

In November 2012, as a result of business contacts made in connection with on-boarding HRC-5, Swedbank Latvia on-boarded High Risk Customer 6 ("**HRC-6**"), a Latvian company that was in the same corporate group as HRC-5. In April 2013, HRC-6 decided that it wanted to open accounts with Swedbank in Sweden. The HRC-6 RM discussed the issue with senior management and decided that if HRC-6 intended to transfer a significant portion of its turnover to Sweden, it would need an account with LC&I.

During the account opening process, Group Compliance questioned why HRC-6 needed an account in Sweden if HRC-6 did not conduct business in Sweden. Swedbank Latvia explained that HRC-6 was invoicing its customers primarily in USD and EUR, and wanted to extend its relationships with European banks beyond the Baltics to diversify its banking relationships and support its customer base. Swedbank Latvia also noted that several of HRC-6's largest counterparties were in Scandinavian countries.

Following this exchange, Group Compliance informed Swedbank Latvia that "[*t]he setup process of [HRC-6] has been moved to a branch office [in Sweden]*." After receiving KYC forms from Swedbank Latvia, the Swedish branch opened HRC-6's account in late May 2013. By January 2014, the Swedish branch raised concerns with Group Compliance about HRC-6 and sought to end the customer relationship. The Swedish branch was concerned that "*they can't rely on the KYC information they have been given*" since HRC-6 was using its local branch account for a high volume of transactions from non-Scandinavian countries such as Russia, which was contrary to the stated business purpose of the accounts. For example, according to contemporaneous communications, during February 2014, the Swedish branch processed Swedish kr 107 million worth of transactions for HRC-6, involving payments from the United States that originated in Brazil and were ultimately transferred to Russia. Group Compliance and Compliance personnel in Baltic Banking also identified risks inherent in HRC-6's complex ownership structure. HRC-6's UBO was a Russian oligarch and numerous offshore entities existed within the larger corporate group. Other entities affiliated with HRC-6 were also indirectly linked to: an OFAC-sanctioned Russian oligarch connected to Russian government officials and to several money laundering scandals; various state-owned Russian enterprises, including some sanctioned by OFAC; and, through payment activity, to a company connected to a former Ukrainian President and to various public criminal prosecutions.

As a result of the Swedish branch's concerns, Swedbank Latvia reached an agreement with HRC-6 to move most of its turnover back to Swedbank Latvia. The customer, however, wanted to retain an additional account in Sweden. To facilitate this, an RM from Swedbank Latvia again asked LC&I to open an account for the customer. However, LC&I indicated that it would need to do its own KYC checks on HRC-6, and that it did not at that time have the capacity to do so. The question of whether to allow HRC-6 to retain an account in Sweden was escalated and, on 3 February 2014, senior managers from Baltic Banking and Swedish Banking (with input from the Swedbank CCO) ultimately decided that the Swedish branch account could remain open if the account was used only for Nordic transactions and not *"for bouncing the money through Sweden*." The Swedish branch agreed to continue the relationship, but with only Nordic transactions generally permitted after the end of February 2014 (non-Nordic transactions would be handled on a case-by-case basis). LC&I also investigated HRC-6 and subsequently reported it to the Swedish FIU.

Neither Swedbank nor Swedbank Latvia appears to have addressed the underlying money laundering risk associated with the payments, and they instead shifted the exposure from one Swedbank entity to another. Moreover, while LC&I indicated it would need to conduct its own KYC checks on HRC-6, the customer was nevertheless permitted to maintain a Swedish Banking account at a branch in Sweden without any further KYC analysis. As discussed further below, HRC-6 remained a customer

at Swedbank Latvia and Swedish Banking for over two more years before Swedbank deemed the risk to be unacceptable.

2. 2013 – 2015: The Magnitsky Allegations Highlight Deficiencies in AML Controls

In early 2013, Estonian media reports linked Swedbank Estonia to the Magnitsky scheme,[37] citing allegations in a complaint filed with the Estonian Public Prosecutor and the Estonian FIU in July 2012 by lawyers for HCM. The complaint alleged that Swedbank Estonia and CPB-1 had facilitated money laundering in connection with the Magnitsky scheme in 2008 and 2009. With respect to Swedbank, the complaint identified two payments in 2008 that a Swedbank Estonia customer had received from a corporate entity reportedly linked to the Magnitsky scheme.

In 2013, Baltic Banking's Compliance function and Swedbank Estonia reviewed these transactions and circulated a joint report summarizing their findings to, among others, Swedbank's then-CCO, Swedbank's then-General Counsel (later appointed CCO in April 2016), and other senior executives. The report explained that there was no failure of due diligence by Swedbank Estonia because the implicated customer lacked the typical characteristics of a "*shell company or money mule*." The report noted that the Estonian FIU had indicated that a criminal investigation was unlikely, and although not referenced by this report, a January 2013 press statement by the Estonian Public Prosecutor announced that the prosecutor's office had declined to open a criminal case following a joint investigation with the Estonian FIU regarding the allegations in the HCM complaint. The report concluded that there were no immediate significant legal or compliance risks for Swedbank arising from the Magnitsky scheme, but there was reputational risk from the negative media coverage.

These issues were reported to the then-General Counsel at Swedbank and a senior executive in the Swedbank Estonia Legal Department for their legal assessment. On 1 March 2013, the senior executive in Swedbank Estonia's Legal Department emailed senior managers in GIA and Baltic Banking's Risk function, among others, and concluded that there was "*at the moment no legal risk identified*." The Investigation has not identified any evidence that a substantive legal analysis was performed in support of this assertion. In the same email, the senior executive in Swedbank Estonia's Legal Department observed that although the Estonian Public Prosecutor and the FIU had not initiated any criminal investigation, since the case had not been closed, Swedbank Estonia would keep a "*close eye*" on any developments. The senior executive in Swedbank Estonia's Legal Department escalated the HCM complaint to Swedbank's then-General Counsel for analysis.

Swedbank Estonia conducted further analysis shortly thereafter, reviewing customers' transactions from 2008 through 2010 with the customers of CPB-1's predecessor bank that were linked to the Magnitsky scheme, which was identified in the HCM complaint. This analysis revealed that six then-current and five former Swedbank Estonia customers had transacted with six such counterparties at CPB-1. One of these then-current customers, and all of the former customers, were part of Swedbank Estonia's HRNR portfolio.

The Swedbank Estonia AML officer who performed this analysis emailed it to other employees, including the AML officer's own manager and a senior manager in Baltic Banking's Risk function. The AML officer observed that, if the identified customers were indeed involved in the fund flows related to the Magnitsky scheme, "*then it would be very bad for this business because it is hard to believe, that they were involved unknowingly and this leaves only two other options which come to my mind – many high risk non-residents are established for money laundering only and are used by many different persons (they provide a service)*" or perhaps their owners "*do not hesitate to make some additional money doing questionable business (brokering payments)*." The

[37] *See supra* note 12.

AML officer's manager later emailed the AML officer separately to advise against giving Baltic Banking management the impression that "*we had major money laundering going on.*"

Relationship Between LC&I and Baltic Banking Regarding High Risk Financial Institutions

Also in January 2013, the LC&I KYC Committee assigned a risk rating of "*not acceptable*" to a financial institution, Counterparty Bank 2 ("**CPB-2**"), due to media reports linking CPB-2 to both the Magnitsky scheme and a suspicious transaction in Ukraine. While the LC&I KYC Committee was unable to corroborate these reports, it concluded that the relationship was unacceptable and should not continue.

In early March 2013 an LC&I RM communicated to a senior manager within Baltic Banking that the LC&I KYC Committee had decided not to approve CPB-2 as a "*suitable counterparty to Swedbank based on comprehensive reporting in both national and international media about the bank's alleged money laundering transactions*." The Baltic Banking senior manager requested to see the material that provided the basis for the Committee's decision in order to "*understand exactly why [they] made the decision and what [they] did in order to verify the information*." The LC&I RM provided the relevant media articles supporting the Committee's decision.

On 19 March 2013, employees from both Swedbank Latvia and LC&I met to develop an off-boarding plan for CPB-2. At an April 2013 meeting with CPB-2, the LC&I RM conveyed the off-boarding decision to CPB-2, at which point CPB-2 indicated that terminating the banking relationship would be catastrophic for CPB-2 and could trigger the collapse of its business. Senior managers in Baltic Banking and Swedbank Latvia advised the RM that Swedbank could not be responsible for CPB-2's demise and, accordingly, proposed that Swedbank terminate some aspects of the relationship, but continue to provide foreign exchange services for CPB-2. The RM expressed discomfort with this proposal, noting that foreign exchange services would potentially facilitate the very conduct that had given rise to the KYC Committee's AML concerns.

A senior LC&I employee then reached out to Group Compliance asking for its opinion on the CPB-2 relationship. Group Compliance responded that they could provide advice on the issue but that it was ultimately a business decision that should be made by the Business Area managers of LC&I and Baltic Banking. At the request of a senior LC&I employee, the LC&I RM prepared a detailed summary of issues relating to the CPB-2 relationship for Group Compliance, noting that the LC&I KYC Committee assessed that Swedbank would be in breach of 3MLD if it continued the relationship with the customer. Group Compliance responded that "*[f]rom a strict AML perspective, we cannot recommend that Swedbank have a business relationship with [CPB-2].*" Group Compliance further stated that it is not necessary to "*prove that money laundering has occurred*" to off-board a customer. Group Compliance concluded that because they recommended off-boarding, the decision should be escalated to senior management at LC&I and Baltic Banking.

By mid-June 2014, with the issue still unresolved, the LC&I RM was becoming frustrated with the lack of progress. When a colleague asked whether CPB-2's expiring foreign exchange limits would be extended or terminated, the RM replied that they believed the limits would be extended *"[i]ndefinitely it seems,"* and observed: *"I am no longer interested . . . Swedbank has decided that Money Laundering is ok and the rest of us will just have to live with that."* On 30 June 2014, however, the RM confirmed that while foreign exchange services would be extended for CPB-2 until the end of November 2014, the RM had "*been instructed to start unwinding the business relationship by the end of September*." On 14 July 2014, a senior manager from Baltic Banking's Risk function confirmed that off-boarding should proceed, noting that "*[b]ased on our discussion that we have had, we confirm that it is ok to go ahead with the*

terminating of the business relationship with [the customer] in an appropriate way, thus giving the customer reasonable time to manage the situation." By 1 December 2014, Swedbank had ceased providing foreign exchange services for the customer, after receiving assurances that this decision would not immediately compromise CPB-2's business.

Due to the extended debate surrounding the off-boarding of CPB-2, the foreign exchange activity that had raised concerns was allowed to continue for over a year while the issue awaited consensus between LC&I and Baltic Banking.

In April 2013, LC&I and Swedbank Latvia personnel also debated whether to de-risk another financial institution, Counterparty Bank 3 ("**CPB-3**"). CPB-3 never held a correspondent banking relationship with Swedbank, but Swedbank Latvia maintained a Relationship Management Application ("**RMA**") arrangement with CPB-3, which is a messaging system on the SWIFT network that allows financial institutions to communicate with one another.[38] Nonetheless, Swedbank treated CPB-3 as a "customer" while the RMA arrangement was in place and performed KYC on CPB-3.

LC&I had given CPB-3 a risk rating of "*not accepted*" since 2009. Given the unacceptable risk rating, LC&I questioned whether Swedbank Latvia should terminate the RMA arrangement with CPB-3. LC&I ultimately determined that Swedbank was "*not at liberty to refuse the exchange of RMAs with*" CPB-3 given regulatory implications because CPB-3 was "*an important player in the domestic payments system. . . and act[ed] under the same supervisory authority as Swedbank AS in Latvia*."

In July 2014, in parallel with terminating the relationship with CPB-2, LC&I again asked Swedbank Latvia to terminate its relationship with CPB-3, noting that this would make the "*risk of violating KYC-bans . . . significantly lower*." The decision was again deferred, with an LC&I employee noting that terminating the relationship with CPB-3 required a *"careful analysis.*"

By 2015, CPB-3 continued to get an unacceptable risk rating from LC&I, yet received a "low" risk rating from Swedbank Latvia. The tension between the two different risk ratings for CPB-3 resurfaced in summer 2015. Internal communications reveal that an LC&I RM explained to a Swedbank Latvia employee that Swedbank and its Baltic Subsidiaries maintained separate KYC and risk-rating analyses for customers, even when the customers themselves overlapped, citing CPB-3 as an example. The Swedbank Latvia employee complained to the LC&I RM and another colleague about the risk of inconsistent approaches to CDD and risk assessments:

> *The whole Compliance principle in the Group, as far as I understand, is that we are 'One Group – One Policy'. You cannot have one Group member consider a certain bank low risk, whilst another decides it is low [sic] risk. How could that possibly make sense and how will our foreign partners react, especially those in the US, when we say that Swedbank has no common policy as regards risk assessment of foreign relationships?*

The employee further urged that the inconsistency "*really must be resolved before our friendly neighborhood FSA comes-a-knocking. Not only is there confusion, there is chaos!"* The same employee noted in a subsequent exchange with the same recipients that *"[i]t is ludicrous to create separate KYC functions or banks in each Swedbank entity. It is not required by local law and is not required by the FSA (they would have said so if anyone would have bothered to ask them).*"

Another LC&I employee disagreed, and observed that while having different customer risk ratings applied by different parts of Swedbank was not ideal, the "*AML Manual*

[39] *See* Wolfsberg Guidance on SWIFT Relationship Management Application (RMA) Due Diligence, at 1 (2016), https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/7.%20SWIFT-RMA-Due-Diligence.pdf) ("The RMA is a messaging capability enabling members of the SWIFT network to exchange messages over the network.").

is clear that our Baltic colleagues are requested by the local FSA to conduct their own KYC and independently come to a conclusion if they want to run a relationship or not." Another LC&I employee elaborated that Swedbank (*i.e.*, LC&I) and the Baltic subsidiaries "*are separate legal entities and the relevant FSAs require a risk assessment of the customers by the relevant entity*."

Nonetheless, the inconsistent application of customer risk ratings by Swedbank and its Baltic Subsidiaries continued. In early 2016, Swedbank Latvia continued to apply a risk rating of "*low*" to CPB-3, while LC&I applied an "*unacceptable*" rating, despite reports linking CPB-3 to money laundering. By April 2016, Swedbank Latvia appears to have changed CPB-3's risk rating to "*medium*," but the RMA arrangement continued.

In March 2017, LC&I continued to list CPB-3 as "*unacceptable risk*" while Latvia listed it as *"high risk*" and Estonia and Lithuania listed it as "*medium risk.*" This discrepancy persisted throughout 2017 and was brought to the attention of personnel in Group Compliance evaluating Swedbank's exposure to high-risk financial institutions in the Baltics. Group Compliance conferred with LC&I, which stated that its impression was that Latvian regulatory requirements mandated that Swedbank Latvia maintain an RMA with other financial institutions such as CPB-3 meaning the RMA relationship could not be easily terminated. In December 2017, Group Compliance pushed LC&I to reconsider its relationships with high-risk financial institutions like CPB-3. Group Compliance concluded that the money laundering risk relating to financial institutions such as CPB-3 was "enormous" and that proper EDD should be performed, and the issue was flagged to the CCO. The RMA arrangement was not closed, however, until a few months later, when US authorities issued notice of their intent to designate CPB-3 as an institution of primary money laundering concern (*see infra* at 126).

As of 2008, Swedbank's policy encouraged all Group entities "*as far as technically and legally possible, [to] apply a consolidated KYC risk management process in order to consolidate information for customers with business in different parts of the Group*," and to implement "*one KYC- and take-on process . . . to avoid double KYC-processes for one and the same customer with business in several Entities/countries and enhance knowledge sharing*." However, as these examples indicate, the Group did not implement a process to ensure a common risk assessment and rating approach to common customers or to resolve disagreements within the Group over appropriate risk mitigation measures.

Internal Deliberations Within the Baltic Subsidiaries Regarding Risks of the HRNR Segment

In March 2013, Swedbank Estonia's Corporate Banking Department conducted a review of Swedbank Estonia's non-resident customer segment for the prior year. The results of this review were compiled into a presentation that was shared with Swedbank Estonia's Management Board. The presentation noted that the HRC-1 Group was the HRNR segment's top customer during 2012. The presentation suggested that Swedbank Estonia had complete transparency regarding the beneficial ownership of its customers: "*We follow existing procedures and criteria for new clients . . . [u]nderstandable business model . . . [n]o AML issues . . . [t]ransparent Beneficial Owners and source of capital.*" During a recent interview as part of the Investigation, the former Swedbank Estonia CEO explained that, consistent with what the CEO characterized as then-prevailing standards, Swedbank Estonia operated under the assumption that, so long as it knew or believed it knew the true beneficial owner of a customer, there was no need to ensure that there was supporting documentation in the relevant KYC systems. Yet, Swedbank's then-applicable policies and procedures (at least since 2010) included record-keeping obligations which mandated that "*[c]ustomer information must be stored in such a form and in such a way that it is possible, without difficulties, to . . . access the information and reconstruct important steps in the processing of all Business relationships and* transactions. . ."

Around this time, a senior manager at Swedbank Lithuania sought to develop a non-resident customer portfolio at Swedbank Lithuania. A March 2013 presentation circulated by this manager to several colleagues across the Baltic Subsidiaries identified a business opportunity in the non-resident sector, noting that the Baltic countries are "*attractive jurisdiction[s] to post Soviet territories,*" and that Lithuania was a particularly favorable market at the time "*due to lack of competition*" following the exit of two major competitor banks from the non-resident market segment. In light of this opportunity, Swedbank Lithuania proposed establishing a "*Baltic non-resident competence center*" that would implement best-practice AML procedures and satisfy all necessary KYC requirements. To develop the proposal, the senior manager at Swedbank Lithuania met with members of the former private banking team from a liquidating financial institution (Counterparty Bank 4, or "**CPB-4**") to explore hiring them. When interviewed for the Investigation, the senior manager at Swedbank Lithuania recalled ultimately deciding based on these meetings that this team would be unsuitable. A senior manager in Baltic Banking's Risk and Compliance function also told Clifford Chance during an interview that the senior manager and others objected to developing a non-resident business in Lithuania due to AML concerns and that, by June 2013, the proposal was abandoned.

Meanwhile, Baltic Banking attempted to create a policy to govern the risk appetite of the Baltic Banking non-resident business. In April 2013, a senior Risk and Compliance manager in Baltic Banking prepared a draft Framework Regulation for the Baltic Non-Resident business (the "**Draft NR Regulation**"), which proposed criteria for the acceptance of non-resident customers. This Risk and Compliance manager circulated the Draft NR Regulation to the then Head of Baltic Banking (who later became Swedbank CEO in April 2016). The compliance manager also shared the Draft NR Regulation with several employees of the Baltic Subsidiaries. The "*Risk Appetite and Risk Tolerance*" section of the Draft NR Regulation proposed, among other things, that "*to minimize Reputation Risk Swedbank [sic] limits High Risk Non-resident business to counterparts with a sizable and relevant connection to our Home Markets*," specifically customers with:

- asset management services;
- general financing services;
- shareholders of resident operating companies; or
- substantial investments in real estate.

The employees of the Baltic Subsidiaries who received the Draft NR Regulation worried about the proposed constraints on the non-resident business. For example, one AML officer at Swedbank Estonia advised the Risk and Compliance manager "*that risk appetite will change, because in current wording it seems that it will deny us lot of good business, including our TOP client [HRC-1] or part of it.*"

In response to these concerns, the compliance manager told the AML officer that the Draft NR Regulation was only a proposal and the ultimate decision rested with the business, but emphasized that "*there is a strong case for limiting the business like this . . . if anything happens there is no way we can explain to shareholders why we did this if it is a business outside Swedbank's profile. We are a low risk profile retail bank with clearly defined business and home markets in the eyes of shareholders*."

On 25 April 2013, the Baltic Banking management team considered the Draft NR Regulation. The minutes of the meeting reflect that the proposed regulation would be re-drafted to "*incorporate limits and tolerance proposed by [the] business*." In preparation for a follow-up meeting in June 2013, a senior manager at Swedbank Estonia inquired about the proposed Draft NR Regulation, noting the proposal was "*quite vague*," and the Baltic "*Board and CEOs and [Baltic Banking] opinion is that*

we should continue with serving the [non-resident] segment." A senior manager at Swedbank Latvia responded that the Baltic Banking Board had determined that the Baltic Subsidiaries should continue serving customer relationships that are at least seven years old, but should "*continue to be EXCLUSIVE, or picky*" in establishing relationships with non-resident customers. This senior manager also noted that there was a clear message from the Baltic Banking Board that "*we do not strive to grow our business substantially in this [non-resident] segment and we continue to live by very high AML and Compliance standards*" and that this would likely involve the Baltic Subsidiaries enhancing their internal processes and adopting a common governance structure for non-resident business.

In June 2013, responsibility for the Draft NR Regulation project was shifted to a different manager within the Baltic Banking business "*to align non-resident banking[,] set risk appetite and harmonize procedures*," but the Investigation has not identified any subsequent progress on the proposal. In March 2014, communications amongst employees within the Baltic Subsidiaries reflect confusion over whether the policy had ever been adopted. An employee ultimately determined in April 2014 that the Draft NR Regulation had never been implemented because it was not "*published as [an] official Baltic document.*"

The failure to finalize the Draft NR Regulation highlights the absence of a clearly articulated policy for managing the risk associated with the growth of the non-resident business in the Baltic Subsidiaries. The Draft NR Regulation would have involved the formulation of a risk appetite and could have led the Baltic Subsidiaries to systematically address whether its existing non-resident customer relationships in the Baltics, as well as prospective ones, were consistent with that risk appetite. However, after employees of the Baltic Subsidiaries recognized that existing non-resident customers (such as HRC-1) would be deemed unacceptable by the Draft NR Regulation, it was never finalized or implemented.

Further Growth of the HRNR Portfolio

In 2013, Swedbank Estonia continued to open accounts for entities it referred to as "wallet" companies. In memoranda distributed to the HRCAC regarding new account openings for approximately a dozen companies in 2013 and early 2014, the HRC-1 Group RM described the function of these "wallet" customers in similar terms.

In the memorandum relating to one new corporate customer, the HRC-1 Group RM noted that the company would be used for "*managing intra-group cash flows, issuing loans/repayment of loans to other companies of the group*" and distributing " *the group's profit among the group's companies*." The memorandum explained that "*the longer route of the money separates the source of the money from other companies of the [HRC-1 Group] and therefore minimizes the risk of inquiries and possible affiliation for the client*." The memorandum further noted that "*this is a recent replacement*" of the HRC-1 Group companies "*that takes place every 1.5 . . .[to] 2 years, not new volume of business. The companies' activity profiles shall not change, only the companies themselves do (recently founded new BVI companies)*." Swedbank Estonia subsequently opened accounts for these "wallet" companies.

These Swedbank Estonia employees and managers, including members of the HRCAC, apparently did not recognize, or did not raise any concern, that the proffered purpose of these "wallet" companies – to minimize the "*risk of inquiries*" and "*affiliation for the client*" – more closely resembled the practice of layering (the use, among other things, of multiple companies and corporate levels to conceal ownership), instead of legitimate intra-group cash management services.[39] The Investigation has not identified

[39] According to the Organisation for Economic Co-operation and Development ("OECD"), layering is one stage in the money laundering process: the goal of layering is "the concealment of the criminal origin of proceeds. Money can be transferred and split frequently between bank accounts, countries, individuals and/or corporations, thus distancing it from its criminal origin." OECD (2019), Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors, at 18, OECD, Paris, www.oecd.org/tax/crime/money-laundering-and-terrorist-financing-awareness-handbook-for-tax-examiners-and-tax-auditors.pdf

any evidence that the relevant Swedbank Estonia employees, including members of the HRCAC, took steps to obtain further information from the HRC-1 Group about the intended use of these "wallet" companies, or to confirm the propriety of their business role, before opening these accounts.

Some of these "wallet" companies also transacted with customers of Swedbank Lithuania. According to internal correspondence, between April and June 2012, an HRC-1 Group company incorporated in the British Virgin Islands made a series of loan payments, totaling approximately €477,000, to a customer at Swedbank Lithuania. In May 2013, an AML officer at Swedbank Estonia questioned the payments, since the underlying loan agreement did not specify any interest rate or loan purpose. This AML officer noted that the customer sending the payments was a "*wallet of the group*" and asked the HRC-1 Group RM how the customer was connected to the counterparty and the reason for the payments. The RM responded that the HRC-1 Group would not share this information. While expressing concern about the customer's reticence, the AML officer decided not to "*keep poking for now*" given that the transaction was "*rather small,*" and the AML officer did not "*have any certain problem with this counterparty*."

At least two other customers of Swedbank Lithuania also had transactions with HRC-1 Group customers. In 2016, the HRC-1 Group RM at Swedbank Estonia requested copies of agreements between the HRC-1 Group and three Swedbank Lithuania customer entities (including the recipient of the loan payments). In response, the HRC-1 Group informed the RM that one of the Russian oligarchs that was a UBO of HRC-1 had a "*service agreement*" with the three Swedbank Lithuania customers, which provided vehicle rental and travel services. Payments to the three Swedbank Lithuania customers under the service contract, however, were not made directly by the Russian oligarch. Instead, funds were sent to the Lithuanian customers by an HRC-1 Group company, pursuant to loan agreements between the oligarch and the HRC-1 Group company (which were also provided to the RM). One of these loan agreements was for €11 million. Based on a review of the contemporaneous communications, there is no indication that the RM asked any further questions about this arrangement, or that a legitimate business purpose for the structure was advanced or identified.

Swedbank Estonia noted the AML risk arising from the use of "wallet" companies in late-November 2013, when its AML officer circulated an inspection report discussing risks relating to the HRNR portfolio. The inspection report recommended obtaining additional information about the HRC-1 Group's activities, observing that the HRC-1 Group customers also used CPB-1 "*for risk mitigation*" but that it was unclear why the "*wallet*" companies made payments to "*high risk clients of small Latvian banks, not with bigger and more reliable banks (they always have said, that they value good infrastructure and reliability/good credit rating)*." This report was circulated to the CCO of Swedbank and other senior managers in the Compliance function. The Investigation has not identified any evidence that the then-CCO elevated this issue to the Board. The Investigation has not identified any evidence that the then-CCO responded to the AML officer, provided any comment on this inspection report, or elevated this issue to the Board. When interviewed for the Investigation, the then-CCO acknowledged that, in retrospect, AML compliance in the Baltic Subsidiaries should have been more of a priority at the time, and simply had not been a focal point for the then-CCO until the latter-half of 2015.

This inspection report also indicated that Swedbank Estonia's HRNR segment had been inspected by GIA earlier in 2013 "*without any negative findings*." In June 2013, GIA had issued an audit report assessing AML processes in the Baltic Subsidiaries. The audit recognized that the Baltic Subsidiaries had improved AML processes, but noted that certain areas "*Require[d] Improvements."* Among other things, the Baltic Subsidiaries had failed to consistently identify foreign PEPs among existing customers. GIA recognized that this failure could result in foreign PEPs being missed and not treated according to "*required customer due diligence and monitoring procedures*

which may lead to potential regulatory fines." GIA's historical database of findings shows that GIA closed this finding on 30 December 2014, following technical delays in the implementation of PEP-screening software. As it had in a 2012 audit, GIA again found deficiencies in AML training at the Baltic Subsidiaries, noting that "*insufficiently trained employees may violate the AML requirements due to low risk awareness*." According to GIA's records, GIA closed the findings for Swedbank Estonia on 23 October 2013, for Swedbank Lithuania on 12 December 2013 and for Swedbank Latvia on 21 January 2014.

GIA presented its Q2 2013 audit findings in a GIA report to the Audit Committee of the Swedbank Board, which the Audit Committee discussed on 15 July 2013. The report referred to the June 2013 AML audit but did not explain any specific findings, and the meeting minutes do not reflect any discussion of the findings. The meeting minutes did note that the Audit Committee had discussed AML issues, noting "*ALM [sic] issues in the light of the S-FSA's more harsh interpretation of some issues, leading to Nordea being fined earlier this year*," which "*underscored the necessity to allocate resources in general and IT resources in particular in order for development of a system that supports the documentation of the screening of the ultimate beneficial owner of companies*." The minutes stated that "*any delays in implementing enhanced routines for AML, expect [sic] due to extraordinary circumstances, will not be accepted*."

Crisis in Ukraine and Scrutiny of High Risk Customers

In late February 2014, the Ukrainian President was deposed, and days later, Russia began to annex Crimea. The crisis in Ukraine prompted customer reviews in Swedbank.

Swedbank Lithuania conducted a review in February 2014 and identified concerns with HRC-2's "*increased level of AML ris[k]*" in light of connections between its beneficial owner and the deposed Ukrainian President. In March 2014, Swedbank Lithuania off-boarded HRC-2 and its affiliates. By April 2014, the accounts for all but one of the HRC-2 Group companies were closed, and the final company was off-boarded in June 2016.

Much later, in early 2019, Swedbank conducted an internal review of potentially suspicious transactions involving HRC-2, after Ukrainian media alleged that that various Ukrainian oligarchs and politicians had funneled over $65 million to companies in Cyprus to pay for political consulting work in support of the former Ukrainian President. This internal review found that, from 2010 through 2013, HRC-2 had been involved in a number of transactions with entities linked to these payments. In addition to HRC-2 (a Swedbank Lithuania customer), the review indicated that two Swedbank Latvia customers and five Swedbank Estonia customers had transacted with counterparties implicated in this scheme.

The SFSA Identifies Deficiencies in AML and KYC at LC&I

In June 2014, the SFSA closed an investigation into Swedbank without sanction, provided that Swedbank perform the remedial activities set forth in its approved action plan. The SFSA had commenced the investigation in early 2013 to examine "*compliance with local AML regulations*" within Private Banking, LC&I, Swedish Banking and Swedbank's Norway Branch. Although the investigation was initially focused on PEPs and correspondent banking activities, the SFSA expanded the scope to include private and corporate clients.

Among other things, the SFSA investigation identified that LC&I and Swedish Banking had low risk awareness and did not sufficiently conduct risk assessments of customers; LC&I and Swedish Banking had many customers without proper KYC, missing KYC documentation and analysis, and too many manual routines in the KYC process; and LC&I and Swedish Banking had insufficient IT support, and had not screened beneficial owners against sanctions lists on a daily basis.

During interviews for the Investigation, LC&I employees recalled that before the SFSA investigation, LC&I was not sufficiently focused on KYC, and that the KYC it performed was of poor quality. Prior to 2014, the LC&I KYC form was a simple single-page Excel spreadsheet filled out by RMs who often maintained relevant KYC documents on their individual hard drives rather than in Swedbank's central systems.

In October 2014, LC&I implemented several changes aimed at addressing the issues identified by the SFSA, including improving the KYC function. Notably, the new policy implemented a new KYC form that scaled the required detail according to the risk class of the customer, *i.e.*, the riskier the customer, the more customer information was needed. In addition, resources were provided for KYC analysts to assist RMs with archiving the necessary KYC documentation, screening beneficial owners against sanctions/PEP lists at the time of on-boarding and drafting KYC analyses for riskier customers. Despite these improvements, there was cultural resistance within LC&I to the changes in the KYC process. When interviewed for the Investigation, one LC&I RM recalled that many LC&I RMs treated the SFSA's findings as an implicit criticism of their customer knowledge, and felt that management did not trust RMs to know their customers.

In furtherance of the action plan submitted to the SFSA, Swedbank set up a "*Swedish-wide AML Programme*" responsible for "*the closing of all gaps related to SFSA findings*." Similar to the parallel LC&I AML project, the Swedish-wide AML Program made several improvements to the AML and KYC function within Swedish Banking, which were reported to the Board in 2014 and 2015. For example, a Q3 2014 Group Compliance Report provided to the Audit Committee and the Board found that although "*some of the activities are running close to their deadlines, mostly due to lack of competent resources in first line which in turn has delayed the start-up of some of the actions*," the Program was running "*without any significant deviations*." This Group Compliance Report also noted challenges in establishing "*effective governance of the [AML] Program*." The minutes from the Audit Committee meeting indicate that this governance issue was discussed, but the minutes from the Board meeting only indicate that "*the AML Program is running according to plan, and deliveries are done according to the set time plan*."

In addition, LC&I began to address its "*backlog*" of KYC. The backlog consisted of customers for which KYC had never been done or was incomplete. The backlog dated back several years—at least to January 2012. For example, a Q1 2014 AML Compliance Report stated that within LC&I's financial institutions customers, the number of customers with overdue KYC were: 653 in June 2013, 394 in December 2013, and 448 in March 2014. The report further indicated that (a) LC&I's financial institutions team had reallocated resources to the issue but the reallocated resources "*have not been able to catch up with the work*," and (b) LC&I's KYC process for large corporates was delayed due to "*limited resources*." The Investigation did not identify evidence that these issues were presented to the Board.

Instead, in April 2014, the Audit Committee and the Board received the Q1 2014 Group Compliance Report that stated "*[m]any parts of the business, including the Swedish regions and LC&I, are working actively to close the KYC gaps that exist*." This report also advised that Group Compliance monitored KYC for "*high-risk corporate customers*" and had concluded that the "*quality is still poor*." The minutes from the Audit Committee meeting on 23 April 2014 reflect that the "*KYC review*" was discussed, but the minutes do not provide detail on the discussion. Although the Q1 2014 Group Compliance Report was discussed at the Board meeting that same day, there is no indication that the KYC backlog was discussed. The minutes only reflect that the Board "*stressed the importance of prioritizing the activity plan with regards to AML and that the [Board] should be updated regularly on the matter*."

Subsequent AML Compliance Reports in 2014 stated that it was not possible to give precise statistics on the backlog because of data retention issues, but noted that the

problem persisted. A Q3 2014 AML Compliance Report also noted that the backlog for large corporates was "*more severe . . . [and] increasing*." In general, the AML Compliance Reports were circulated within Group Compliance, and to the CCO. The Investigation has not identified any evidence that these AML Compliance Reports, or the details about the ongoing KYC backlog from these reports, were provided to the Board or its committees.

In November 2014, an LC&I Compliance officer estimated to senior management in LC&I that there were approximately 5,000 customers with overdue KYC. This compliance officer also stated that only one employee was dedicated to reducing the backlog and that it would take that employee over three years to complete the task if other resources were not provided.

Later, the Board and Audit Committee received an update on the AML Program for their 19 October 2015 meeting, including that "*LC&I's plan is that the [KYC] backlog will be closed by year end*." Despite this projection, the minutes of a 1 February 2016 Audit Committee meeting reflect that the KYC backlog had not been closed. In particular, the CCO told the Audit Committee that performing KYC on existing customers is "*ongoing, but . . . time consuming*." At the Board meeting on the same day, the CCO stated that "*[o]f Swedbank's 4.2 million customers in Sweden, 3.2 million now has [sic] a satisfactory KYC. Only 694 customers are 'red'*" and are being off-boarded or the business relationship restricted.

In 2014, LC&I's efforts to remediate the other deficiencies identified by the SFSA encountered other challenges. For example, a Q3 2014 AML Compliance Report noted that LC&I was still performing manual sanction screening of beneficial owners. This was despite Swedbank's adoption in February 2014 of a policy on payment screening which required all payments be screened against EU and OFAC sanctions lists. The Q3 AML 2014 Compliance Report noted that screening was only done at the time of on-boarding and periodically thereafter, which was "*a clear breach of external regulations*." The report also noted that the issue of sanctions screening of beneficial owners was "*reported as closed*" to the SFSA even though the identification of beneficial owners in the system was still not complete. Finally, the report found that LC&I's internal instructions to not identify beneficial owners for low-risk customers was also a "*breach [of] external regulations*." This report was sent to the CCO, but the Investigation has not found any evidence that it was provided to the Board or any of its committees. The minutes of the Board and Board committee meetings at the time reflect no discussion of the issue.

A report issued in February 2015 by Group Compliance outlined LC&I's work to address the SFSA findings and related issues. Regarding the SFSA's findings, Group Compliance found that LC&I was non-compliant with the requirement to implement "*geographical risk*" in its customer risk assessments. It also found that, although not explicitly mentioned by the SFSA, LC&I was not compliant with EU and SFSA sanctions-related regulations. The report explained that under applicable regulations, any entity owned 50% or more by a sanctioned entity is itself considered sanctioned, and therefore all beneficial owners need to be identified to comply with sanctions regulations. As such, the report found that sanctions regulations "*precede*" AML legislation that did not require beneficial owner screening for simplified CDD. According to the report, however, "*LC&I have declared that they are of a different opinion and thus have no intention of making any adjustments*." This report was circulated to the CCO, but the Investigation has not found any evidence that it was provided to the Board or any of its committees. The Q4 2014 Group Compliance Report that was provided to the Board and Audit Committee did not mention these issues.

Russian Tax Reform Leads to a Restructuring of the HRC-1 Group

Throughout 2014, Russian authorities took steps to restrict capital outflows from the country. In March 2014, the Russian Ministry of Finance proposed a "*de-offshorization*" law, which the Russian Duma passed in November 2014. In general, this legislation required Russian tax residents to notify the Russian tax authorities of any existing direct or indirect participation in foreign entities by 1 April 2015, and made them liable for tax over undistributed profits deemed made by a foreign company, trust, or other structure controlled by a Russian tax resident. This development affected the UBOs of the HRC-1 Group.

In October 2014, a KYC analyst for LC&I assessed that HRC-1 required EDD due to a high risk of money laundering. The analyst observed that the two main UBOs were Russian oligarchs, one of whom was a PEP (with links to an OFAC SDN). This KYC analyst described the situation as "*remarkable*" due to adverse media reports linking the PEP to organized crime and sanctioned parties and entities, and recommended acceptance as "*high risk*" only if continuous transaction screening was implemented. Otherwise the analyst's recommendation would be "*unacceptable*." The resulting KYC form with an appendix memorializing this analysis and decision was dated 28 October 2014, and was received and signed by the LC&I RM for HRC-1 and two senior managers in LC&I. It was also circulated in late-October 2014 to senior managers and AML officers in LC&I, in preparation for a discussion regarding the customer at the next DMC.

In late-December 2014, HRC-1 disclosed that it would restructure its ownership due to changes in Russian tax laws. On 30 December 2014, HRC-1 informed the Swedbank Estonia RM for the HRC-1 Group via email that "*the shareholder of the company changed*," and that a BVI-registered entity would now own 100% of HRC-1. In an internal exchange that same day, the Swedbank Estonia RM for the HRC-1 Group explained to the LC&I RM that, based on prior discussions with HRC-1 representatives, the RM learned that HRC-1's "*main concern*" was the prior declared owner's nominal 100% ownership, which would trigger the new legislation in Russia and require the owner to "*declare the income from [HRC-1] and pay income tax*." Later that day, the Swedbank Estonia RM for the HRC-1 Group followed up with the LC&I RM to explain that HRC-1 had provided a flow chart of the restructuring plan that would reduce the former 100% owner's interest to a less than 10% ownership in the BVI entity, but give this person the right to receive 90% of dividends, while installing a new natural person owner who would own over 90% the BVI entity with the right to receive only 10% of the dividends. In the ensuing exchange, the two RMs noted that the sudden structural changes likely breached an agreement with Swedbank requiring HRC-1 to seek the bank's "*prior approval before changing the ultimate owners*," but decided to move forward with gaining the requisite approval from the relevant committees because "*this has been a long-term client and very profitable for us*."

The following day, on 31 December 2014, an attorney for HRC-1 emailed the two RMs to provide further information on the restructuring. The email attached a letter from a "*director*" for HRC-1 stating that the restructuring was due to "*changes in the legislation of the Russian Federation*," and that, as a result of the changes, "*the current UBO [i.e. the Russian businessman] will reduce [the current UBO's] ultimate shareholding from 100% to 9.9%, thus complying with the new Russian tax legislation, but will have shares of such a type that provides him opportunity to receive 90% of the amount of dividends.*"

In January 2015, following notification from HRC-1 of the restructuring, the RMs from Swedbank Estonia and LC&I exchanged emails about a newsletter from an international accounting firm summarizing and commenting on the changes to the Russia tax code. The LC&I RM wondered about a statement in the newsletter pointing out that:

[a] Russian tax resident will be deemed to be controlling a foreign entity/ structure if . . . [t]he Russian residents exercises, or has the power to exercise, a decisive influence on decisions regarding the distribution of profits of the foreign/company structure, regardless of the legal basis for such control.

Reacting to this statement, the Swedbank Estonia RM responded to the LC&I RM as follows:

[I]f I was a tax officer, I would not be satisfied with their setup (10% of shares giving 90% of profits). There have been probably discussions with lawyer and corporate advisors that led to that scheme. As a conclusion, it theoretically leaves some opportunity to tax the current ultimate owner, but this is job for legal and financial advisors. As a bank, I would leave it 'as is' for now.

On 2 March 2015, HRC-1 provided additional documentation to the Swedbank Estonia RM. The cover email, sent by an attorney for HRC-1, included the following statement (which the Swedbank Estonia RM translated from Russian for the benefit of the LC&I RM):

Inter alia, on the recommendations of other credit organizations, we have prepared the conclusion of independent lawyers, whose services are used by [the current UBO], confirming that the transaction has no tax consequences. We hope that this will help us in the passing of compliance.

The email attached a one-page memorandum, purporting to be from a Russian "Law bureau" that went by the same name as the Russian law firm originally proffered by the HRC-1 Group as ultimate beneficiary in 2006, and also the name of one of the *Stichtingen* that the HRC-1 Group used as a beneficial owner. The memorandum addressed the "*Sale and Purchase of Shares*" in connection with the HRC-1 restructuring but did not address whether the restructuring was permissible tax avoidance under Russian law. In its entirety, the memorandum stated (with minor modifications in brackets):

We, [the Russian Law bureau], hereby confirm that our firm is a consulting company that provides professional advisory services. Further we confirm that we advised [the current UBO] in relation to the transaction on the sale and purchase of shares in [HRC-1] dated December 15, 2014 (the "Transaction").

Among other issues within Transaction advice we analyzed tax matters in relation to [the current UBO] and we hereby confirm that no tax consequences arise for [the current UBO] in connection with the Transaction.

This confirmation is being given only in connection with Transaction without any guarantee or liability on the part of our firm or its representatives. It is based solely on the circumstances as known to us today. In keeping with standard practice, we refrain from making any statement whatsoever with respect to the future, nor is it possible for us to issue any update or correction of the information contained herein based on facts or circumstances of which we subsequently become aware.

On 3 March 2015, the legal memorandum—renamed "*Legal Opinion UBO Change*"—was included in the final package of KYC documentation compiled by the Swedbank Estonia RM for review by the LC&I RM. A document contained in the package noted that:

In November 2014 [the President of Russia] enforced Amendments to the Tax Code of Russia, under which the Russian residents who have control (or direct of ownership) in Controlled Foreign Companies, must declare this ownership to the Russian Tax Board, no later than 31 March 2014. The threshold (%

of ownership) that will cause tax consequence (Russian income tax will be withheld from undistributed profit) will gradually decrease from 50% (in 2015) to 10% (in 2017). Therefore Client wishes to avoid tax consequences to [the current UBO], and in December 2014 the company decided to change its shareholder.

While this change of ownership was being considered by LC&I and Swedbank Estonia, the LC&I RM for HRC-1 and the Swedbank Estonia RM for HRC-1 Group discussed concerns that, in addition to the previously declared owner of HRC-1, the renewed KYC process would have to identify the two Russian oligarchs who were the primary ultimate beneficiaries of the HRC-1 Group. The Swedbank Estonia RM explained to the LC&I RM that the two Russian oligarchs had been included as UBOs in prior documentation because of their receipt of dividends and their ultimate controlling interest, as evidenced by movements of funds among related accounts in Swedbank Estonia. Even though these factors had not changed, both RMs agreed that the information "*regarding ownership chart, PEP, etc.*" not visible in "*official docs*" would be omitted from future KYC analyses.

After this exchange, the resulting Credit Committee applications and subsequent LC&I KYC analysis in 2015 for HRC-1 did not identify the two Russian oligarchs as beneficial owners of HRC-1, but did note a "*close*" relationship between HRC-1 and one of the oligarchs.

In January 2017, the LC&I RM for HRC-1 circulated a memorandum to LC&I senior managers that reviewed the history of the HRC-1 relationship, and noted that LC&I performed a KYC analysis in March 2015 due to HRC-1's restructuring, and that the DMC approved the change in ownership with the continued risk class of "*High*." The memorandum referred to documentation that HRC-1 had provided in 2014 to support its change in ownership, and maintained that *"[w]hile it was fully transparent and also made clear to the bank that the change in UBO was made for tax reasons, we did at the time not realize or suspect that there was a risk for (illegal) tax evasion.*"

GIA Continues to Note Deficiencies in AML and Sanctions Controls in the Baltic Subsidiaries

In the second quarter of 2015, GIA performed several audits of AML and sanctions controls in the Baltic Subsidiaries that noted areas requiring "*Major Improvement*."[40] For example, a GIA audit report issued on 10 April 2015 noted the imposition of Russia-related sanctions arising out of the Ukrainian crisis. While GIA found that the allocation of responsibilities for sanctions management between the business units and compliance was clear and the screening of customers and international payments was regularly performed, the Baltic Subsidiaries received an "*Unsatisfactory*" finding with respect to monitoring the quality of their sanctions screening data, specifically that the screening systems did not always include complete and accurate data about entities and individuals subject to sanctions. The audit found that this deficiency placed the Baltic Subsidiaries at "*an increased risk of violati[ng] international sanctions*," given the "*loss of relations with correspondent banks [and] inquiries from the authorities and reputation damage*."

GIA summarized the findings of its April 2015 audit on sanctions controls at the Baltic Subsidiaries in its Q1 2015 reports both to the Board and the Audit Committee. The Q1 2015 reports noted that the Baltic Subsidiaries "*nee[d] to establish and implement systematic monitoring of data quality in the bank's systems used to be screen the customers and international payments*," and that "*[i]dentified gaps in sanction data quality, without taking a timely corrective action, could lead to sanctions breaches, loss of relations with correspondent banks, inquiries from the authorities and reputational damage*."

[40] In 2015, the GIA audit grading schema changed to: Satisfactory (Risks are managed effectively. An individual action may be required), Minor Improvement Required (Risks are mostly managed effectively. Some actions are required), Major Improvement Required (Some risks are not managed effectively. Prompt action is required), Unsatisfactory (Risks are not managed effectively. Urgent action is required).

Minutes from the 27 April 2015 Audit Committee meeting in which GIA presented its Q1 2015 report do not reflect any discussion of findings related to sanctions. Minutes from the Board meeting that same day also do not reflect any discussion of the audit findings.

According to GIA's database, GIA closed its "*Unsatisfactory*" finding related to monitoring the quality of sanctions screening data on 29 December 2015. It closed the remaining findings from the audit by June 2016.

Another GIA audit report issued on 30 June 2015 concluded that AML controls and transaction monitoring in the Baltic Subsidiaries required "*Major Improvement*." As with a prior finding from 2013, that GIA only closed in late 2014, GIA again found deficiencies in identifying PEPs among existing customers. At Swedbank Estonia, GIA found insufficient monitoring and documentation of transactions by HRNR and private banking customers. At Swedbank Latvia, GIA found: insufficient follow-up by compliance personnel to ensure complete KYC; no controls around the classification of customers as high-risk in the relevant customer database (that was used both for AML monitoring and reports to the FCMC); and no controls around the transfer of blocked funds from accounts that were closed for insufficient KYC. At Swedbank Lithuania, GIA found insufficient documentation demonstrating the handling of potentially suspicious transactions.

GIA summarized the findings of the audit in its Q2 2015 reports to the Board and the Audit Committee, specifically that "*Baltic Banking Compliance should sufficiently document monitoring activities and results for adequate evidence and transparency and should timely escalate to appropriate level management monitoring process related challenges as well as continuously identified gaps in KYC business processes*." Minutes from the 15 July 2015 Audit Committee meeting in which GIA presented its Q2 2015 report reflect only brief reference to the "*area Anti Money Laundering*" and no discussion of or reaction to the specific findings. Minutes from the Board meeting that same day also do not reflect any discussion of the audit findings.

Based on a review of GIA's historical database of findings, GIA reported that it closed its findings with respect to PEP screening across the Baltic Subsidiaries on 4 December 2015. With respect to Swedbank Estonia, GIA closed its finding on HRNR transactions on 7 December 2015 and closed its finding on private banking customers on 30 November 2015. With respect to Swedbank Latvia, GIA closed its finding on insufficient KYC on 31 March 2017, its finding on high-risk classification in the customer database on 5 January 2016 and its finding on blocked funds on 25 March 2017. GIA closed its finding with respect to Swedbank Lithuania's handling of potentially suspicious transactions on 18 August 2015.

During this period, Swedbank began to establish sanctions-focused policies and supporting materials, and to revisit and update most of these materials annually. Swedbank's Policy on Financial Sanctions, which established a common standard within the Group for compliance with financial sanctions, was first adopted on 23 June 2015 by the Board and updated annually through 25 May 2018. The 2015 policy required "*the Bank and all Subsidiaries*" to comply with EU and US financial sanctions and *"[w]here relevant and with due regard to local regulation*" to conduct "*systematic screening of international payments and customer databases (including beneficial owners)*." Prior to the issuance of these policies, financial sanctions were covered as part of Swedbank's general AML policies and directives, which from at least 2008 included a prohibition on "*engag[ing] in business relationships"* with persons listed on *"applicable national or international sanctions lists*" or "*applicable lists from national financial supervisory authorities or similar.*" A 2010 Group AML Directive also referred to assessments on the "*scrutiny of transactions*" being based on screening against applicable sanctions lists, and lists provided by financial supervisory authorities.

While Swedbank implemented an automated payments screening system (ProScan) in 2009, use of the system was not implemented across Swedbank and the Baltic Subsidiaries uniformly. For example, ProScan was not implemented in the Baltic Subsidiaries until 2017. A GIA employee recalled in an interview conducted as part of the Investigation that before ProScan, the Baltic Subsidiaries relied on a manual solution that involved the use of an Excel spreadsheet and the non-straight-through-processing (also known as "non-**STP**") system for sanctions screening, which the employee characterized as primitive, because it predominantly relied on manual input into the Excel and would not automatically download updates to the OFAC list.

Migration of HRNR Customers from CPB-1

In 2015, CPB-1 closed its non-resident customer portfolio after an internal audit identified deficiencies in AML controls. During this time, Swedbank Estonia pursued opportunities to grow the HRNR customer portfolio by migrating former customers of CPB-1. In April 2015, a Swedbank Estonia manager prepared a presentation for the Management Board of Swedbank Estonia about the development of the HRNR customer portfolio. The presentation noted that due to another financial institution's decision to close its non-resident business, and the reduced interest of CPB-1 in this segment, *"a lot of clients are interested in opening an account with Swedbank. Although we reject most of them (business profile is not transparent enough and/or volumes are too small), we still consider a number of new prospects as attractive and potentially profitable counterparties*."

In June 2015, contemporaneous communications between Swedbank Estonia RMs indicate that CPB-1 employees proposed referring non-resident customers to Swedbank Estonia. In addition, some CPB-1 customers approached Swedbank Estonia directly to open accounts. CPB-1 customers related to the HRC-1 Group were affected by the off-boarding at CPB-1, which disrupted cash flow within the HRC-1 Group organization. As a result, the Swedbank Estonia RM for the HRC-1 Group received account opening requests from an HRC-1 Group representative for these former CPB-1 customers. Starting in July 2015, Swedbank Estonia began opening new accounts for companies related to the HRC-1 Group that formerly banked at CPB-1. For three of these companies, the HRCAC approved the account openings even though it was aware that it was "*hard to obtain*" documentation verifying the ultimate beneficial ownership, and that an offshore jurisdiction (BVI) was used in order "*not to show their links with Russian structures*." By August 2016, Swedbank Estonia had opened accounts for at least 27 former CPB-1 corporate customers related to the HRC-1 Group. Accounts for at least another nine former CPB-1 customers unrelated to the HRC-1 Group also were opened.

However, not all account opening requests from former CPB-1 customers were approved by Swedbank Estonia. An internal presentation drafted by a Swedbank Estonia employee to the Management Board of Swedbank Estonia noted that the bank "*accepted less than 10% of the applicants because most of the clients level of business transparency weren't up to our standards*."

Some of these former-CPB-1 customers accepted by Swedbank Estonia during this period were referred by a corporate services provider linked to the Panama Papers leak.[41] Based on contemporaneous communications, two Swedbank Estonia RMs, including the HRC-1 Group RM, appear to have had a close relationship with this corporate services provider. In one exchange, the HRC-1 Group RM told a colleague that the RM's contact at the corporate services provider would keep the "*pool of trashy clients*" at CPB-1 away from Swedbank Estonia. In another exchange, one of these employees remarked that the corporate services provider could easily provide customer documentation, noting: "*[t]hey certainly can make the docs. No questions asked!*"

[41] *See infra* at 92, The Panama Papers Leak Leads to Acceleration of HRNR De-Risking.

3. 2016: The Panama Papers are Released and Swedbank Begins Efforts to De-Risk

Swedbank Estonia Seeks to Limit Exposure to HRNR Customers

In 2016, Swedbank Estonia took more active steps to manage risk related to the HRNR portfolio by beginning to off-board some of its high risk customers. This initiative was motivated, at least in part, by exposure to PEP-risk from the HRC-3 Group, and included managing the deposit and transaction volume thresholds of the HRNR customer segment at Swedbank Estonia given the recent influx of customers from CPB-1.

In a memorandum dated 11 January 2016, the RM for the HRC-3 Group (who was also the RM for the HRC-1 Group) described a proposed exit strategy for the customer relationship. The memorandum noted that Swedbank Estonia's AML department was urging for this relationship to be severed because HRC-3's "*main . . . beneficiary*" was then a senior government official. The 11 January 2016 memorandum also stated that, with the exception of two HRC-3 Group companies, the public connection between the main beneficiary and the other HRC-3 Group companies was "*not that easily visible/ traceable*," and indicated that "*Corporate understands AML's position, but is requesting a longer exit period for this client group (until 31.12.2016)*." Swedbank Estonia proceeded to close the accounts for the HRC-3 Group companies during the course of 2016.

On 14 March 2016, the Swedbank Estonia Management Board received an update indicating that the size of Swedbank Estonia's HRNR deposits was close to exceeding the mandated threshold of 10% of overall customer deposits, which had previously been set in 2014 by the Swedbank Estonia Management Board. The minutes of this meeting reflect that the Swedbank Estonia Management Board was informed that "*[t]hough internally set limits have so far been followed, then taking into account the overall developments of the business sector in both Estonia and abroad, it was stressed that the volume of the named business sector should be reduced and the current checking and monitoring procedures need to be reviewed.*" Following this update, the Management Board noted that it expected a proposal regarding additional management and monitoring of the risks associated with the HRNR business to be presented at its next meeting on 25 April 2016.

At the same time, a correspondent bank raised concerns with Swedbank Estonia with respect to a "*possible increase*" of the volume of the offshore payments "*by clients moving away from [CPB-1].*" In March 2016, Swedbank Estonia employees met with representatives of the correspondent bank, who were concerned that CPB-1's former customers would try to establish new relationships with other Latvian or Estonian banks. Internal email communications reveal that Swedbank Estonia employees represented to the correspondent bank that, unlike CPB-1, Swedbank Estonia had accepted, "*after extensive background checks*," only a "*limited amount of clients who have [a] very clear relationship with Estonia,*" and that it did not "*accept clients brought to us by some middle-men*."

In fact, as discussed above, several Swedbank Estonia RMs were aware that Swedbank Estonia had accepted some former customers of CPB-1 referred by a corporate services provider. Moreover, several Swedbank Estonia employees had, since at least 2007 and as late as 2009, collaborated with the same corporate services provider (and others) to offer account opening packages for customers that included "*ready-made*," or "*shelf*" companies in low tax jurisdictions. However, the Investigation has not identified evidence that the specific Swedbank Estonia employees who met with the correspondent bank were aware of these practices.

A New CEO for Swedbank and a New AML Program for the Baltic Subsidiaries

On 9 February 2016, Swedbank's CEO stepped down, and the then-Head of Swedish Banking was appointed acting CEO. The then-Head of Swedish Banking was

confirmed as CEO on 22 April 2016. Before becoming CEO, this senior executive had also served as Head of Baltic Banking from 2011 through 2014. When interviewed for the Investigation, this senior executive recalled setting risk tolerance limits while serving as Head of Baltic Banking. During the interview, this senior executive also opined that Swedbank's understanding of risk appetite was becoming more sophisticated in 2016.

During this same period, Group Compliance increased its scrutiny of AML risk in the Baltic Subsidiaries. On 1 March 2016, in advance of a meeting in Estonia, Swedbank's CCO circulated a memorandum titled "*Management of AML Risks in BA Baltic Banking*" to other senior managers in Baltic Banking and LC&I. The memorandum reported that Group Compliance had conducted a gap analysis of AML processes and risk management in the Baltic Subsidiaries that revealed deficiencies requiring prompt handling, and that "*the challenges are highest in Latvia.*" The memorandum identified five gaps in order of importance:

1. Risk Assessment Control on Country Level: Risk assessments had not been carried out by Swedbank's Baltic Subsidiaries, and therefore Group Compliance recommended that an AML program be established so that assessments could be documented in each country on an annual basis.
2. Screening of Payments: The system for screening payments was inadequate, and therefore Group Compliance recommended implementing ProScan to ensure proper screening.
3. Monitoring of Transactions: The Baltic Subsidiaries used a manual transaction-monitoring method. Group Compliance recommended implementation of Nice Actimize, an automated system for transaction monitoring for potentially suspicious activity.
4. Governance and Organisational Setup: Group Compliance noted insufficient separation between first- and second-line functions in the Baltic Subsidiaries, and therefore recommended increased delineation of responsibilities and enhanced training.
5. KYC: Lastly, Group Compliance noted that differences in types of KYC documentation made it difficult to consistently obtain adequate information. The report recommended standardization of KYC forms and implementation of a process for updating KYC documentation.

The memorandum recommended that Baltic Banking management initiate an AML Program to coordinate these efforts across all the Baltic Subsidiaries. The memorandum also noted that the proposed Baltic AML Program should be similar to the Swedish Banking/LC&I AML programs that had been implemented under the action plan agreed with the SFSA in 2014 (*see supra* at 82-84).

On 7 March 2016, members of Baltic Banking management (including a senior manager who received the CCO's memorandum on 1 March 2016) met with the European Central Bank ("**ECB**") in Estonia. Baltic Banking senior management presented a Baltic Banking business plan for 2016 through 2018 that touched on many different topics. Although the CCO's memorandum was not referred to or discussed with the ECB, the Baltic Banking business plan anticipated, with respect to AML compliance, the establishment of "*strong and efficient risk management in the first line of defense (including AML procedures, KYC) to avoid violation of sanctions and reputational risk relating to client activities.*" During the meeting, the ECB asked what was motivating Swedbank to focus on AML issues, and was told that the Baltic Banking business had *"politically exposed persons and non residen[t] clients"* that required monitoring in light of "*more and more extensive*" US and EU regulatory requirements, including "*a combination of particular Russian names [on the] sanction list*," internal policy on US

sanctions, the Foreign Account Tax Compliance Act (FATCA), and other EU directives. The minutes of the meeting reflect that when the ECB asked whether these were issues affecting Swedbank Group, the Baltic Banking senior manager responded that "*the Baltic countries*" were more affected by these issues when it came to correspondent banking relationships, and that it has become a "*competitive advantage*" to be compliant "*in this area.*" The minutes indicate that the meeting also covered numerous other matters unrelated to AML risk or compliance.

In mid-March 2016, shortly after the meeting with the ECB, Baltic Banking management agreed to establish the AML Program for the Baltic Subsidiaries, and in April 2016 Group Compliance, LC&I and Baltic Banking worked to implement the Program. On 21 March 2016, the CCO emailed the memorandum titled "*Management of AML Risks in BA Baltic Banking*" to several managers in LC&I, explaining: "*We have done an overall gap analysis of [Baltic Banking] with respect to AML and determined that they need to initiate an AML program equivalent to what we have in Sweden. . .[t]he report covers the entire business area [of] BA [Baltic Banking], not just Latvia, but of the three countries, the situation in Latvia is the worst from an AML perspective.*"

A steering committee for the Baltic AML Program was established later in 2016. When interviewed for the Investigation, a senior employee in Baltic Banking recalled that the Baltic AML Program was run by senior management in Baltic Banking and the Baltic Subsidiaries, the CCO, and other senior employees. A project manager was also appointed, who developed clear deliverables such as policies and procedures related to ProScan and Nice Actimize, KYC questionnaires and related updates. The Baltic AML Program began the process of implementing ProScan by 2017, and Nice Actimize by 2018, across the Baltic Subsidiaries.

According to a senior employee in Baltic Banking, the Baltic AML Program included the development of a new risk classification system, which was initially developed in Latvia and later rolled out to the other Baltic Subsidiaries. While the scope of the Baltic AML Program expanded, and the steering committee continued to meet regularly over the ensuing years, the senior employee in Baltic Banking explained during an interview conducted as part of the Investigation that the increase in customers needing EDD because of the new risk classification system created a constant struggle to maintain sufficient resources. The Investigation's review of contemporaneous documents, including relevant Swedbank Board minutes, indicates that the Swedbank Board was broadly informed of the remediation of insufficient KYC processes and inadequate AML risk assessments in the Baltic Subsidiaries (as discussed further below). Between 2016 and 2018, the Board was also told of resource issues within the Compliance function in general. The Investigation, however, did not find evidence that the Board was informed that the remediation of identified deficiencies in AML and KYC processes in the Baltic Subsidiaries, and in particular the increase in required EDD, was hampered by inadequate resources.

The Panama Papers Leak Leads to Acceleration of HRNR De-Risking

In April 2016, the ICIJ published the results of a year-long investigation based on a leak of 11.5 million confidential documents from the Panamanian law firm Mossack Fonseca (the "**Panama Papers**"). ICIJ's investigation linked hundreds of international politicians, business leaders and celebrities to over 200,000 offshore shell companies and complex webs of potentially suspicious transactions. Almost immediately after media reports on 3 April 2016, publicizing the release of the Panama Papers, Swedbank initiated an internal review to identify and analyze its exposure to Mossack Fonseca.

On 5 April 2016, the Swedbank CCO reported to the Swedbank Board regarding the developing impact of the Panama Papers. Minutes from that Board meeting indicate that the CCO told the Board that Swedbank was reportedly referenced 700 times in the database of materials leaked from Mossack Fonseca. The CCO informed the Board

that "*each business area [was] performing an investigation to identify if Swedbank has in any way been involved in such engagements*." The minutes reflect that the Board requested a presentation on the outcome of the review at the next Board meeting.

On 25 April 2016, the Swedbank CCO reported to the Board regarding the results of the review of Swedbank and the Baltic Subsidiaries' links to Mossack Fonseca, as well as related AML controls. The minutes from this Board meeting reflect that the CCO determined that a risk assessment was necessary, as were improvements in transaction monitoring and customer screening. The CCO informed the Board that an AML program had already been initiated in Baltic Banking. Finally, the CCO informed the Board that "*[t]he preliminary mapping of the Group's customers shows that there are few connections to [Mossack Fonseca] and no recommendation[s] or advice given to customers encouraging tax evasion have been found*." The memorandum accompanying the CCO's report to the Board, titled "*Customers with offshore engagements,*" summarized the findings on links to Mossack Fonseca in Swedish Banking, LC&I and Baltic Banking:

- Swedish Banking: "*[No] indication of customers that hold a relation [to] Mossack Fonseca*"
- LC&I: "*[N]o direct contact with Mossack Fonseca on record, neither as a client nor partner nor in any other capacity. Our payments department reports no payments transacted by our bank in the last 12-month period either to or from Mossack Fonseca*." *However, 10 former clients in Swedbank Luxemburg prior to 2012 executed payments to Mossack Fonseca*."
- Swedbank Estonia: Twenty-eight customers from 15 customer groups were identified *"who have used Mossack Fonseca as their registered agent in founding and managing an off-shore company. Ultimate beneficiaries of all these customers have non-Estonian background. The largest number (13) of Mossack Fonseca related companies are related [to the HRC-1 Group].*"
- Swedbank Latvia: "*The only relation with [Mossack Fonseca] discovered is in the form of 2 outgoing payments*" (from customers that were residents of Latvia).
- Swedbank Lithuania: "*1 outgoing payment made during 2015 to Mossack Fonseca by [a Lithuania] resident customer*" whose ultimate beneficial owner was connected to a PEP.

In an email from the CCO to the CEO in advance of the 25 April 2016 Board meeting, the CCO provided a draft of the "*Customers with offshore engagements*" report and stated that in preparing the report for the Board the CCO had "*tried to tone [it] down without lying*." The CCO further stated that the report would be provided to the SFSA and "*so it has to be formulated correctly*." The CEO responded that the CEO believed the report "*should begin with explaining the reasons for choosing an offshore construction, i.e. the reasons that we at the bank have condoned setting up offshore solutions or for referral to external party*." The Investigation did not identify a response from the CCO; however, the final version of the report provided to the Board contained the following language in the "Summary" section at the beginning of the report:

> *There are several cases when the bank, or its subsidiaries, have business relations with customers located in offshore jurisdictions. This can be accepted when it is proven and documented that the customers have a legitimate reason to reside in such place . . . To enable a relevant business decision whether a customer can be accepted or not, it is essential that each customer's full identity, the purpose and nature of the relationship with the bank, source of funds, etc. . . . is carried out and properly documented . . . Compliance will advise and support the business to achieve an updated relevant KYC. Moreover, Compliance will monitor the area during Q3/2016 and thereafter report status to Board.*

The initial draft of the report sent to the CEO did not contain this reassuring language. Nevertheless, in an interview for the Investigation, the then CCO recalled being severely criticized by the CEO following the 25 April Board meeting, because the CEO considered the CCO's presentation to the Board too alarmist. Shortly thereafter, the CEO appointed a new CCO (with the appointment formally becoming effective on 1 June 2016), and the former CCO voluntarily left Swedbank. While there was a short period of overlap, the incoming CCO recalled only general discussions with the outgoing CCO about the role and did not receive briefings on any particular pending issues.

On 25 April 2016, an employee in Baltic Banking circulated another memorandum to the senior management of the Baltic Subsidiaries. According to this memorandum, Baltic Banking recognized "*the current increased focus on [offshore] business*" and noted that Swedbank "*might encounter perception challenges despite the fact that our belief is that our processes and routines are solid*." The memorandum noted that "*regulators are increasing the AML and KYC demands on banks and we also encounter substantial increased concerns from correspondent banks on AML and KYC issues in the Baltic region*." As a result of these pressures, the memorandum noted that Swedbank Estonia and Swedbank Latvia had initiated a review of their HRNR customer portfolios; Baltic Banking had launched an AML program to enhance AML and KYC processes; and that Baltic Banking was considering creating a "*high risk steering body*" with participants from Baltic Banking and Swedbank's head office to discuss areas of potential reputational risk.

In addition, the memorandum noted that Swedbank Estonia had decided to exit the relationship with the HRC-3 Group, "*a top 3 customer group*," along with other high risk customers. With respect to Swedbank Latvia, the memorandum noted that 73 HRNR accounts had been closed in 2015. In 16 of those cases, the closure was for "*not understandable transactions or customer activity not corresponding*" to what had been declared. Swedbank Latvia would close additional accounts "*if business activities are not transparent, not corresponding to declared ones and/or if customer is not cooperating in . . . provid[ing] respective documents*."

Also on 25 April 2016, Swedbank Estonia's Management Board received a memorandum that reported significant growth in the HRNR business in the prior two years. The report indicated that while most of this growth resulted from the decision of some large customers to keep higher cash buffers due to turbulence in financial and commodity markets, the appreciation of the USD and the addition of new customers (partly due to CPB-1's decision to close its HRNR business) also contributed to the growth of this business. The memorandum noted that the 10% limit on HRNR deposits was slightly surpassed in November 2015, and Swedbank Estonia was taking measures to reduce the deposit amounts of the biggest depositors by December 2016. These measures accorded with the decision reached at the 14 March 2016 Management Board meeting, which reflected that HRNR payment volumes should be monitored and restricted when necessary.

Scrutiny of HRNR Customers Leads to De-Risking

In May 2016, the Swedbank CEO, senior executives of Baltic Banking, and the Supervisory Councils of Swedbank Estonia and Swedbank Latvia received a memorandum by Baltic Banking discussing efforts to off-board HRNR customers. This memorandum included specific statistics about the HRNR segment in Estonia and Latvia, prominent customer groups and the historical development of the portfolio. The memorandum concluded that, due to increased regulator focus and reputational risk surrounding HRNR customers, Swedbank Estonia and Latvia "*initiated a review of its HRNR business model and client base in order to decide further steps to decrease the risks for this customer segment*." The meeting minutes reflect that the memorandum and off-boarding of HRNR customers was discussed at this May meeting.

Soon afterward, in June 2016, Swedbank Estonia began to consider how to mitigate its exposure to AML risk arising from "*the biggest high-risk non-resident group*," the HRC-1 Group. A memorandum by the HRC-1 Group RM and the RM's supervisor at Swedbank Estonia, dated 15 June 2016, acknowledged AML risks around the HRC-1 Group, but advocated continuing the relationship, because "*[w]e understand the business logic well, the main beneficiary has [a] clear business relationship with Estonia [and] the client relationship is highly profitable for Swedbank.*" The memorandum noted that the Swedbank Estonia Management Board had decided on 25 April 2016 to consider the HRC-1 Group separately from the general effort to reduce the number and payment volumes of the HRNR segment. The memorandum stated that it was debatable whether one of the Russian oligarchs that was a main UBO of the HRC-1 Group should still be considered a PEP. However, the memorandum did not address prior negative media coverage of the two oligarchs who were the primary beneficiaries. The memorandum did recommend that one of the customers within the HRC-1 Group (a railway transportation company) should be off-boarded because of probable connections to another Russian PEP.

Parallel with these developments in the Baltics, Swedbank Group Compliance also proposed a broader assessment of the risk arising from Swedbank's exposure to offshore entities in high risk jurisdictions. A memorandum from Group Compliance to the GRCC identified several issues to address, including:

> *1. Define the Bank's risk appetite when it comes to business models operating with SPVs in low tax countries . . . 2. Define the bank's risk appetite when it comes to business models operating with SPVs in low tax countries for other reasons, such as in Baltic Banking where the reasons could be to protect the assets from political risks (state intervention). 3. Identify Swedbank's exposure to private persons and corporates that are named in the [Panama Papers leak]. The mapping is ongoing and once finished customer relationships need to be analysed and possible further actions need to be decided upon based on the bank's risk appetite.*

This memorandum was discussed at a GRCC meeting on 14 June 2016, at which the CCO presented. The meeting minutes state that "*the task to move forward is complex given that the area is unregulated in some places*," and reflects that the CCO proposed, and the GRCC agreed, to create a working group with participants from Compliance, Risk and the relevant business units. The GRCC minutes also state that the effort would prioritize issues related to the Baltic Subsidiaries.

On 17 June 2016, the CCO contacted the CRO to progress the joint effort between Group Compliance and Group Risk to address the "*aftermath*" of the Panama Papers. The CRO then conferred with other colleagues, noting that the issue was "*fairly urgent as Baltics needs some guidance from the group (they have historically quite a few clients with tax haven accounts).*"

Swedbank and the Baltic Subsidiaries Respond to Increased Regulator Scrutiny in the Wake of the Panama Papers Leak

In April 2016, Swedbank and Swedbank Estonia were also working on responses to requests from regulators relating to the Panama Papers and Mossack Fonseca. On 12 April 2016, Swedbank and Swedbank Estonia received requests from the SFSA and EFSA, respectively.

Among other questions, the EFSA asked Swedbank Estonia to provide information about whether it, or its customers, had any "*associations or connections with the 'Panama Papers,'*" and, if so, to provide (1) information about the nature of the association or connection; and (2) any steps taken by Swedbank Estonia in relation to the matter.

The SFSA request also pertained to the Panama Papers. It referenced the recent publication of the "*so-called Panama documents and the information which has emerged from these concerning off-shore structures*," and asked Swedbank a number of questions including whether there were "*business areas of the bank, its branches or subsidiaries*" that offered services or products to offshore structures.

Swedbank responded to the SFSA on 15 April 2016. With respect to the Baltic Subsidiaries, Swedbank noted that a large number of customers had companies registered in offshore countries, but stated these corporate structures had been established without Swedbank's involvement, and that the purpose of these companies, according to the customers, was to protect their assets from "*corruption and criminality in certain states*." Swedbank stated that it was aware of the elevated risks for tax evasion and money laundering that can arise from these structures, and therefore required such customers to go through a special review process before on-boarding. The response also noted that there was close monitoring of those customers' transactions, which included random sample monitoring on an ongoing basis, and that "*[t]he Bank also has close cooperation with relevant supervisory authorities in the Baltic countries in which the conditions for the business relationship with these customers is discussed, which assures transparency*."

However as outlined above (*see supra* at 64-71, 80) although Swedbank Estonia had the HRCAC, it frequently had incomplete information about the customers it reviewed, did not engage in significant analysis, and approved customers on the RM's recommendation despite the existence of red flags. Swedbank Estonia also repeatedly opened accounts for shell corporations and processed transactions for such customers when the apparent purpose was to shield from third parties the identity of the high-risk customer group's UBOs as well as the source and ultimate destination of funds. Some Swedbank Estonia employees had previously worked with corporate services providers to offer account opening packages to customers that included "*ready-made*" companies in low tax jurisdictions. In addition, at this time, as set forth above, the Baltic Subsidiaries did not consistently monitor for potentially suspicious transactions. However, the Investigation has not identified evidence that the Swedbank CCO or Baltic Banking senior managers who prepared this response to the SFSA were aware of the prior use of corporate service providers, or that they were aware of the specific examples of deficient transaction monitoring set forth above.

On 19 April 2016, Swedbank Estonia responded to the EFSA. Swedbank Estonia stated that after the Panama Papers were published, it had immediately checked documents (primarily the articles of association and registration certificates) for all customers who were legal entities registered in low tax rate countries, to identify any associations with Mossack Fonseca. Swedbank Estonia confirmed that as a result of this review, it had identified 29 customers for which the registered agent was Mossack Fonseca and had listed these customers in an Annex. The response identified the Annex as "*[a] list of clients where Swedbank has identified a connection to the law office Mossack Fonseca.*"

Swedbank Estonia's response also stated that:

> *Already for several years before the so-called 'Panama papers' articles were published, [Swedbank Estonia] has been handling low tax rate countries as high-risk countries, and companies registered there are subject to significantly larger restrictions and a stricter process when opening their account or making transactions associated with such accounts. Opening accounts for companies registered in high-risk countries is only permitted based on a decision by the relevant committee. In their decisions, the non-resident committee considers various factors, incl. the background and origin of assets of the beneficial owner, the transparency of the applicant's economic activity, transparency of counterparties, the motivation for registering the company in a specific territory, etc. Additionally, transactions by enterprises registered in high-risk countries are subject to strict monitoring, incl. asking additional information and documentation regarding transfers which are bigger, unusual, or otherwise of interest to the bank.*

As with Swedbank's response to the SFSA, Swedbank Estonia's response to the EFSA did not disclose that, in practice, the HRCAC had on-boarded numerous customers without either a complete understanding of the customer's ownership structure or a legitimate commercial purpose, and that these customers had engaged in potentially suspicious transactions.

In May 2016, the Baltic Subsidiaries identified additional customers with links to Mossack Fonseca. Senior managers in Baltic Banking and in the Baltic Subsidiaries were updated through an internal report that noted that Swedbank Estonia had 37 customers that used Mossack Fonseca as a registered agent (and that there were another 56 natural persons referenced in the Panama Papers leak that were either customers or associated with customers). When the EFSA requested additional information from Swedbank Estonia a year later on 20 March 2017 regarding "*additional measures in order to assess your potential involvement with the Panama Papers case*," Swedbank Estonia's response of 12 April 2017 repeated that it had identified 29 customers with links to Mossack Fonseca, without updating the numbers. Although several Swedbank Estonia employees who participated in producing the 12 April 2017 response had received the updated numbers in May 2016, the Investigation has not found evidence that the reporting of the inaccurate number in 2017 was intentional.

On 22 April 2016, the SFSA sent Swedbank – using the same reference number as the 12 April request – a follow-up request for information with six subparts that noted that it was in connection with the SFSA's "*on-going supervision of Swedbank AB*." Among other things, the different subparts requested (1) a list of all of "*Swedbank's Private Banking and LC&I customers*" that completed transactions to or from certain listed countries between 14 June 2014 and 19 April 2016, and (2) a list of "*legal persons*" that were (a) "*customers of Swedbank AB (Publ), Luxembourg Branch or Swedbank Management Company S.A. with fiscal domicile,*" in certain listed countries, and had at least one beneficial owner "*with a business relationship with Swedbank*," or (b) had either "*assets exceeding 25 million SEK or equivalent with Swedbank*" or "*credit engagements (excluding credit cards) with Swedbank*" and also "*at least one beneficial owner with fiscal domicile*" in one of certain listed countries.

The SFSA's 22 April request did not expressly refer to Swedbank's "*branches or subsidiaries,*" as it did in its 12 April request, but rather used the term "Swedbank," except when referring to specific entities or businesses, such as "*Swedbank AB (Publ), Luxembourg Branch*."

A few days later, Swedbank employees discussed how to respond to the SFSA's 22 April request, and among other things, the relevant scope of the request. On 25 April 2016, employees of LC&I met regarding the response to the SFSA and discussed the question of the request's scope. Contemporaneous communications reflect that LC&I, in consultation with Group Compliance, decided that for the scope of the 22 April request, "*[t]he interpretation is that Swedbank = Swedbank AB, i.e. the questions also cover the branches but not the subsidiaries, except in question 4, where this is specified for Manco in Luxembourg.*" The Investigation did not identify evidence that Swedbank discussed this interpretation with the SFSA.

On 28 April 2016, an LC&I employee explained to LC&I Baltic colleagues that Swedbank employees working on the response had determined that customers with accounts in the Baltic Subsidiaries who received LC&I products or services were not covered by the SFSA request because "*these clients formally belong to the legal entities in the Baltics even though they organizationally belong to LC&I in Swedbank. As the Swedish FSA asks only about clients belonging legally to Swedbank AB (Sweden) and its branches, the scope will not include these clients. In short, you are off the hook*."

Swedbank provided initial answers to the SFSA's 22 April request in two tranches, on 4 May 2016 and on 16 May 2016. In addition, an internal email exchange in August 2016

between two LC&I employees stated that Swedbank's response to the 22 April request "*didn't report any Baltic customers to the SFSA in connection to Panama since the choice was made to interpret the questions as concerning Swedbank AB, on the other hand the question is whether the LC&I customers in the Baltics were controlled in the correct manner*."

On 23 May 2016, the SFSA made a follow-up request for information on 30 (including HRC-1 which had been identified due to its FX relationship with LC&I) of the approximately 440 customers listed in Swedbank's May response. The request included the following three subparts:

> *1. [. . .] all transactions exceeding SEK 500 000 or equivalent in all accounts of select customers in the bank between the period of May 19, 2015 and May 19, 2016 [. . .]*
>
> *2. All customer knowledge information that the bank has for each selected customer. The information shall be provided to the SFSA in electronic format.*
>
> *3. Information on the risk of money laundering and terrorist financing the bank has assessed each selected customer to constitute. A description of the reason for the assessed risk is also required. The information shall be provided to the SFSA in electronic format.*

Swedbank responded to this request on 3 June 2016, providing the follow-up information requested by the SFSA. In preparing the KYC submission, LC&I employees contacted employees at Swedbank Estonia to request additional documents for inclusion in the KYC file for HRC-1.

On 15 June 2016 (after the Bank had submitted its response to the SFSA), an LC&I manager who handled the preparation of the SFSA response emailed several employees, including the LC&I RM for HRC-1, stating that "*[on] a review of the material that we were supposed to send in with respect to the actual KYC, Group Compliance determined that* ***NO KYC*** *was satisfactory in terms of quality.*" The LC&I manager directed that all KYC documentation already submitted to the SFSA be examined, completed, and risk assessed by the end of the month. A 15 June 2016 report prepared by an LC&I analyst also found problems with LC&I KYC, noting that the backlog of customers lacking relevant KYC persisted in LC&I despite the fact that LC&I had been working to eliminate the backlog, and had set a deadline to do so by the end of 2015. This report explained that monitoring was conducted in Q1 2016 to confirm whether the deadline had been met; it found that 30% of 168 sampled customers lacked relevant KYC. The report also noted that this assessment was quantitative only; it had not tested the quality of any existing KYC. The report was later circulated in early-July 2016 to the Swedbank CCO and senior management in LC&I. The Investigation has not identified evidence that the Board nor any of its committees were informed about this 15 June 2016 report. On 22 June 2016, however, the CEO provided the Board with an update on the ongoing SFSA review regarding the Panama Papers. The minutes indicate that, in response to a question from the Board, "*the CEO responded that no structural wrongdoings have been found*."

On 20 July 2016, the Board was informed by the CCO that, in response to the SFSA's request, Swedbank had "*submitted transactions and KYC document[s] . . . on 30 specific customers (LC&I and [Swedish Banking])*" in early June and was awaiting a response. The Investigation has found no evidence that the Board was informed that all of the LC&I customers selected by SFSA for review had, by LC&I's own assessment, incomplete KYC materials. However, that same day, the Swedbank Board and Audit Committee received a report noting the continuing KYC backlog in LC&I and Swedish Banking, but without a proposed timeline for completing outstanding KYC (which had been provided in prior reports in 2015 and 2016). The minutes from the 20 July 2016 Board meeting do not reflect a discussion about the KYC backlog. During the

Audit Committee meeting that same day, the CCO stated that "*there is a continuous positive trend as regards [KYC]*" and that a recent review of KYC for Swedish Banking determined that 91% of new private customers and 67% of new corporate customers had proper KYC materials.

In a presentation submitted to the Audit Committee on 20 July 2016, the Bank's external auditor reported that "*there has not been a documented risk analysis performed since 2014 to evaluate [i]f the controls are considered to be the most essential to mitigate current AML risks. In addition, GIA testing revealed that the control documentation differs between regions and that the KYC quality control performed on new customers is not consistently assessed*."

The minutes of subsequent Board meetings do not reflect discussion of KYC issues in LC&I. Instead, the minutes indicate that discussions focused on emerging AML issues such as the FCMC audit of Swedbank Latvia, which, as discussed below, began not long after the Panama Papers leak in April 2016.

FCMC Inspection of Swedbank Latvia in April 2016

In late-April 2016, the FCMC began a two month on-site inspection of Swedbank Latvia's AML controls. The FCMC submitted the preliminary results of its investigation to Swedbank Latvia on 19 August 2016, and Swedbank Latvia responded with comments on 12 September 2016.

The FCMC's 19 August report identified a number of deficiencies in Swedbank Latvia's internal AML/CTF control system. The report stated that the Swedbank's "*internal control system allows for the possibility of a client on whose economic activity the Bank has not acquired sufficient amount of information, to open an account and to do business on a large scale and within [a] few months to close the account*." In response, Swedbank Latvia's September comments on the FCMC report included the statement that, "*[e]ven though Swedbank agrees with the importance of efficient internal control systems, and continuous improvements thereof, Swedbank urges the Commission to evaluate the fact that the irregularities have not increased the actual risk for money laundering or terrorist financing as extenuating circumstances.*"

Based on GIA reporting, this response appears to have been an overstatement. In connection with its inspection, the FCMC had requested on 1 April 2016 that Swedbank Latvia provide "*Internal Audit inspection plan[s] for 2014, 2015 and 2016, and plan fulfilment for 2014 and 2015.*" In response to this request, Swedbank Latvia provided two GIA reports from January 2015 and February 2016. The Investigation did not find evidence that Swedbank Latvia provided the FCMC with the 30 June 2015 GIA report, which contained the most serious criticism of Swedbank Latvia's internal control systems.

The GIA report dated 30 June 2015 stated that "*due to deficiencies in the KYC process, Swedbank Latvia may not timely identify suspicious or unusual client activities*" and the failure of Compliance to monitor "*non-residents' accounts*" or to appropriately document "*money transfers from these accounts*" could lead to breaches of regulations and "*potential fraudulent activities might not be timely identified*." The report also revealed that, for some of the transactions reviewed by GIA, "*customer due diligence (. . .) was not performed by client managers during 45 days as required by external regulations,*" whereas in such instances "*Latvian FSA rules on Customer Due Diligence require*" the termination of the relationship with these customers. These deficiencies remained unresolved as of October 2016, when a GIA report identified two "*overdue*" findings from the 2015 audit report relating to the quality of the existing transaction monitoring process, and the need to update internal regulations to improve non-resident account monitoring.

Later GIA Reports in 2016 identified continued inadequacies in Swedbank Latvia's AML/KYC processes and governance. Many of these GIA reports, including the

critical GIA report issued on 30 June 2015, were subsequently provided to the FCMC in connection with a regular inspection in December 2017 that requested, among other things, "*Internal audit reports on audit engagements carried out in 2015, 2016 and 2017, including information on the follow-up of the improvement actions' implementation and status on 2017-11-30.*"

Swedbank's Further Responses to the SFSA Regarding the Panama Papers and Related Requests

On 24 August 2016, the Swedbank CCO met with the SFSA for a quarterly compliance meeting. During the meeting, the SFSA requested information about measures Swedbank had taken, or planned to take, as a result of the release of the Panama Papers. A day after this meeting, the SFSA informed the CCO by email that it wished to further discuss Swedbank's AML processes, including at the Baltic Subsidiaries, at the next quarterly meeting on 8 November 2016.

On 9 September 2016, Swedbank responded to the SFSA's request for information in writing, stating that it was working to define a comprehensive framework for "*so-called* '*conduct risk' specifically related to questions associated with the Panama [Papers].*" The Bank's response added that this work would particularly address issues of tax avoidance in an effort to formulate an approach to situations that could be considered a "*gray zone*" from a tax perspective. Swedbank also advised that it was reviewing its customer base against the ICIJ Database, and that it had identified two customers in Swedish Banking with links to the Panama Papers.

Swedbank's 9 September response to the SFSA also disclosed that Swedbank had identified customers of its Norwegian branch and the Baltic Subsidiaries with links to the Panama Papers (without providing the number of such customers), and that in light of "*the Baltic countries' exposed geopolitical situation*," a broader survey of the customer base in the Baltic Subsidiaries was underway. The letter stated that these actions and ongoing reviews would be reported to Swedbank's GRCC.

Minutes from a GRCC meeting on 8 September 2016 indicate that the CCO and an AML Compliance employee presented on a "*Project related to conduct risk*." The minutes state, without further detail, that there was a "*general discussion*" and that the GRCC approved a "*workshop to move the matter forward*." The GRCC meeting materials packet also included a memorandum prepared by a Group Risk employee dated 8 September 2016, titled "*Tax handling and business ethics*." This memorandum stated that as part of a larger review of conduct risk, Group Operational Risk performed an assessment of tax-related issues at Swedbank, including "*complicity to customers['] tax planning*." On this point, the memorandum noted:

> *In Baltic Banking, clients utilise offshore structures to e.g. protect assets from corruption and criminal activities in certain geographies. The Baltic [Subsidiaries] are well aware of the increased risk of tax evasion and money laundering that those structures entail and [have] implemented more granular on boarding and monitoring procedures for such clients. The Baltic [Subsidiaries] also maintain a close relationship with supervisory authorities on those matters to ensure transparency and compliance.*

On 8 November 2016, the Swedbank CCO and a senior executive from Group Compliance met with the SFSA for its next quarterly meeting. In preparation for this meeting, the SFSA had written the Swedbank CCO on 24 October 2016, requesting that Swedbank "*report on the points below for the 8 November AML meeting*," including *"all Swedbank's current and ongoing events in the money laundering area*" and a "*summary of Swedbank's internal investigation in response to the Panama documents*." In response, the CCO circulated to the SFSA on 4 November 2016, among other things, a memorandum titled "*Money Laundering follow-up Swedbank*

AB presented at the Financial Supervisory Authority meeting of 8 November 2016." This memorandum provided an overview of the AML work performed by Swedbank up to that date, including a section on the "*[s]tatus of activities related to the Panama Papers leaks/offshore*" that noted work on the conduct risk initiative was continuing, and that an ongoing "*wider review of the customer base with a focus on customers within Swedish Banking and LC&I that are established in high-risk countries according to the Bank's internal country risk list"* and that "*the preliminary results show areas for improvement where the next step is to increase the level of awareness of the risks associated with, for example, tax havens.*" With respect to the Baltics, the memorandum stated:

> *For the business area [of] Baltic Banking, the work on evaluating customer relationships where links to the Panama leak were identified has continued. As a consequence of the links, the business area has introduced stricter requirements in the decision-making process at the time of on boarding of new customers with links to offshore jurisdictions. The business area has also off-boarded customers with low-activity, where the link to the host country is considered to be weak and the re-evaluated risk has been considered to be unacceptable.*

The memorandum added that "*[a]t the request of the [SFSA] in connection with the most recent quarterly meeting, this letter also includes a section on the Bank's operations in the Baltic countries.*" This section in the memorandum was approximately one page in length, and contained general descriptions about the Baltic Banking business, KYC and AML program. This section stated that "*[o]versight and proactive work to terminate the relationship with a number of high-risk customers who are 'non-residents' are in progress.*" The Investigation otherwise has not identified evidence that Swedbank disclosed during this meeting that it had identified significant AML issues with the HRC-1 Group and was preparing to terminate the entire customer relationship (as discussed below).

With respect to the conduct risk initiative, a subsequent CEO Report to the Board covering October 2016 reported that the initiative was "*moving slowly due to the complexity of the matter*," and that a first draft of a possible conduct risk framework would be discussed in the GRCC in December 2016. A 12 November 2018 memo titled "*Conduct risk: current activities and the way forward,*" discussed the development of a conduct risk definition and framework, but noted that the initiative first proposed in 2016 had not yet been implemented. The Investigation has not identified any further discussion of the conduct risk initiative after November 2018.

Decision to Off-Board the HRC-1 Group

While Swedbank was responding to the SFSA in 2016, an LC&I AML officer conducted enhanced due diligence on HRC-1, given that it was one of the subjects of the SFSA's request for information on 23 May 2016 (as described above). From late May 2016 through the end of June 2016, the AML officer repeatedly escalated to senior managers the AML risk posed by HRC-1, based on research that the AML officer had performed through examination of compliance databases and public media reports. The AML officer raised questions about HRC-1's complex ownership structure, the accuracy and completeness of beneficial ownership information, and the source of funds used by the current owners to acquire full control from the previous owners.

As a result, LC&I began to review its relationship with HRC-1, and sought additional information from HRC-1 through Swedbank Estonia. In August 2016, the LC&I AML officer asked the main RM for the HRC-1 Group to provide a list of customers associated with the two primary beneficial owners of the HRC-1 Group. The RM responded with a list of approximately 200 customers in the HRC-1 Group, which categorized them as, among others, holding companies, private assets, and "*wallet*

companies." The AML officer observed to the RM that many were incorporated in tax havens, and several were referenced in the Panama Papers leak. The RM assured the LC&I AML officer that all of the HRC-1 Group companies had been approved by the HRCAC, that the RM had clear information on their business activities and source of funds, and that HRC-1 Group's transactions were subject to enhanced monitoring.

In September 2016, the LC&I AML officer distributed a report highlighting the AML officer's findings about the elevated AML risk presented by HRC-1. Senior managers in LC&I agreed that HRC-1 should be off-boarded from LC&I. When interviewed for the Investigation, the LC&I AML officer recalled that the decision to off-board HRC-1 was a joint decision made by several senior managers. The AML officer also stated that there was resistance to this decision from the CEO of Swedbank Estonia, other senior managers within Baltic Banking, and the HRC-1 Group RM in Estonia. The LC&I RM for HRC-1 also reported that Swedbank Estonia took longer than LC&I to conclude that it should off-board HRC-1.

On 20 October 2016, Swedbank Estonia's CEO circulated a memorandum to the CCO and senior management at Baltic Banking and the Baltic Subsidiaries, among others, reporting that Swedbank Estonia's Management Board had come to a "*joint decision*" with LC&I to off-board the HRC-1 Group by Q3 2017. The HRC-1 Group was then described as comprising "*1/3 of [the] total HRNR customer base (~200 legal persons) [in Estonia] and 1/2 of [transaction] volumes*." Swedbank Estonia's CEO also described a number of risk mitigation measures that the Management Board had approved. These included off-boarding: (1) offshore HRNR companies with a "*weak link*" to Estonia, (2) HRNR companies whose beneficial owners were registered in an offshore jurisdiction, and (3) any accounts of HRNR financial institutions. In addition, the HRCAC would evaluate whether to off-board offshore HRNR customers with a "*medium connection*" to Estonia. Finally, the Management Board decided to limit outgoing USD payments by HRNR customers and reduce the HRNR deposit volume limit to 8% of Swedbank Estonia's total deposits.

Conclusion of FCMC Investigation

A few days later, on 24 October 2016, the CCO (accompanied by the CEO) provided an update to the Audit Committee of the Swedbank Board regarding the outcome of the FCMC's on-site inspection of Swedbank Latvia earlier that year. According to the minutes of this Audit Committee meeting, the CCO advised that the FCMC conducted its inspection from April to June 2016, examined 66 customer files, and found the following AML deficiencies:

- "*[T]oo much reliance on manual procedures*."
- "*[I]nsufficient analysis of clients unusual and suspicious transactions, including source of funds*."
- "*[B]eneficial owners were not always sufficiently analyzed or documented.*"
- "*[S]carce resources*."

The minutes indicate that the CCO summarized several remedial actions, including the "*decision to terminate part of non-residential clients in Latvia and Estonia*." The minutes further reflect an interest from the Audit Committee regarding the implications of these findings for the Group. When the Audit Committee asked the CCO whether the newly identified AML deficiencies in the Baltic Subsidiaries "*could be anticipated in Sweden*," the CCO replied "*not necessarily*." The Audit Committee also asked what GIA had done in this area, and a GIA senior executive reported that "*audits were performed in 2011, 2013, and 2015 including reviews of inter alia KYC, screening and the sanction catalogue with a bad audit result*." The GIA senior executive continued that *"[d]uring the*

last couple of years Sweden came into AML focus due to a SFSA investigation, and the vast majority of resources were put into Sweden rather than Baltic Banking."

The minutes reflect that the CEO then remarked that "*the bank has changed a lot*" and that *"[a]t the moment the bank is reviewing what is included in the business,"* with the CCO adding that this was being done with the help of Group Compliance. The CCO discussed, from the perspective of Group Compliance, the main areas of reputational risk for Swedbank as a group, such as reputational risk for Latvia as a country, the potential for spillover effects from Latvia to Estonia and Lithuania, high reputational risk in Sweden, and the risk of a negative reaction from correspondent banks. The CCO further indicated that when another bank was fined for AML issues, there had been no significant impact on its share price. The CCO informed the Committee that the next step for Swedbank Latvia consisted of negotiating an "*administrative agreement*" with the FCMC and, following questions from the Audit Committee during the meeting, added that the authority had indicated the Bank could risk "*a warning in combination with a fee.*" The minutes do not reflect any further discussion regarding risks arising from historical activity.

Minutes from a 24 October 2016 meeting of the Swedbank Board reflect a similar presentation from the CCO to the Board on the findings of the FCMC inspection, including on actions already taken by Swedbank to address deficiencies. The actions included:

- an "*AML-program in Baltic Banking during spring*;"
- new compliance heads at Swedbank Latvia and at the Baltic Banking level;
- "*[i]mproved internal procedures*;"
- "*[o]nline PEPs screening implementation*;"
- monitoring of suspicious activities and payment flows; and
- a "*[d]ecision to terminate part of non-residential clients in Latvia and Estonia*."

The minutes reflect only high-level observations regarding reputational risk and follow up actions, and do not indicate any reaction from Board members regarding reputational risk or reactions to the findings. By this time in October 2016, Swedbank Latvia management had already decided to de-risk its HRNR customer segment, committing to a plan to off-board 75% of the HRNR customers by the end of 2016, and then the remaining 25% would be individually evaluated in conjunction with Group Compliance.

On 23 November 2016, Swedbank Latvia entered into an administrative agreement with the FCMC, accepting a reduced fine with the commitment to eliminate the deficiencies found and to implement improvements. One of these commitments was to substantially reduce Swedbank Latvia's HRNR customer segment. Pursuant to this commitment, Swedbank Latvia initiated a review of its HRNR customer segment and decided to off-board its HRNR customer segment in phases. Swedbank Latvia management chose to off-board in phases because they were concerned that if all HRNR customers were off-boarded at once, Swedbank Latvia risked losing the RMs who were needed to assist with the off-boarding process.

Swedbank Latvia Reassesses its Risk Profile and Decides to Off-Board HRC-6

In November 2016, shortly before concluding its administrative agreement with the FCMC, the Latvian Supervisory Council was informed that the Management Board of Swedbank Latvia had decided on 27 October 2016 to no longer serve HRNR legal entity customers as of 1 January 2017, and that any exception would need to be approved by the CEO of Swedbank Latvia. Although HRC-6 was a domestic customer of Swedbank Latvia, a correspondent bank inquiry would soon cause Swedbank to re-assess its risk tolerance for HRC-6.

Soon afterwards, one of Swedbank's USD correspondent banks (the "CB") notified Swedbank that it had noticed an increased amount of suspicious transactions from Swedbank Latvia customers. A Baltic Banking employee noted that the same correspondent bank had been closing the USD accounts of "*small Baltic banks*" resulting in their customers seeking new USD banking relationships. Accordingly, the employee noted, "*[w]e must be extra careful in on boarding new corps*."

Swedbank briefed the CB on Swedbank Latvia's administrative agreement with the FCMC in early December. Later that month, the CB followed up by email to provide a list of Swedbank Latvia customers with the highest volume of USD payments in the previous six months, one of which was HRC-6. The list included 41 customers, of which almost half were indicated as being non-resident customers. The correspondent bank stated that it did not immediately require additional information, but that it might seek "*further information regarding the beneficial ownership of those largest non-resident* clients" in the new year. A Swedbank Latvia employee forwarded the list to a colleague requesting that they look into the non-resident customers (which included HRC-6) in preparation for potential requests by the CB. As a result of these inquiries, Swedbank Latvia assessed that 19 entities on the list, including HRC-6, were domestic legal entities for whom banking services could continue, while others had been, or were in the process of being, off-boarded.

A Swedbank Latvia senior executive, however, made further internal inquiries about HRC-6 to determine whether proper KYC had been conducted on the customer. The senior manager concluded that KYC and EDD checks had been performed at various times, but only limited information could be obtained about the customer's Russian political connections from publicly available sources. During early December 2016, a Swedbank Latvia senior executive discussed HRC-6 with senior Group Compliance personnel, noting that the beneficial owner was not a PEP based on available information, and that the customer's activity fit the customer's business profile and did not run afoul of AML policy. Nevertheless, the Swedbank Latvia senior executive questioned whether the customer was acceptable from a Swedbank Group perspective. In response to an email from the senior Swedbank Latvia executive asking whether HRC-6 "*is the type of [] Client with whom we want to continue business*," a senior Group Compliance employee emphasized that Swedbank "*should avoid doing business with [beneficial owners] of this kind as a local retail bank*" because even if "*the specific engagement/operations [] might look ok there is always a risk that suspicious money flow[s] through our system.*"

Also in early December 2016, in the context of a request to approve an HRC-6-related company's letter of credit arrangements, a managing director of corporate customers within Swedbank Latvia's Large Corporates Division had conferred with a senior manager within Swedbank Latvia Compliance, who advised that the HRC-6 affiliate and its transactions were acceptable. However, another Swedbank Latvia employee objected, noting that the HRC-6 affiliate's transactions "*have nothing to do with Latvia*." The senior Swedbank Latvia executive echoed these concerns, stating that "*[f]rom the Group's point of view, this is a very high-risk client and it is mentioned several times that [this is] not the Swedbank Group['s] business . . .*"

In late December 2016, following the request from the CB, and in connection with a determination to exit relationships with HRNR companies that lacked a business relationship with Latvia, Swedbank Latvia's Compliance function conducted EDD on HRC-6. At that time, a senior manager within Swedbank Latvia Compliance sought input from a Group Compliance employee to conduct a proper risk assessment. The senior manager noted that relevant concerns included HRC-6's relatively large turnover (which had drawn attention from the correspondent bank), as well as the fact that although the company was registered in Latvia, its business consisted of serving as an intermediary between producers in Russia and buyers in regions as diverse as South America and China. The senior manager noted that an EDD form recently completed

in Latvia recommended continuing the relationship while monitoring transactions, on the basis that HRC-6's activities were "*economically justified*." The EDD form contained little information on ultimate beneficial ownership, noting merely that UBO had not changed. The Group Compliance employee conducted additional research and developed a chart demonstrating risk-relevant links for HRC-6, including that the Chairman of the ultimate Russian parent entity of HRC-6 was a PEP. By the end of January 2017, the Group Compliance employee recommended that Swedbank Latvia conduct more detailed EDD, including reviewing ownership documentation, if Swedbank Latvia wished to keep the customer.

On 15 February 2017, Swedbank Latvia decided to off-board HRC-6 given these identified risk factors. The following week, the relevant RM entered into discussions with HRC-6 to begin closing its accounts at Swedbank Latvia.

On 2 March 2017, representatives of the CB contacted Swedbank to request a meeting regarding changes to that bank's "*handling of non-financial risk*," and its "*future strategy for the Baltics*." At the meeting on 16 March 2017, the CB informed Swedbank that it would be discontinuing USD clearing services for Swedbank Estonia and Swedbank Latvia. Following the meeting, a Swedbank employee noted that the decision was not specific to Swedbank or its Estonian or Latvian operations, writing in an email that "*it's not about us, it's about them*." On 20 March 2017, Swedbank's CEO reported to the GEC on the CB's exit from those countries. According to the minutes from that meeting, the CEO stated that the CB "*has announced they consider Estonia and Latvia [to be] high risk countries*" and would soon exit those jurisdictions entirely.

In April 2017, senior executives of Swedbank met with counterparts at the CB and various other correspondent banks and discussed Baltic HRNR customers. Swedbank's presentation at this meeting identified HRC-6 (along with certain HRC-1 Group entities) as among then-current customers whose accounts Swedbank would close.

By 15 June 2017, all of HRC-6's accounts at Swedbank Latvia were closed. On that date, a Group Compliance employee examined some of HRC-6's transactions and recommended conducting further checks going back several years on transactions involving certain counterparties going back several years. In particular, one HRC-6 counterparty had previously been connected to a UK company linked to proxy networks and a former Ukrainian politician.

In August 2017, the Group Compliance employee followed up with the senior Swedbank Latvia Compliance manager, asking if the manager had done anything else to reach a conclusion on whether or not to report the transactions to the FIU. Another Swedbank Latvia Compliance employee responded that, because HRC-6 had been off-boarded and HRC-6's RM had previously left the Bank, it would be difficult to obtain documents concerning HRC-6's historical transactions.

In July 2017, HRC-6 attempted to transfer funds to its Swedish branch account (which Swedbank had neglected to close). When the HRC-6 account in Swedish Banking came to the attention of the CCO, Compliance personnel wrote to a Swedbank senior RM, noting that HRC-6 should be off-boarded in Swedish Banking because the customer was high risk and Swedbank would not be able to handle the related monitoring. As a result, Swedbank decided to close the Swedish Banking account as well. The senior RM stated that if Swedbank had a well-functioning customer management system, it would have been able to see each jurisdiction where the customer had a relationship, and accordingly "*if off-boarding takes place in one country, it would send a signal to other countries, as well. But then our system isn't*

that sophisticated." The CCO agreed, noting that there was now an obligation for the off-boarding employee to check if the customer has a relationship elsewhere within Swedbank. The CCO noted that while the new instruction was "*good on paper . . . like you said, we don't have any system support*," and "*maybe we should have thought of checking [HRC-6 in Sweden] too*."

Swedbank Latvia Begins to Exit the Relationship with HRC-5

When Swedbank realized that HRC-6 still had an open account in Swedish Banking, the CCO wrote to the senior employees within Swedbank Latvia Compliance and Group Compliance, seeking confirmation that HRC-6 had been off-boarded from Swedbank Latvia. The senior Swedbank Latvia Compliance manager stated that the accounts were indeed closed in Latvia, but there were ongoing discussions between the business and Group Compliance on how to handle HRC-5,which was partially owned by a corporate affiliate of HRC-6.

Since June 2017, a special AML task force within Group Compliance had been conducting a review of high risk customers, and in September 2017, identified several customers presenting "*a potentially huge legal and reputational risk for the Bank*." A member of the AML task force prepared a draft memorandum that summarized this review and identified HRC-5 as among Swedbank Latvia's customers that "*pose the highest legal and reputational risk*." According to the draft memorandum, its recipients were the Swedbank CCO and two other senior executives. The Investigation has not found any evidence that this draft memorandum was ever finalized, or circulated to the Swedbank Board or its Committees.

On 15 November 2017, Group Compliance confirmed that Swedbank had filed suspicious activity reports on HRC-6 in both Latvia and Sweden, noting that a separate correspondent bank had asked questions about HRC-6's transactions in April 2017. Also in November 2017, an RM and a senior executive at Swedbank Latvia prepared an EDD memorandum delivered to the KYC/AML steering group (consisting of Group Compliance, Baltic Banking and Swedbank Latvia personnel), which concluded that HRC-5 constituted a "*borderline risk relationship from [an] AML perspective*" due to (1) income generation through the related entity HRC-6, which Swedbank Latvia had off-boarded earlier in 2017, (2) assumptive ties to money laundering issues related to the ultimate beneficial ownership of the HRC-6 group, and (3) reputational concerns. Unlike HRC-6, however, HRC-5 had a direct business presence in Latvia. Nevertheless, in light of the associated risks identified, the memo proposed a "*soft*" off-boarding for HRC-5 by limiting the scope of services provided. A "*hard*" off-boarding was not considered viable.

In April 2018, the Swedbank CCO and other senior managers approved a soft exit for HRC-5. Swedbank Latvia was required, however, to implement numerous risk mitigation measures in the meantime such as the monitoring of transactions, restricting new products and obtaining all beneficial owner information. Swedbank Latvia decided to phase out the relationship with HRC-5 gradually.

LC&I Restructures its KYC and AML Functions While Problems in the Baltics Persist

In 2016, although new AML and KYC processes had been implemented, an LC&I AML manager reported that risk assessments remained inadequate. In particular, the manager noted that RMs viewed KYC as an "*administrative hurdle*" and that there was not sufficient "*risk maturity*." RMs would often fail to make proper risk assessments for their customers. As discussed above, a 15 June 2016 report prepared by an LC&I AML officer found a continued "*backlog consisting of customers lacking relevant KYC*" within LC&I. This report was distributed to senior managers within LC&I as well as the Swedbank CCO. The report concluded that "*LC&I [has] yet to have compliant KYC decisions in relation to some of their customers*" and that when "*no risk assessments have been conducted (. . .) there is no way of knowing [what] risks the bank is exposed to*." As next steps, the report recommended, among other things, that LC&I perform a "*root cause analysis to set the basis for a long term vision and plan on set-up, competence and process enhancements [including] system support*."

Shortly thereafter, a KYC manager within LC&I proposed a strategy to improve the KYC and AML functions within LC&I. The strategy consisted of combining all of the KYC units within LC&I into one team. In addition, LC&I's AML unit would be subsumed into this team. The new unit would be responsible for all processes of customer on-boarding and off-boarding, including KYC and EDD. There was some internal disagreement regarding this proposal, but nevertheless, the proposal was implemented in Q4 2016.

Despite LC&I's effort to consolidate and streamline its KYC and AML processes, AML officers at the Baltic Subsidiaries continued to have problems liaising with their counterparts in LC&I. During an interview with Clifford Chance, a former LC&I KYC manager recalled that there were differences between how the two teams handled KYC analyses, but noted that LC&I started coordinating more with the Baltic Subsidiaries after noticing occasions where LC&I rated a customer as high risk, but Swedbank Estonia had rated the same customer as low risk. According to the LC&I manager, although LC&I and the Baltic Subsidiaries aspired to have one KYC procedure for common clients at the Group level, that goal was never fully achieved.

A GIA audit report issued on 5 October 2016 highlighted this issue, stating that AML & KYC processes for LC&I in the Baltics required "*Major Improvements*." The audit found that, while LC&I had restructured its AML process in 2014, LC&I had not ensured that the KYC process was appropriately established in the Baltic Subsidiaries. For example, the audit found that the Baltic Subsidiaries had not sufficiently implemented the LC&I manual for AML and CTF (including its KYC processes and principles), and transaction monitoring for LC&I customers in the Baltics did not incorporate appropriate monitoring scenarios or sufficient audit trail, thus risking noncompliance with internal and local regulatory requirements.

GIA summarized these findings in its Q3 2016 reports to the Swedbank Board and its Audit Committee in late October 2016. The reports noted that "*processes have not been adequately designed and implemented*," which "*could prevent Swedbank['s] ability to adequately prevent money laundering and terrorist financing in the Baltic jurisdictions, lead to regulatory sanctions and elevate reputational risk*." Minutes from the Board meeting on 24 October 2016 identify the "*AML Transaction Monitoring System*" and "*AML/KYC Processes in LC&I in the Baltic Countries*" as being "*Main Theme Areas*" for the third quarter of 2016. Minutes from the Audit Committee that same day reflect discussion of the October 2016 audit; specifically, that the audit had "*revealed that the root cause of the identified room for improvements is lack of well-functioning co-operation between LC&I in Baltic Banking, Compliance Baltic Banking and LC&I in Sweden*." The minutes noted an instruction that "*[t]he respective legal entit[ies] need to take their responsibility for KYC*."

GIA closed its finding with respect to KYC processes in December 2017, but its finding with respect to transaction monitoring remained open until 30 April 2019.

Other GIA audits in late 2016 found that "*Major Improvements*" were required for both sanctions screening and KYC renewal in the Baltic Subsidiaries. On 27 December 2016, GIA issued an audit report finding deficiencies in manual sanctions screening while the implementation of an automated screening tool, ProScan, remained ongoing. Specifically, the report's findings included delays of over a month in the updating of EU and OFAC sanctions lists; outdated guidelines for when to stop or release transactions; inaccurate or incomplete audit trails showing the investigation of stopped transactions; and problems in the implementation of fuzzy logic in ProScan. GIA closed each of these findings during April and May 2017.

GIA referred to the payments screening audit in its Q4 2016 reports to the Swedbank Board of Directors and its Audit Committee. The reports referred to GIA's conclusion that payments screening and monitoring at Swedbank "*required major improvements*," based on findings that (i) the sanctions screening list was not updated during October 2016 and this failure was not detected, (ii) audit trails did not completely document the handling of alerts, and (iii) its screening tool, ProScan, failed to capture misspellings of names of sanctioned individuals. The reports cautioned that "*[d]ue to these process gaps Swedbank faces an increased risk of violation of international sanctions and, without taking a timely corrective action, could face loss of relations with correspondent banks, losses, inquiries from the authorities and reputation damage*."

GIA presented its findings in meetings of the Board and Audit Committee on 1 February 2017. Minutes of the Swedbank Board indicate that "*Anti-Money Laundering*" was the "*main theme area[]*" of GIA's Q4 report, but otherwise reflect no reactions to the findings of the payments screening audit. Minutes of the Audit Committee reflect that the Committee, in reaction to the audit's findings, "*stressed that it is important that [screening] is working properly both from a Financial Supervisory Authority perspective, and a customer perspective*."

Internal Deliberations Regarding Lithuanian Company

During 2016, at the same time that GIA was identifying deficiencies in AML, KYC and sanctions compliance processes for LC&I in the Baltics, Swedbank LC&I was engaged in internal deliberations about the appropriate risk assessment for a customer of Swedbank Lithuania, which also had accounts with LC&I. This customer was a Lithuanian company (High Risk Customer 4, or **"HRC-4"**), with subsidiaries in the Baltics.

LC&I had concerns about HRC-4 as early as 2015, when LC&I employees identified AML and sanctions risk from HRC-4's connections with Russian PEPs and an OFAC SDN, who was a board member for HRC-4's Russian majority owner. In August 2015, a KYC analyst at LC&I noted that HRC-4 and its subsidiaries in Estonia and Latvia (which were also customers of Swedbank Estonia and Swedbank Latvia) had connections to the Russian government and indirect links to high-level Russian officials. In light of this, the LC&I analyst applied a risk rating of *"unacceptable,"* and recommended that Swedbank end its relationship with these customers. The RM for HRC-4 at Swedbank Lithuania stated that although this was for the LC&I KYC Committee to decide, the RM would defend the customer relationship during the meeting. Subsequently, in November 2015, the LC&I KYC Committee approved the continuation of the customer relationship with HRC-4 with an assessment of *"high risk*."

In June 2016, a manager in LC&I had an email exchange with a KYC employee in Baltic Banking and the RM for HRC-4 at Swedbank Lithuania. The LC&I manager explained that HRC-4 *"was referred to [LC&I] by Baltic Banking,"* but the LC&I RM

"is not comfortable with having [the RM's]name on it. The opinion . . . is that any press coverage of this relationship would look bad for Swedbank . . . and they would prefer to close the relationship [in LC&I]." After some discussion, they agreed that the RM at Swedbank Lithuania would prepare, by the end of the month, a memorandum setting forth HRC-4's *"Business case for [the] Baltics,"* addressing *"Group KYC, client profile,"* and explaining the necessity of HRC-4 banking with LC&I.

On 28 June 2016, the Baltic Banking KYC officer circulated to the LC&I manager, copying the RM, the business case memorandum for HRC-4, which assigned a "medium" risk rating to HRC-4 and its related entities because *"company activities are clear and transparent in the Baltic markets," and noted, "[t]he client team in the Baltics confirms that they have done full screening of the company fulfilling Baltic KYC requirements for [the] company and its subsidiaries in Estonia and Latvia. . . "* The memorandum explained that HRC-4 and its affiliates had been customers of the Baltic Subsidiaries for a significant period of time, and that the Baltic Subsidiaries helped to open accounts for HRC-4 and its subsidiaries at Swedbank several years earlier.. The memorandum also addressed why HRC-4's connections to a Russian national who was an OFAC SDN did not justify off-boarding: among other things, the SDN's membership on the board of HRC-4's majority owner did not make the SDN a beneficial owner of HRC-4, and HRC-4's majority owner was not itself an entity sanctioned by either the EU or OFAC.

In the email, the Baltic Banking KYC officer noted that the RM had discussed with a Baltic Banking senior manager the matter of *"'Russian risk appetite,'"* and that the Baltic Banking senior manager had advised the RM that *"there was a discussion on Group level on that topic with [the CCO]. It was noted that for Baltics we need some guidance on group risk appetite quite soon as Russian related customers are part of our business . . . [h]owever, I don't have any more specifics or timeline to give you right now."*

Notwithstanding the business case memorandum for HRC-4, LC&I employees continued to raise reputational and AML risk concerns with the relationship. Swedbank Lithuania responded by proposing to move the HRC-4 relationship from LC&I to the Baltic Subsidiaries. Some LC&I employees expressed concerns about this course of action, with one remarking that the RM appeared to want to take HRC-4 *"local"* in order *"to 'get out of' the [LC&I] KYC requirements."* Another LC&I employee expressed to an LC&I colleague that it *"would look very wrong if we put unacceptable risk here and the Baltic [Subsidiaries] chose to keep the customer."*

Despite these concerns, on 28 December 2016, LC&I made *"a final LC&I KYC decision . . . and the conclusion is: The customer is not compliant = exit / off-boarding in [LC&I] / on boarding in Baltics with the help of legal."* Accordingly, LC&I decided to (i) transition its relationship with HRC-4 to the Baltic Subsidiaries; and (ii) freeze all LC&I accounts with HRC-4 except for a trading account at LC&I. LC&I noted that this was not an off-boarding from Swedbank, but *"a transfer [of HRC-4] from LC&I to Baltic Banking, i.e. an internal reorganization."* At this time, an LC&I AML officer also noted that the *"[r]isk class [for HRC-4] is set as unacceptable by LC&I . . . due to missing full official documentation from the customer at the moment,"* including deficiencies in KYC documentation for one of the UBOs that held a significant minority share in HRC-4. These deficiencies in documentation were expected to be remedied by the customer.

After this decision, primary responsibility for resolving HRC-4's KYC deficiencies shifted to Swedbank Lithuania. In early 2017, Swedbank's CCO reiterated to Swedbank Lithuania the importance of obtaining adequate KYC information about HRC-4, noting that while the customer may be *"very profitable"* for Swedbank Lithuania, given that LC&I had deemed the customer an *"unacceptable"* risk, Swedbank Lithuania needed to obtain the missing customer documentation as a priority.

At around the same time, an LC&I employee prepared an assessment for Swedbank Lithuania regarding HRC-4, noting that Swedbank Lithuania must be able to show that it has *"the adequate tools, resources and the competence to handle and monitor"* the customer. LC&I appeared to have limited information about the nature of Swedbank Lithuania's existing relationship with HRC-4, however, noting that *"if Baltic Banking [has] a larger exposure [to HRC-4 than just LC&I's [account] . . . that must be taken in account in the [AML] analysis."*

While LC&I's decision to adjust its risk assessment of HRC-4 may indicate a maturing of Swedbank's risk appetite (at the time, an internal initiative led by Group Compliance to articulate a Group-wide risk appetite was underway, *see infra* at 143-44) the decision to transition the LC&I customer relationship with HRC-4 to the Baltic Subsidiaries appears inconsistent with applicable policy. At the time, Swedbank LC&I's AML Manual (adopted in January 2016) made clear that if *"any part of the risk assessment"* assesses *"the client or the business relationship . . . as unacceptable"* then the *"final assessment shall always be deemed unacceptable risk of [m]oney [l]aundering and the client shall not be approved or an already existing relationship shall, if and when possible, be terminated."* Although the manual did not explicitly address whether the termination of the customer relationship should be applicable to Swedbank and the Baltic Subsidiaries or only within LC&I, such ambiguity was emblematic of the lack of clear governance procedures.

Throughout 2017, Swedbank Lithuania attempted to obtain outstanding KYC information from HRC-4. While Swedbank Lithuania received assurances from the customer about the nature of the customer's ownership structure, it was unable to obtain sufficient supporting customer documentation. In late September 2017, the Swedbank CCO attended a meeting at Swedbank Lithuania to review customers, including HRC-4. The CCO noted during the meeting that the *"risk level and the corruption risk . . .is enormous here, and currently there are no solutions [on] how to mitigate it."* After further deliberations, the minutes of this meeting reflect that the participants decided to continue the relationship with HRC-4, subject to *"addi[tional] mitigation actions: (substitution, monitoring, needed resources),"* a *"communication plan with clear deadlines"* and an *"updated ECDD memo for the approval"* by the Swedbank Lithuania KYC committee.

In early 2018, Swedbank Lithuania attempted a *"soft exit"* from the customer relationship with HRC-4 and its related companies, to allow time for HRC-4 to find an alternative banking relationship. After these efforts were explored and rejected during the course of 2018, Swedbank Lithuania decided to maintain the relationship with HRC-4, and to focus on ensuring adequate EDD and transaction monitoring to manage the risk associated with the customer relationship which, given the AML remediation activities since implemented, the bank is now better equipped to do.

Conclusion of Panama Papers Investigation by the SFSA

On 23 December 2016, the SFSA issued a "*verification letter*" following its inspection of Swedbank's compliance with the Swedish Money Laundering and Terrorist Financing Act. Of the 30 customers for which the SFSA requested information, the SFSA found deficiencies in the KYC information for 12 customers. It assessed that "*Swedbank has collected limited information from the customer and that it is not possible to understand the company's purpose and type for the business relationship or what the customer's*

commercial activity is actually based on. Therefore, Swedbank was unable to carry out adequate Know-Your-Customer measures in order to reduce [its] exposure." The SFSA's preliminary findings also observed generally with respect to the 12 customers that:

> *[I]t is difficult to understand what enhanced Know-Your-Customer measures Swedbank uses based on the cases where the bank considers the customer high risk. The bank does not adequately analyze the know-your-customer information that the bank collects and assesses the customer on the basis of this analysis. Although it is possible to register different Know-Your-Customer information in the bank's Know-Your-Customer system, Swedbank's employees do not seem to make use of the possibility.*
>
> *Moreover, the identified random checks demonstrate that Swedbank has not collected information about the origin of assets to an adequate extent or verified the customer's information in this respect.*
>
> *Based on what is indicated above, [SFSA's] preliminary assessment is that Swedbank has not taken enhanced Know-Your-Customer measures for any of the customers that the bank has assessed as high risk in accordance with chap. 2, §6 of the Anti-Money Laundering Act.*

HRC-1 was one of these 12 customers. The SFSA specifically noted in its verification letter that it "*appears as though the Bank has not assessed the risk associated with the fact that the customer's ownership structure changed strictly for the purpose of avoiding taxes*" and that "*Swedbank has not taken additional measures to reduce the bank's risk exposure to being exploited for money laundering*." The SFSA concluded by stating that after it had received Swedbank's comments it would issue "*an official opinion on the matter's further course of action.*"

Swedbank responded in writing to the SFSA's verification letter on 27 January 2017, and stated that as a general matter:

> *[the Bank] has adequate procedures and processes in its operations . . . a good understanding of the customer, as well as the purpose and type of the business relationship. In some of the cases of random checks, the purpose and type of the business relationship could have been documented more clearly, even if the purpose and type were clear to the Bank. With respect to the transactions that [SFSA] has used as examples, it is also the Bank's opinion that the measures that have been taken are adequately effective and that the assessments that the Bank has made about the transactions are relevant.*

Further, Swedbank stated that "*[i]f it is [the SFSA's] view that the Bank has failed to meet its obligations, any potential deficiencies, should be viewed as minor and/or excusable in consideration of the ongoing and planned measures outlined above*."

With respect to HRC-1, Swedbank provided a two paragraph response to the SFSA, with the first paragraph describing in general terms HRC-1's business and noting that "*[t]he bank has classified the customer as high risk based on country risk, complicated corporate structure and the products and services that are provided*," noting that "*[t]he transactions and the customer relationship are in the process of off-boarding.*" The second paragraph described Swedbank's understanding of the "*change in ownership structure*:"

> *As indicated in the Bank's Know-Your-Customer information, the Bank's understanding is that the change in the ownership structure was an adjustment to the proposed regulations in Russia and thus driven by changing tax regulations. The customer information that was received in this respect was*

clear and documented, which was why the Bank did not consider it necessary to collect additional information from the customer at the time. The information from the customer also included a legal opinion from a Russian law firm. Furthermore, the Bank also obtained general information about the Russian law proposal and what it entailed. It was the Bank's understanding that the change was made for the purpose of adapting the structure to new tax regulations and determined that the implemented change would not entail tax evasion. This assessment is the reason why the Bank did not see the need to ask further questions or request additional documentation.

As noted above, however, the substance of the legal opinion from the Russian law firm was perfunctory (conveyed in under 100 words), did not squarely address whether the ownership restructuring was permissible tax avoidance rather than tax evasion, and instead opined only "*that no tax consequences arise for [the former majority owner] in connection with the Transaction.*" The Investigation's review of the HRC-1 KYC files provided to the SFSA in connection with the 3 June 2016 response found no evidence that Swedbank had provided a copy of the Russian law firm's legal opinion, nor that Swedbank provided a copy in connection with its 27 January 2017 response.

The CCO supervised the drafting of this response to the SFSA. Swedbank began preparing comments to the SFSA's verification letter by first preparing a memorandum outlining a proposed response. As discussed below, between 29 December 2016 and 27 January 2017, employees within Compliance, including the CCO, as well as LC&I employees, reviewed and revised the draft memorandum.

At the outset, an LC&I employee sent an email to LC&I Compliance employees on 30 December 2016, explaining that, in preparing the response to the SFSA's preliminary findings, "*[w]e shall 'defend' ourselves, i.e. attempt to show explain [sic] that we, in our opinion, fulfilled the requirements that are made on purpose and type. . .*" The LC&I employee also added that "*for [HRC-1] . . . just write the current situation, we don't need to defend [ourselves].*"

A memorandum prepared by Swedbank Compliance, dated 11 January 2017, conveyed that Swedbank was comfortable with the documentation and analysis of the HRC-1 restructuring, setting out that "*the bank's stance (via Group Tax) [is] that we are comfortable with the arrangements because there is transparency towards tax authorities [and] the arrangements fall within the scope of double taxation agreements.*" The memo noted, "*[SFSA] may criticize that we have not documented the purpose of the arrangement sufficiently well.*"

In a 24 January email, an LC&I manager involved in reviewing the draft response expressed concern to a Group Compliance employee (also involved in reviewing the response), stating: "*I think we're being a bit aggressive when we want to point out that we're completely compliant, considering how it looks.*" The LC&I manager attached a mark-up of the draft response, which flagged the statement that Swedbank has "*a good understanding of the customer, as well as the purpose and type of the business relationship*," with the following comment: "*I think this is a pretty strong statement in consideration of what is hiding behind [HRC-1] . . . . What is our thinking here?*" The LC&I manager flagged the next statement, "*[w]ith respect to the transactions that FI has used as examples, it is also the bank's opinion that the measures that have been taken are adequately effective and that the assessments that the Bank has made about the transactions are correct*," with the comment "*same here*." The Group Compliance employee responded the same day, encouraging the LC&I manager to raise this concern and explaining that the strategy being pursued was to avoid admitting any shortcomings.

On 25 January 2017, the Group Compliance employee sent the draft of the response to the Swedbank CEO, to the Communications Department, and to the Legal Department

requesting "*feedback as soon as possible*." The same day, the CEO's assistant responded on behalf of the CEO to the Group Compliance employee, stating that the "*[CEO] has looked at the document and thinks it is OK*."

On 26 January, the Group Compliance employee then wrote an email to the CCO to provide feedback on the draft response, stating that:

> *We know that we have deficiencies concerning a number of customers, which we also state under each respective customer, if not very clearly. . . . There should be an understanding . . . that there will always be the odd deficiencies on a customer level. There is a risk that we, in a possible continuation of the review, are unable to live up to what we now write in the replies. I know that you don't want to admit to any deficiencies, as we did in the previous review [by the SFSA in 2014]. But would still like to suggest alternative wording if we are to reply more similarly to the reply of the previous review. [These] are found in the comments in the margin. Naturally, you choose which way for us to take, the comments are merely suggestions.*

The "*comments in the margin*" however, did not include the comment raised by the LC&I manager ("*I think this is a pretty strong statement in consideration of what is hiding behind [HRC-1] . . . What is our thinking here?*"), nor do the comments in the margin to this section, or any other section of the draft response, include any similar concerns. The comments did include, however, a recommendation not to reference the legal opinion from the Russian law firm concerning HRC-1, stating "*the legal opinion referred to does not support our assessment . . . . It may be difficult to explain [in case the SFSA] requests [it].*"

Also on 26 January, the LC&I manager wrote to the Group Compliance employee that the LC&I manager had had a call with the CCO to raise the concerns expressed in the LC&I manager's email and mark-up of 24 January. The Group Compliance employee responded that the updated conclusion to the response, from the CCO, represented an improvement and better reflected the situation.

The 27 January 2017 response that the CCO submitted via email to the SFSA was signed by the CEO. The final version of the response reflected that the word "*correct*" in the 24 January draft version of the following statement was changed to "*appropriate*" as follows: "*With respect to the transactions that FI has used as examples, it is also the bank's opinion that the measures that have been taken are adequately effective and that the assessments that the Bank has made about the transactions are appropriate.*"

The Investigation found no evidence that the concerns raised by the LC&I employee regarding the content of the draft response were shared with the CCO. The Investigation also did not identify any evidence that the CCO made any changes to the draft response to address the comments provided by the Group Compliance employee. The 27 January 2017 response that the CCO submitted via email to the SFSA was signed by the CEO.

At a 1 February 2017 Swedbank Board meeting, the Swedbank CCO presented the Q4 2016 Compliance Report and informed the Board that Swedbank had received "*preliminary views*" from the SFSA's Panama Papers investigation, including a finding of "*deficiencies related to [KYC] practices and actions regarding high risk customers, including the transaction monitoring*." The CEO Report provided to the Board includes the same language as the CCO report but also adds that an "*answer has been made in dialogue with business and will be submitted to the CEO for sign-off prior to submitting it.*"

The Board received a further update from the CCO about the SFSA's findings at a 23 March 2017 meeting. A 23 March 2017 "*Summary of regulatory contacts*" report prepared for the Board and included in the Board meeting materials, noted that Swedbank had informed the SFSA that "*due to the planned actions and the actions already taken by the bank, any alleged breaches should be considered as actions of minor importance and hence argued that the matter should not be handed over for a sanction process*." The CCO update did not provide any other details regarding Swedbank's 27 January 2017 response to the SFSA.

On 14 November 2017, the SFSA closed its investigation without "*additional measures.*" In its 14 November 2017 letter to the Bank, the SFSA noted that it had "*identified potential threats and risks to the Bank . . . because of the way [it handles] money laundering and terrorism financing matters*" and added that "*the [SFSA] will follow up within the scope of supervision to determine how the Bank views the weakness and deficiencies that [the SFSA] identified and how they are handled*."

The CCO updated the Board on the outcome of the SFSA investigation at the 5 February 2018 Board Meeting with the minutes stating that the "*Panama Papers [investigation] had been closed with some identified deficiencies by the SFSA*." The CCO also provided the Board with the Compliance Report for Q4 2017, which noted that:

> *The investigation by the SFSA regarding 'Panama Papers' was closed on 14 November 2017; however the SFSA has identified deficiencies in the bank's ability to comply with the regulations regarding AML/CTF. Several measures have been proposed, however no further actions will be conducted by the SFSA in the scope of the investigation. [Swedbank] is expected to regularly report on the progress to the SFSA. Swedbank Compliance will follow up on respective BA level what extra measures they propose as a result of the proposed actions and will continue with investing in advice and support to the respective BA.*

The Board minutes do not reflect any other discussion about the SFSA investigation or its findings.

A few months prior to the closure of the SFSA's Panama Papers investigation, Swedbank adopted its first risk appetite statement, an effort that was related to the response to the SFSA investigation and the attention surrounding the release of the Panama Papers. In its 21 June 2017 AML/CTF Policy, Swedbank defined its risk appetite as follows:

> *Neither the Bank nor any of its Subsidiary [sic] shall tolerate Money Laundering or Terrorist Financing, and it will not knowingly conduct business with individuals or legal entities it strongly believes to be engaged in such inappropriate behaviour. This means that the Group:*
>
> - *will not operate any line of business or do business with any customer segment where the residual risk for Money Laundering or Terrorist Financing exceeds the risks that are acceptable for achieving the strategic goals of the Group, having duly considered the Group's control environment, and*
>
> - *will normally not do business with any customer(s) or customer segments where the inherent risk for Money Laundering or Terrorist Financing is high unless it has appropriate controls to mitigate exposure to a moderate level of residual risk.*

The 21 June 2017 AML/CTF also provided that Swedbank would document its processes for assessing the effectiveness of its mitigation measures, in order to ensure that any residual AML/CTF risk was consistent with the Group's risk appetite. In 2018, this risk appetite statement was formally implemented by the Baltic Subsidiaries, which adopted

a risk assessment methodology requiring customer risk to be within the risk appetite as "*defined in the Group AML Policy*" and to be calculated taking "*into account the geography, customer profile, product/services/transactions and channel's view*."

4. 2017 – 2019: Swedbank Investigates and Remediates AML Deficiencies in the Baltic Subsidiaries

Reviews by Swedbank and External Consultants Identify Extensive AML Deficiencies in the Baltic Subsidiaries

In late December 2016, Swedbank engaged an international consulting firm (the "**Consulting Firm**") to review AML processes in the Baltic Subsidiaries. The decision to hire a third party to carry out this review was prompted, in part, by recent regulatory investigations, including the sanction by the Latvian FCMC.

In early January 2017, the Consulting Firm began its review, which involved comparing each Baltic Subsidiary's AML procedures and practices to (1) the local AML laws and regulations for each respective country; and (2) international standards, as defined by sources such as FATF Recommendations and the Wolfsberg AML Principles.

In January and February 2017, the Consulting Firm conducted interviews with relevant employees, reviewed AML-related policies and procedures, and assessed KYC documentation for a sample of 30 customers from each Baltic Subsidiary. The customer samples were selected using "*commonly recognized money laundering risk factors*" such as PEP status, industry, account turnover, geography and Swedbank risk rating. While there were some low-risk customers included in the samples, the majority were considered high risk. The Swedbank Estonia sample included four HRC-1 Group customers.

The Consulting Firm delivered its final report to Swedbank in March 2017. This report was shared with the CCO and with senior managers in Baltic Banking, the Baltic Subsidiaries, and Group Compliance, among others. The Consulting Firm's report outlined a number of "critical" and "*significant*" findings related to KYC, customer risk scoring, transaction monitoring and reporting, risk assessment, resources, and training. Notable findings for all three Baltic Subsidiaries included the following five points:

- Verification of beneficial ownership and source of wealth for high risk customers was mainly based on information received from the customer rather than data from verified sources.
- Risk assessments were general in nature, not supported by a comprehensive analysis of the Baltic Subsidiaries' exposure to the identified risk factors, and did not identify whether there are other risk factors that should be considered.
- Customer risk scoring models were simplistic and "*inhibit [the] identification of 'high risk' clients and escalation of their acceptance*."
- Transaction monitoring processes were manual and ineffective, creating a high risk that suspicious transactions were not detected.
- There were not enough personnel dedicated to AML compliance to handle the current or anticipated workload.

A CEO report to the Swedbank Board of Directors noted that the Consulting Firm's report "*sets out gaps vs international standard as well as local standards in each of the Baltic countries*," and opined that a detailed study of the report was needed, together with an action plan. This CEO's report was included on the agenda and in the packet for the Board of Directors meeting on 23 March 2017, but the minutes did not reflect any discussion of or reaction to the CEO's description of the findings. The CCO later briefed the Audit Committee of the Swedbank Board on the Consulting Firm's findings at a 24 April 2017 meeting. According to the minutes from this meeting, the CCO

informed the Audit Committee that the review had identified "*major gaps related to risk assessments, monitoring, due diligence, IT Screening tools for transaction monitoring, resources, training and framework and feedback, [and that] all the identified issues are part of the Baltic AML Programme*."

The minutes reflect that the CEO also attended this Audit Committee meeting, and that when asked about AML efforts at Swedbank, the CEO reported that "*[t]here are not many such businesses [referring to non-resident business] in Estonia, they have been cleaning up*," and that "*Lithuania will need to take action*." The CEO also referred to "*the AML Programme in the Baltics and a specific AML project in Estonia [that] reports directly to the CEO*." Although the minutes do not reflect any further discussion about the nature or work of this "*specific AML project*," it appears to be a reference to an internal review and off-boarding effort being conducted by Swedbank at the time to address the risks associated with the HRC-1 Group in Estonia. Swedbank referred to this work as "*Project Clear*."

Project Clear and Related Updates to the Estonian Authorities

In January 2017, Group Compliance decided to engage an external firm to assist in the off-boarding of the HRC-1 Group, and to assess related AML risks and employee conduct issues at Swedbank Estonia. The impetus for Project Clear came from several factors including the decision by LC&I and Swedbank Estonia to terminate the customer relationship with the HRC-1 Group, the Panama Papers-related inquiries by the EFSA and SFSA in 2016, the FCMC investigation in Latvia, and the Financial Conduct Authority's notice to a correspondent bank in January 2017 "*explicitly referr[ing] to suspicious transactions having links to Estonia.*" In early February 2017, Swedbank engaged a Norwegian law firm, Grimstad AS, to perform this review. Grimstad AS was retained to assist Swedbank in, among other things, identifying affiliates of the HRC-1 Group to facilitate the off-boarding of these entities. Ultimately, approximately 210 then-current customers were identified and off-boarded in connection with Project Clear by July 2017.

In January 2017, Grimstad AS had an initial meeting with Swedbank's CCO. Soon after Grimstad AS was formally engaged, responsibility for leading the project shifted to the CRO because the CCO was concerned about potential conflicts of interest that might arise from overseeing a project that would examine prior conduct by Compliance personnel. However, the CRO, who had previously been a senior manager at Swedbank Estonia with responsibility for the relevant business unit, was removed from Project Clear due to a potential conflict of interest. Project Clear was then overseen by senior managers from Group Risk and Group Information Security. Grimstad AS's primary contact remained a senior member of the Group Compliance team. Swedbank's CEO also received weekly briefings and status update memoranda regarding the project.

Grimstad AS's primary task was to identify customers for off-boarding through analysis of suspicious activity and identification of links between customers. Grimstad AS did not conduct a full assessment of historical AML deficiencies at Swedbank Estonia. Due to limitations in time and personnel, Grimstad AS also did not conduct an investigation of employee conduct issues or managerial failures, nor did it conduct a comprehensive review of the adequacy of KYC documentation. While Grimstad AS did prepare preliminary observations about AML risk and employee accountability issues that it identified during its work, it did not provide any specific recommendations about employee culpability or suitability. For example, in June 2017 a member of Grimstad AS's team prepared a preliminary assessment for Swedbank of the conduct of certain Swedbank Estonia employees, which observed that Swedbank Estonia's senior management had not adequately understood the risks associated with the HRC-1 Group, and had failed to fulfill AML obligations. Grimstad AS also observed, however, that while this preliminary assessment had "*not found any one criminal act purported by any one member of the management of [Swedbank Estonia]*," there had been, "*to different degrees*," a collective failure to adhere to adequate AML standards.

Information about Project Clear was kept within a limited group of people while the Project was ongoing. When interviewed for the Investigation, neither members of the Swedbank Board, nor members of the Management Board or Supervisory Council for Swedbank Estonia, recalled being briefed about the work while the Project was ongoing. Other than the CEO's generic reference to "*a specific AML project in Estonia*" in the minutes of the 24 April 2017 meeting of the Board's Audit Committee (discussed above), the Investigation has not identified any evidence that Project Clear was reported to the Board before April 2019, when the full Swedbank Board was informed of the existence of Project Clear.

Beginning in February 2017, the Swedbank Estonia CEO was asked to assist and support the off-boarding of the HRC-1 Group in connection with Project Clear, but did not receive the written reports from the Project. However, the Swedbank CEO did discuss some aspects of the Project with the Swedbank Estonia CEO.

The Estonian FIU was first briefed in February 2017 about the ongoing review of the HRC-1 Group and the off-boarding of that customer relationship. Contemporaneous internal communications reflect that a senior manager in the Legal Department, a Swedbank Estonia Compliance officer, and a senior manager in GSI met with the Estonian FIU in February 2017, and provided the Estonian FIU with an overview of the HRC-1 Group and their activity. In addition, they "*also confirmed that there ha[ve] not been any negative signals from the client or related persons so far.*" In a suspicious transaction report("**STR**") filed with the Estonian FIU, Swedbank Estonia noted that the Russian oligarchs associated with HRC-1 were "*possibly PEP[s]*" with "*close business relations*" with one of the beneficial owners of HRC-1 and were also the "*beneficial owners of more than 200 offshore entities who are or [were] clients of Swedbank Estonia*".

In April 2017, Swedbank Estonia's CEO (along with a senior employee from Group Compliance who was involved with Project Clear, and a manager from GSI) met again with the Estonian FIU. During the meeting, they briefed the Estonian FIU on the Estonian Management Board's decision in 2016 to de-risk the HRNR segment, and also provided an overview of the measures being implemented to review transactions by the HRC-1 Group.

That same month, Swedbank Estonia responded to a series of EFSA questions about its AML compliance procedures in relation to non-resident and other high risk customers. Swedbank Estonia's 12 April 2017 response (signed by the Swedbank Estonia CEO) provided a chronological overview of the Management Board's decisions in 2016 to limit and downsize its non-resident business, and discussed a number of pending initiatives to mitigate AML risk. The 12 April 2017 response to the EFSA did not refer to Project Clear explicitly, but did inform the EFSA about certain actions related to the HRC-1 Group, including: the decision of Swedbank Estonia in late 2016 to terminate the relationship with all HRC-1 Group companies; an analysis of the 50 Swedbank Estonia non-resident customers with the highest turnover that found that most of these customers were related to the HRC-1 Group; and additional scrutiny of HRC-1 Group transactions in light of the Russian Mirror Trades scheme.[42] Further, as previously noted, the 12 April 2017 response mistakenly reported that Swedbank Estonia had 29 customers with links to Mossack Fonseca, without accounting for additional customers identified in May 2016 (*see supra* at 97). The 12 April 2017 response also included a presentation of the HRC-1 Group and named several Russian oligarchs (including the ones discussed in February 2017 with the FIU) as main UBOs of the HRC-1 Group.

[42] The Russian Mirror Trades was a scheme that involved $10,000,000,000 in funds laundered out of Russia using the Moscow and London branches of an international financial institution. As part of the scheme, Russian customers of this financial institution would purchase securities in rubles through the bank's Moscow office. Shortly thereafter, a related counterparty would sell identical stocks at the same price in foreign currencies, including US dollars, through the bank's London office. The selling counterparty would typically be registered in an offshore jurisdiction, and the trading activity lacked any apparent legitimate economic rationale.

On 28 June 2017, the Swedbank Estonia CEO and two members of the Project Clear leadership team, gave a presentation to the EFSA on the HRNR segment. Although the presentation did not refer to Project Clear or to the HRC-1 Group specifically, it did cover the status of the HRNR de-risking, noting that from the end of August 2016 through the end of May 2017, the number of open accounts for HRNR customers in Estonia went from 655 to 139, and total deposits declined from 7.24% to 0.51%.

Grimstad AS Findings on Project Clear

Grimstad AS delivered its findings on Project Clear in a draft report to Swedbank in July 2017 titled "*Focus Clients AML Investigation*." This memorandum was only shared with a select group of individuals from Swedbank, all of whom were part of the Project Clear leadership team.

Grimstad AS found that Swedbank Estonia's deficient AML processes and weak compliance culture increased the risk that Swedbank Estonia was used to facilitate money laundering by the HRC-1 Group. Swedbank Estonia had "*made such transactions possible by giving the clients the opportunity to transfer significant amounts in different currency to bank accounts controlled by straw men of offshore entities, without fully understanding the real nature of [the] business, the interests beyond transactions or questioning the source of funds*." Grimstad AS also identified "*no real signs . . . of an efficient risk based approach*." Additionally, members of Swedbank Estonia management involved in AML processes for the HRC-1 Group did not have a firm understanding of their roles and responsibilities, which led to a "*lack of proper monitoring and oversight of [Swedbank Estonia's] AML obligations*."

Grimstad AS found that transaction monitoring and customer on-boarding were the primary deficiencies in Swedbank Estonia's AML framework. With respect to transaction monitoring, Grimstad AS "*found no evidence of any proper investigation of suspicious transactions [pertaining to the HRC-1 Group] in the reviewed period from 2012*" through February 2017. While Swedbank Estonia did conduct transaction monitoring for HRC-1 Group customers on a weekly basis, the analysis gave "*the impression that all these efforts were done more or less as a 'tick in the box' exercise with no real understanding of the aim or the purpose of the AML requirements*." The report also found that up to and until the off-boarding of HRC-1 Group customers in 2017, no suspicious transactions related to the HRC-1 Group were ever reported to the Estonian FIU, despite evidence of suspicious activity.

Regarding customer acceptance, Grimstad AS noted that: *"[t]he due diligence of new clients was inadequate and [Swedbank Estonia] failed to obtain sufficient information about the client and its business . . . [which] should have led to the decision not to accept the client*." New customers were often accepted despite their refusal to provide necessary documentation, and new accounts were opened without any information regarding the source of funds. Further, "*[s]everal of the Senior Managers in [Swedbank] Estonia had knowledge of the [HRC-1 Group] and their refusal to provide [Swedbank Estonia] with documents, e.g. shareholder agreements, signed documents of ownership and proper documentation of links between entities*" and purported beneficial owners.

In its report, Grimstad AS did recognize that Swedbank Estonia had engaged in a series of risk mitigation and remediation efforts since 2016. Grimstad AS also stated that "*there is no concrete evidence*" that the transactions for the HRC-1 Group had "*a direct link to proceeds from identified criminal actions*."

In addition to these findings, Grimstad AS also examined instances in which Swedbank Estonia had maintained relationships with customers with links to certain well-publicized money laundering schemes. These schemes included the Magnitsky

scheme, Russian Mirror Trades, and illegal arms trading. Grimstad AS recommended further investigation of these connections and reporting to the FIU where appropriate.

These findings included:

- *The Magnitsky Scheme.* Three customers of Swedbank Estonia had transactions totaling over $2.5 million with a company alleged to have received funds related to the fraud. Another Swedbank Estonia customer was connected to this counterparty through its corporate shareholder.
- *Russian Mirror Trades.* Five customers of Swedbank Estonia transacted with entities linked to the Mirror Trades scheme. A general power of attorney for another Swedbank Estonia customer appeared to be signed by a person also linked to the Mirror Trades scheme.
- *Latvian Proxy Networks.* These proxy networks, reportedly run by Latvian nationals, utilized nominee directors or shareholders to obscure the true beneficial ownership of entities. At least one customer of Swedbank Estonia had transactions with a counterparty that was controlled by an entity that used individuals connected to a well-known proxy network as directors.

Project Clear Findings are Reported to the CEO and CCO

The findings from Project Clear were summarized for the Swedbank CEO in an internal memorandum prepared by a senior manager in Group Risk (with input from a senior employee of Group Compliance and other members of the Project Clear team) ("**Memorandum Project Clear**"). In July 2017, Memorandum Project Clear was submitted to the Swedbank CEO (and shared by email with the Swedbank CCO and members of the Project Clear leadership team).

The findings in Memorandum Project Clear were divided into two sections: (1) a review of AML risk arising from the activities of the HRC-1 Group; and (2) a review of potential wrongdoing by Swedbank Estonia employees. The language and conclusions in the first section largely mirrored those from Grimstad AS's memorandum, as the authors of the memorandum relied on Grimstad AS's report while drafting Memorandum Project Clear.

Regarding the second section (which was not discussed in Grimstad AS's July 2017 report) Memorandum Project Clear did not identify any evidence of criminal conduct by any Swedbank Estonia employees. The review found no evidence that employees had received kickbacks from HRC-1 Group customers. Nor were there "*external ties between employees and the [HRC-1] Group*." However, the report did find that Swedbank Estonia's senior management "*collectively failed to act to protect [Swedbank Estonia] and to comply with [Swedbank Estonia's] legal obligations*." Specifically, the report concluded that "[*s]enior management ha[d] not fulfilled its express obligations in key areas of responsibility related to anti-money laundering[,] . . . ha[d] not promoted a culture of competence, transparency and trust in relation to AML obligations[,] . . . [and this] failure to comply ha[d] been ongoing throughout the whole period of review (2012-2016).*"

As to whether Swedbank Estonia employees knew about irregularities in the customer information for HRC-1 Group entities, Memorandum Project Clear noted that: (1) the HRC-1 Group entities set up in Cyprus were owned by entities in the British Virgin Islands to "*hide the names of the real owners*"; (2) "*[o]n paper*" there were no links between HRC-1 Group entities and their UBOs – rather these links were established based on information provided orally by contact persons for the HRC-1 Group, as well as the "*interpretation of transactions, historical cash flow, and counter parties*"; and (3) the vast majority of these entities had nominee shareholders. Moreover, members of Swedbank Estonia's Management Board were aware of the HRC-1 Group's refusal to provide necessary KYC documentation.

The primary RM for HRC-1 Group left Swedbank Estonia shortly after Project Clear began. Nonetheless, the Investigation identified email communications from the HRC-1 Group RM that showed an awareness that certain transactions were suspicious. For example, the HRC-1 Group RM referred on 10 August 2015 to information provided by a customer regarding the purpose of a transaction as a "*fairy tale,*" and suggested that the customer could be presented to the HRCAC as member of the HRC-1 Group. A subsequent investigation by Swedbank Estonia determined that, after leaving Swedbank Estonia, the former HRC-1 RM went to work for an entity associated with HRC-3.

Memorandum Project Clear concluded with the following recommendations for improving Swedbank Estonia's AML compliance culture and processes:

- all circumstances associated with legacy business culture (*e.g.,* complex customer structures, difficulties confirming an entity using open sources, close connections between businesses and the owner's private wealth, etc.) should be flagged and questioned;
- a formal AML strategy should be developed and updated;
- the Supervisory Council for Swedbank Estonia should approve and oversee its AML risk policies and request quarterly reports from the CEO of Swedbank Estonia highlighting improvements made and further actions needed;
- an updated and factual AML Risk Assessment should be prepared;
- Swedbank Estonia should provide periodic AML training for leaders, AML compliance staff, RMs, and other relevant staff, tailored to their roles and responsibilities;
- GIA should be committed to conducting an internal audit program that tests the effectiveness of the AML program and compliance with AML and sanctions regulations and laws;
- Swedbank Estonia should conduct a thorough review of the weaknesses identified during the Project Clear AML investigation.

A preliminary draft of the memorandum contained a recommendation to "*[e]nsure [Swedbank's] Board of Directors, executives and relevant supervisors are informed of the risks concluded from the AML investigation and understand the challenges and the need for changes as described to ensure compliance with rules on combating money laundering.*" The draft was circulated in early-July 2017 to the Swedbank CEO, who met with several employees involved in the project to discuss the draft memorandum. When interviewed for the Investigation, a Swedbank Group Compliance employee involved in drafting the memorandum stated that the CEO had requested the removal of the recommendation to inform the Swedbank Board about the findings of Project Clear. However, in an interview, the then-CEO asserted that there had never been any recommendation to report the findings to the Swedbank Board; rather the intent was always to handle the issues at the Swedbank Estonia level.

Following the meeting with the Swedbank CEO, the Swedbank Group Compliance employee and the CCO exchanged emails about how to phrase the recommendation regarding Board reporting. The Swedbank employee later circulated a final version of the memorandum to the Swedbank CEO and CCO on 7 July 2017, noting that the revision "*[p]oints to the [Swedbank Estonia Management Board] in general and leaves open the question of how to handle the info.*" The final version amended the relevant provision to read that "*the board of directors in Swedbank Estonia should have a clear understanding of the AML risks,*" and did not reference informing the Swedbank Board about Project Clear.

When interviewed for the Investigation, the then-CEO recalled having a brief discussion about Project Clear with the then-Chair of the Board, around the time when Memorandum Project Clear was finalized. However, when interviewed, the now-former Chair denied ever discussing Project Clear with the then-CEO. Although the Memorandum Project Clear was delivered to the Swedbank CEO, neither the Swedbank Board nor the full Swedbank Estonia Management Board or Supervisory Council were apprised of the existence of Project Clear or its findings until 2019.

The Board did, however, receive updates from Swedbank management during 2017 about off-boarding efforts in the Baltic Subsidiaries. For example, a CEO Report provided to the Board on 23 March 2017 projected that by the end of Q1 2017, Swedbank Estonia would reduce its number of HRNR customers to 317, and that notices of closure had been given to another 62 companies. The report also indicated that Swedbank Latvia had off-boarded 420 HRNR companies out of 434 and that the remaining entities would be closed "*within [the] near . . . future*."

GIA was also not informed about Project Clear, even though the Memorandum Project Clear recommended that GIA test the effectiveness of Swedbank Estonia's AML program.

Given the significance of Project Clear, the failure to escalate its findings to the Swedbank Board, or to report the findings to GIA, was a significant governance failure. The failure to inform the Swedbank Board denied the Board full visibility into the extent of Swedbank Estonia's AML deficiencies and attendant legal risks for Swedbank. Similarly, the failure to inform the Swedbank Estonia Management Board or Council impeded their ability to ensure compliance with their responsibilities.

Conclusion of Project Clear and Follow-On Actions

Grimstad AS's work on Project Clear ended after the delivery of its draft report in July 2017. Grimstad AS did not receive any substantive feedback from Swedbank following delivery of that report. Although Grimstad AS had offered to assist on subsequent remediation efforts and assess Swedbank's AML policies, procedures and practices as a separate phase of work, the CCO informed Grimstad AS during summer 2017 that Swedbank would instead perform that work itself.

Project Clear ultimately identified 208 then-current customers of Swedbank Estonia that were related to the HRC-1 Group, and off-boarded these customers. According to internal bank records, 207 of the customers were off-boarded by July 2017, and the remaining customer has a blocked securities account.

Swedbank Consolidates its AML Structure in GSI

While Project Clear was ongoing, a proposal was developed by Group Compliance, Group Risk, Group Information Security, and the Swedbank CEO Office to create a single, group-wide unit to combat financial crime. In April 2017, this proposal was presented to the GEC, with the following primary reasons for establishing this unit: (1) a rise in financial crime; (2) more stringent AML regulations; and (3) increased expectations from regulators related to transaction monitoring and group-wide investigative capabilities. The Group's AML structure and defense systems in place at the time were found to be too dispersed and localized to effectively address these developments. Thus, a more efficient and centralized organization with increased cooperation at the Group level was needed. The GSI proposal was accepted by Swedbank senior management, and, in July 2017, an acting head of the new unit was appointed to implement the proposed mandate.

The new unit became known as GSI, and was intended to be a first-line unit responsible for AML, financial fraud investigations, transaction monitoring, financial sanctions screening, reporting to FIUs, and physical security. GSI reported to the CEO Office and had direct reporting lines to local units in the Baltic Subsidiaries.

Almost immediately after being formed, GSI began to work with Group Compliance to conduct follow-up analyses based on Project Clear and the observations of Grimstad AS, such as examining potential connections between existing customers and entities off-boarded due to affiliation with the HRC-1 Group. As part of this analysis, Group Compliance identified that certain customers at Swedbank Estonia had utilized a form of legal entity, a Swedish *Handelsbolag*[43] ("**HB**"), that had "*no business activity identified in Sweden or abroad*" and "*known proxy/nominee Directors, some linked to several of hundreds of other companies as well as linked to other existing clients in Estonia.*" In October 2017, a follow-up GSI analysis described this HB structure as possibly designed to obscure the true ownership and tax residency of the customer, and identified 14 customers at Swedbank Estonia (including 11 HB entities and two related entities) for off-boarding. These customers included one entity that Swedbank Estonia assessed to be essentially the same customer that it had off-boarded in December 2016 due to being an HRNR customer, but which remained a customer of Swedbank Estonia in the form of an HB entity (with the same name).

Resourcing for GSI continued to be a challenge. On 27 October 2017, GSI informed Swedbank senior management that maintaining support for GSI was essential for Swedbank's compliance with applicable legislation, and warned that any delay in adding resources could increase the chances of fines from the SFSA. In December 2017, GSI informed the CEO office that existing GSI units suffered from a lack of funding and resources, and characterized this as a high risk. According to GSI senior management, all the GSI units needed investment both in human resources and in systems to alleviate manual processes. The required investments, especially in AML/CTF, were critical because without them, Swedbank could be deemed non-compliant with external regulations.

During a recent interview with Clifford Chance, a senior manager within GSI was critical of the amount of resources allocated to GSI. The lack of resources for GSI was a source of tension between the senior management of GSI and the CCO.

Mounting Media Scrutiny of CPB-1 Prompts Swedbank to Examine its own Customers

During 2017, media reports revealed potential instances of money laundering at CPB-1, and Swedbank began to conduct internal reviews to address its exposure to these issues. These media reports related to well-known money laundering schemes such as the Russian Laundromat and the Azerbaijani Laundromat. Swedbank's internal reviews of historical transactions by customers of the Baltic Subsidiaries with counterparties at CPB-1 identified AML risks similar to those that Grimstad AS had identified during Project Clear.

Russian Laundromat

In March 2017, while Project Clear was ongoing, the Estonian media reported that over $1 billion in funds linked to the Russian Laundromat scandal had flowed through CPB-1. According to media reports, the Russian Laundromat operated between 2011 and 2014 through the use of 21 primary entities registered in the United Kingdom, Cyprus, and New Zealand. These companies generated fake debts and then obtained a court order in Moldova requiring 19 Russian companies to pay these debts to financial institutions in Moldova and Latvia. Over $20 billion was allegedly moved out of Russia and into the global financial system as a result of this scheme.

Swedbank Estonia informed the EFSA in April 2017 that 21 of its customers were included in a list of companies that media reports had connected to the Russian Laundromat scheme. Swedbank Estonia also explained to EFSA that, following an internal analysis, it had decided to close the accounts of five of these customers due to suspicious transactions being identified in its analysis.

[43] A Handelsbolag is a form of partnership established under Swedish law.

Azerbaijani Laundromat

In early September 2017, the Danish news publication *Berlingske* reported that, between 2012 and 2014, certain wealthy Azerbaijanis had laundered approximately $2.9 billion through four UK entities with customer accounts at CPB-1, in what became known as the Azerbaijani Laundromat.

Following these media reports, Baltic Banking conducted a transaction analysis that indicated, between 2012 and 2017, customers of the Baltic Subsidiaries had performed approximately 50 transactions with the four main UK entities reportedly linked to the Azerbaijani Laundromat, and over 1,000 transactions with entities or individuals identified by the Baltic Banking AFCIS as related to the Azerbaijani Laundromat scheme. The results of the this review were provided to senior management of the Baltic Subsidiaries, and to the then-CEO. However, the Investigation did not find evidence that they were shared with the Swedbank Board.

Focusing on the four main UK entities identified in public media reporting, Swedbank Estonia identified three customers who performed four transactions with the named companies. After receiving an "*explanation and underlying documents*" for the transactions in question, Swedbank Estonia concluded that "*no negative information*" was obtained about the customers and the customers' activities were "*in accordance with Swedbank Estonia['s] risk appetite*." One of these customers was later off-boarded in 2019. The Baltic Banking review also determined that 98 unique customers of Swedbank Estonia (including 71 active customers) performed 390 transactions with entities or individuals identified by the Baltic Banking AFCIS as related to the Azerbaijani Laundromat scheme amounting to €5.4 million and $26.7 million.

Swedbank Lithuania identified two customers who performed two transactions with one of the main UK entities. After failing to receive underlying transaction documentation from one of these customers, Swedbank Lithuania blocked the account. The other customer provided an explanation and documentation that Swedbank Lithuania "*considered sufficient*." Swedbank Lithuania also identified 66 unique customers (including 62 active customers) that performed 388 transactions with entities or individuals identified by the Baltic Banking AFCIS as related to the Azerbaijani Laundromat scheme amounting to €11.4 million, and $178,000. A total of 349 of these transactions were made between 2012 and 2014.

Swedbank Latvia identified eight customers who performed 43 transactions with the four CPB-1 customers. Swedbank Latvia Compliance proposed closing four customer relationships due to "*unclear activity*," but the Latvian KYC Committee ultimately decided to terminate relationships with two of the customers and to assign an AML risk rating of "*high*" to the remaining two customers. Swedbank Latvia determined that the "*other customers['] explanations and documents (when applicable) [were] considered sufficient.*" Swedbank Latvia also found that 98 unique customers (78 active) performed 433 transactions with entities or individuals identified by the Baltic Banking AFCIS as related to the Azerbaijani Laundromat scheme amounting to €4.2 million, $6.8 million, £29,000, and ₽3.1 million.

2017 GIA Audit Findings

In December 2017, although not informed of the findings arising from Project Clear, GIA issued several audit reports on AML/KYC in the Baltic Subsidiaries that continued to identify areas that required "*Major Improvement*." GIA's report dated 20 December 2017 concluded that the Baltic Subsidiaries' AML risk assessment methodology did not fully incorporate Group and external legal requirements for AML risk assessment processes, and that relevant employees were not properly trained on risk assessment processes and objectives, assessing that "*Major Improvement*" was required. According to GIA's records, GIA closed these findings in July 2018.

GIA's report dated 21 December 2017 found that the process of preparing and updating AML scenarios in NICE Actimize lacked sufficient guiding principles, potentially impacting AML transaction monitoring, assessing that "*Major Improvement*" was required. GIA's database of findings confirmed that GIA closed this item on 20 June 2018.

GIA's next report, dated 28 December 2017, concluded that deficiencies remained in processes surrounding manual updates to sanctions lists and monitoring of quality, completeness, and effectiveness of transaction screening in ProScan, resulting in a "*high dependency on key personnel and weak internal controls*" and "*increased non-compliance risk due to operational failures in the screening process*," assessing that major improvement was required. According to GIA's records, GIA closed this item on 7 June 2018.

In another audit report from 29 December 2017, however, GIA noted that progress had been shown in on-boarding KYC processes at the Baltic Subsidiaries, finding that only "*minor improvements*" were needed to monitor the existence, quality and completeness of KYC to ensure consistency across the Baltic Subsidiaries.

GIA summarized findings from all four audits in its Q4 2017 reports to the Swedbank Board of Directors and Audit Committee, including: (i) with respect to AML in the Baltics, that the findings "*could result in potential criticism from the supervisory authorities*" and "*breach of external regulations*;" (ii) with respect to sanctions in the Baltics, that "*gaps [that] might increase non-compliance risk, lead to operational failures in the screening process and result [in] payments to sanctioned counterparties not being stopped*;" and (iii) with respect to KYC in the Baltics, "*[l]acking or poor controls in the processes [that] could lead to on-boarding of unwanted customers and elevate the risk of regulatory criticism*."

Minutes from a 5 February 2018 meeting of the Board reflect that GIA presented its quarterly report and referred to AML as a "*main theme area[]*" for the fourth quarter. The minutes do not reflect any discussion about, or reaction to, the specific findings of the audits. Minutes from an Audit Committee meeting on the same day reflect that GIA "*informed [the Committee] that GIA has performed several AML engagements during Q4*," that "*[t]here is a lot of focus on the AML area from the financial supervisory authorities*," and that despite improvements in KYC processes and risk assessments "*[m]ajor deficiencies have been revealed in Baltic Banking*." The minutes do not reflect any reaction to the specific findings of the audits.

In an interview, one senior audit manager acknowledged that the continued recurrence of these significant negative findings demonstrated that identified problems persisted for years and that personnel on the ground were often unaware of or resistant to acknowledging such problems. In addition, a senior GIA employee told Clifford Chance that GIA would have structured its audit plans differently if GIA had access to the relevant information developed during Project Clear and the subsequent reviews performed by Group Compliance. However, GIA was not given access to these materials.

Bank of Lithuania Issues Warning on Swedbank Lithuania

In the fall of 2017, an inspection by the Bank of Lithuania ("**Lietuvos Bankas**," or "**LB**") found deficiencies in Swedbank Lithuania's AML/CTF control systems, processes and documentation during the period from January 2016 through March 2017. In February 2018, LB issued a warning to Swedbank Lithuania, and required it to implement remedial measures to eliminate AML/CTF deficiencies by 1 May 2018.

While LB's inspection was ongoing, Swedbank Lithuania met with LB on 24 October 2017 to discuss customer on-boarding. Later that day, LB sent follow-up questions by email, asking, *inter alia*, whether the Bank's customer management system was, for

the purposes of customer screening, "*linked to the Dow Jones, World Check, or any other external data base, or is it linked exclusively to the internal blacklist of the Bank (specifically, at the time of on-boarding of new customers)?*"

Swedbank Lithuania responded to LB on 25 October 2017, stating that "*[e]very morning, the latest lists of EU and US sanctioned individuals and PEP/RCA lists are uploaded*" from various government and subscriber sources (including Dow Jones). Swedbank Lithuania therefore assured LB that "*[w]ith the start of the new working day*" the applicable customer management system would have "*relevant information on both Terrorist List and Restriction List which is used for checking customers during on boarding*."

Swedbank Lithuania employees internally discussed whether to include in the response to LB information about known gaps in the Restriction List. One employee explained that "*if a PEP/RCA does not have a date of birth, they will not be uploaded onto the Restriction List*," and commented, "*[t]his is how it was and how it is, I don't know why. Maybe we shouldn't mention this. This is more for our information.*"

In its response to LB on 25 October 2017, Swedbank Lithuania did not identify this gap in the Restriction List. Instead, Swedbank Lithuania emphasized that the "*automated system in the bank*" which was designed to automatically display a warning message if the "*customer is sanctioned or [a] PEP*" during new customer on-boarding "*has been in operation for more than 10 years*," without noting that its automated system did not always effectively perform screening at the time of on-boarding.

On 27 November 2017, LB provided Swedbank Lithuania with a draft report detailing its conclusions and allowed the Bank to comment and provide additional information. In its 12 December 2017 response, Swedbank Lithuania stated that it "*is not maintaining [...] risky business relationships with non-residents or performing transactions with high risk jurisdictions as the mainstream of the Bank's activity*."

A senior Group Compliance employee, however, informed senior Swedbank Group colleagues and Swedbank Lithuania employees that Swedbank Lithuania had counterparty risk exposure to non-residents and high risk jurisdictions and that the data submitted to LB pertained to "*a lot of payments with counterparties that can be considered questionable and suspicious and should raise a red flag*," including approximately "*240 clients with transactions with questionable or suspicious counterparties*" and "*[c]lose to 300 LP/LLPs (majority of them controlled by offshores or nominee Directors) being counterparties of our clients (some offshore/onshore companies and Directors profiled in ICIJ-Panama Papers and Offshore Leaks)[,] with approx. 900 transactions of a total of approx.. 40m EUR/USD (many in round amounts). . . ,*" concluding that "*[m]any of these LP/LLPs are registered with offshore companies [that are] reported in media to be linked to money laundering, corruption, fraud and illegal arms trade, including such as* "*Magnitsky case*", "*DB mirror trade case*", "*Moldova bank fraud*" *and so on...*" In internal communications with the CCO, that senior Group Compliance employee remarked that LB had "*all of the data that is directly harmful to us.*"

After Swedbank Lithuania provided the requested information and exchanged correspondence over several months, LB issued its final report on 13 February 2018. LB made three overarching findings regarding Swedbank Lithuania 's approach to AML/CTF. First, it found that "*[d]uring the period under inspection, the Bank did not have the current and updated KYC information on the majority of its clients.*" Second, the Bank's "*risk assessment-based method of distributing clients into risk groups did not ensure an effective management of ML/TF risk management during the period under inspection.*" And third, "*monitoring of business relationships and transactions at the Bank was not organized properly during the period under inspection.*"

To address these findings, Swedbank Lithuania submitted a remediation plan to LB on 16 March 2018. The remediation plan included, among other things, a risk assessment for AML/CTF and outlined a procedure for updating KYC data and terminating relationships with or blocking accounts of customers who failed to provide updated information.

By 1 May 2018, Swedbank Lithuania reported to LB that it had completed its remediation plan, including improvements to its risk scoring models, implementation of a new transaction monitoring system (Nice Actimize) in March 2018, the establishment of GSI and the implementation of a renewal KYC questionnaire for all of its high and medium risk customers. Swedbank Lithuania also provided LB with statistics on how many of its customers had successfully updated their renewal KYC questionnaires, broken down by risk category: as of 30 April 2018, 84% of Swedbank Lithuania's corporate, high and medium risk customers had successfully submitted a valid KYC questionnaire; the 16% that had not updated the KYC questionnaire had their accounts restricted. Similarly, 92% of Swedbank Lithuania's private, high risk customers had successfully submitted a valid KYC questionnaire; the remaining 8% had their accounts restricted.

Swedbank Further Examines its Exposure to Suspected Money Laundering at CPB-1 and Other High Risk Financial Institutions

In October 2017, CPB-1's head office disclosed that French authorities were investigating CPB-1 for suspicions of money laundering. Based on these media reports regarding CPB-1, Group Compliance conducted a review at Swedbank Estonia of HRC-1 Group customers' transactions with customers of CPB-1 between 2012 and 2016. Group Compliance determined that, during the review period, 50 HRC-1 Group entities transacted with 77 unique CPB-1 counterparties, with turnover of $852,709,170 outgoing and $12,734,918 incoming. Many of the CPB-1 counterparties were incorporated in either Cyprus or the British Virgin Islands, and 13 were identified in the Panama Papers or Offshore Leaks databases, some with links to Mossack Fonseca. The Compliance review also identified transactions between HRC-1 Group entities and offshore-controlled UK LLP entities, which were found to be supported by little or no business activity, and incoming payments to the Swedbank Estonia accounts of HRC-1 Group entities from 29 accounts at CPB-1 belonging to HRC-1 Group entities.

In January 2018, because of ongoing media scrutiny regarding suspected money laundering at CPB-1, Swedbank Group Compliance continued to review Swedbank's potential exposure to potential money laundering by customers of CPB-1. Group Compliance undertook a review of transactions between all Swedbank Estonia customers and customers of CPB-1 from 2008 through 2011. This analysis identified 25 Swedbank Estonia customers that had transacted directly or indirectly with companies linked to the Magnitsky scheme during the review period, a greater number than had been previously identified internally in 2013. However, the review did not identify evidence that any proceeds from the Magnitsky scheme were transferred between CPB-1 and Swedbank Estonia. 19 of these 25 customers were off-boarded by January 2018. One additional customer was off-boarded in April 2018 as a result of the review. The remaining five customers were subject to an additional risk-based review, which led to decisions to keep four customers and the off-boarding of the remaining customer in 2019.

While the CCO did receive these reports, the Investigation has not found any evidence that these reports were circulated to the Board.

US Authorities Designate CPB-3 as an Institution of Primary Money-Laundering Concern

In February 2018, US authorities issued a public notice proposing to designate CPB-3 as a foreign financial institution of primary money laundering concern and prohibiting

CPB-3 from opening or maintaining any US correspondent accounts. That same day, Swedbank terminated its RMA relationship with CPB-3. Subsequently, on 14 February 2018, Swedbank restricted its customers' SWIFT payments to and from counterparties with accounts at CPB-3. In late February 2018, in consultation with Group Compliance, the Management Boards of Swedbank Estonia, Latvia, and Lithuania passed resolutions further restricting business with CPB-3. In particular, the resolutions included measures to review historical incoming and outgoing payments with CPB-3, and to restrict payments to or from CPB-3 in the future, including by:

- manual processing of all domestic transactions exceeding €1,000;
- rejecting all international transactions in any currency; and
- monitoring all transactions involving clients of CPB-3 from 14 February 2018 onwards.

Shortly thereafter, CPB-3 entered into voluntary liquidation. In March 2018, GSI prepared a memorandum (circulated to Swedbank senior management, including the CEO, CCO, and CRO) summarizing the measures taken up to that point and proposing additional steps to mitigate risks associated with CPB-3 and non-resident Latvian banks, including "*stopping and assessing international payments to/from Latvian high risk banks in USD exceeding equivalent of 1 000 EUR in all Baltic entities*", a threshold change which was implemented in late March 2018. These measures and Swedbank's further response were discussed in March and April 2018 meetings of the Baltic Banking Crisis Management Team that included senior management in Baltic Banking and the Baltic Subsidiaries. During the course of 2018, the Baltic Subsidiaries applied additional risk mitigation measures to transactions with CPB-3 and other high risk financial institutions due to the risk of money laundering and sanctions violations and providing statistics on the number of international transactions to/from high risk Latvian banks which had been "*stopped and assessed*" by the Baltic Subsidiaries. These measures included a retrospective analysis of thousands of transactions and reporting to FIUs.

Group Compliance and GIA Identify Governance and Resource Deficiencies within the First and Second Lines of Defense

On 7 May 2018, an internal report prepared by Group Compliance was circulated in advance of a Performance Review Meeting with Swedbank senior management, including the CEO and CCO, and Group Strategic Alignment. Group Strategic Alignment was established in 2017 as part of the CEO Office and was assigned the task to oversee periodic Performance Review Meetings, for which various Swedbank functions and business areas would submit activity plans and report updates on risks, value streams, finances and other challenges. The report submitted by Group Compliance highlighted persistent governance and resource problems impacting AML/CTF compliance despite the recent creation of GSI.

The report addressed the demarcation of responsibilities between GSI and Group Compliance. Following a discussion of the resource strain within Group Compliance, the report noted that "*unclarities of the borderlines between Compliance and GSI*" remained, especially with regards to AML/CTF. The report stated that, for example, "*Compliance has noted that GSI has down-prioritized some tasks that Compliance regard[s] as vital in the Group's AML/CTF management, e.g. investigating and analyzing transactions/customers related to news/information concerning ML/TF schemes in order to determine the Group's possible risk exposure*." The report states that "*Compliance can cover for these kinds of investigations for some time,*" but a "*final decision on what unit . . . shall be responsible needs to be decided and the need for further resources analyzed*." The report also proposed the creation of a Group AML Committee. It noted, however, that after the proposal for such a committee was submitted to GSI, it had "*not been handled*" and had been "*down prioritized by GSI due to scarcity of resources*."

The report also briefly discussed AML issues in Baltic Banking. It stated that although "*a lot of good* work" was being done, "*there is still a need to change the risk culture with respect to [AML/CTF] and to further embed the risk awareness in the daily operations*." It also stated that Group Compliance would continue to support the Baltic Subsidiaries on AML issues.

The report concluded with "*[c]oncerns, [c]hallenges and [b]usiness risks*." With respect to business risk, the report stated:

> *Non awareness in and adequate actions to handle Money Laundering and Terrorist Financing risk can cost us lack of trust, termination of business relationships, including reputable correspondent banking relationship and last but not least also lead to different types of sanctions from regulators.*

The CEO Report provided to the Board for the 17 July 2018 Board meeting stated that "*Swedbank Compliance has drafted a directive in order to set out the operational responsibilities that ha[ve] been delegated to the employees within GSI from the Chief Compliance Officer*" and that the draft has been sent to the relevant stakeholders. The Q2 2018 Compliance Report provided to the Board for this meeting stated that "*there is a lack of resources and competence, both in terms of personnel and infrastructure, to secure compliance with external and internal regulations in the area of AML/CTF*." It stated that Swedish Banking, Group Lending & Payments, Group Savings and GSI were struggling with resources and competences in AML. The minutes from the 17 July 2018 Board meeting indicate that the CCO presented the highlights of the Q2 Compliance Report, emphasizing that "*the risk related to Anti Money Laundering/ Counter Terrorist Financing (AML/CTF) needs to be prioritized given the impact on the compliance risk level within the Group and the risk for money laundering/terrorist financing (ML/TF)*." The Investigation has not, however, identified evidence that the Board was informed of any specific details of the issues with GSI, or the lack of a proper risk culture in the Baltic Subsidiaries.

The problems identified by Group Compliance in May 2018 were echoed by GIA. In July 2018, GIA issued an audit report that assessed Swedbank Group's efforts in the prior year to improve its management of AML/CTF risk as "*Major improvement required*." The audit mentioned the reorganizations that occurred over the prior year in the first and second lines of defense, including the establishment of GSI and the improvement in demarcation of functions and areas of responsibilities in the AML/ CTF space. But there were "*still some demarcation line issues to be solved, and some responsibilities that need to be documented*," including the absence of a clear role for the Group AML Office. The audit further noted that there was "*no clear Group AML/CTF strategy in place*," and described the Group AML/CTF strategy as "*reactive*" rather than "*proactive*," leading to inefficiencies such as "*recurring remediation programs and task forces involving a lot of resources, including the senior management*."

GIA summarized its findings in its Q2 2018 reports to the Swedbank Board of Directors and its Audit Committee, including its conclusion "*that a clear AML/CTF strategy, including a desired future AML/CTF state connected to the risk appetite as well as a road map, would contribute to the Bank's ability to identify necessary improvements in the AML/CTF area based on changing regulatory demands and external expectations on combatting money laundering and terrorist financing*."

Minutes from a 17 July 2018 meeting of the Swedbank Board of Directors do not reflect any discussion of or reaction to the GIA findings. Minutes from a meeting of the Board's Audit Committee on the same day reflect that the Committee inquired about the findings of the Q2 2018 GIA reports, to which GIA, according to the minutes, replied: "*the audit addressed that the Group does not have a set AML strategy on Group level. In some jurisdictions, for example in Latvia, it is a legal requirement to have an AML strategy. The AC concluded that is important for the Bank to address and handle the AML risks*."

Swedbank Conducts Further Analysis of Money Laundering Risk

In July 2018, *Berlingske* reported that it had obtained leaked bank statements for 20 accounts at CPB-1, and named five entities connected to the Magnitsky scheme among the customers behind these accounts.

In light of these allegations, GSI first confirmed that none of the five entities named by *Berlingske* had been customers of Swedbank. Thereafter, GSI conducted a counterparty search from 1 January 2007 through 5 July 2018 which revealed that nine customers of the Baltic Subsidiaries had received 13 payments totaling €1,061,394 from three of the entities named by *Berlingske*. In all cases, the counterparty bank had been CPB-1. On 11 July 2018, GSI Baltic Banking reported these findings in a memorandum to the senior managers within Swedbank and the Baltic Subsidiaries.

In late spring 2018, in response to further adverse media coverage about CPB-1, Swedbank Group Compliance initiated a review to identify any suspicious transactions between customers of the Baltic Subsidiaries and CPB-1 from 2007-2015. On 12 July 2018, the results of this internal review were reported in a memorandum to the Swedbank CEO, CCO, and other senior managers. The front page of the memorandum bore a legend at the top that stated it was strictly confidential and could not be shared without the "*explicit consent of the CEO*."

This review indicated that customers of the Baltic Subsidiaries performed nearly 16,000 potentially suspicious transactions with CPB-1 counterparties, denominated in both EUR and USD, amounting to a transaction value of approximately €2 billion and $2.8 billion, respectively. A number of these CPB-1 counterparties had links to Mossack Fonseca, the Azerbaijani Laundromat, the Russian Laundromat, the Magnitsky Case, the Russian Mirror Trades, or media reports relating to illegal arms trafficking, drug trafficking, fraud, corruption and other criminal activities. Some Baltic Subsidiary customers were identified as having transactions with counterparties linked to a well-known proxy network that Group Compliance considered to present significant reputational risk because of its reported affiliations with companies used for illicit activities. The review also found that a principal of the proxy network had been an indirect shareholder of a customer of Swedbank Latvia between 2015 and October 2017.

This 12 July memorandum further noted that, because of adverse media about AML risks around two other financial institutions, more transactional analyses were ongoing or planned. Specifically:

- Group Compliance analyzed transactions between CPB-3 and Swedbank in Sweden and found similar high risk transactions to those in the Baltic Subsidiaries. Group Compliance therefore stated it would initiate a similar review of customer transactions with counterparties at CPB-3, as was being performed for CPB-1, going back at least five years.
- Group Compliance had begun to examine transactions between customers of the Baltic Subsidiaries and another financial institution (Counterparty Bank 5, or "**CPB-5**"). Group Compliance reported initial findings that Swedbank Lithuania customers had transactions with CPB-5 counterparties reportedly linked to the Syrian chemical weapons program, and that the results of this analysis would be finalized later in 2018.

The Investigation did not find evidence that the specific findings from Group Compliance's 12 July 2018 report were shared with the Swedbank Board. However, minutes from a 17 July 2018 Board meeting indicate that the Board was informed that

"*Swedbank [was] looking into transactions and other links*" to CPB-1.

Later in 2018, an employee in Group Compliance continued the analysis of the transactions between customers of the Baltic Subsidiaries and CPB-5 from 2012 through 2015 discussed in the 12 July 2018 report. The results of this draft analysis were reported to the CCO in February 2019. The review was designed to detect any high-risk transactions that might warrant further review. The review identified approximately 340 customers (of which 213 were current) of the Baltic Subsidiaries that had performed 1,890 transactions during the review period with 222 customers of CPB-5, worth a total of €51 million and $140 million. Of note, this analysis identified two Swedbank Lithuania customers that had transacted with CPB-5 counterparties that were potentially linked to individuals and entities sanctioned in relation to the Syrian chemical weapons program. In addition, one customer from Swedbank Estonia (related to the HRC-1 Group) and two from Swedbank Latvia had transacted with companies connected to the alleged perpetrator of the Magnitsky fraud—an individual also reportedly linked to the Syrian chemical weapons program. According to internal bank records, accounts for all five of these customers of the Baltic Subsidiaries have been closed.

Continued Focus on Transactions with CPB-1

During the summer of 2018, Group Compliance engaged an external consultant to conduct an expanded transaction analysis to assess the Baltic Subsidiaries' exposure to transactions with customers of CPB-1 between 2007 and 2015. Compliance limited the scope of the analysis to: (1) parties and transactions identified as potentially suspicious, based on the application of specific risk indicators; and (2) domestic payments greater than or equal to €5,000 and foreign payments greater than or equal to €2,500. Compliance considered the following risk indicators in determining whether parties and transactions were potentially suspicious: (1) entities with the legal forms LP, LLP, LTD, Limited, LLC, INC, CORP, or S.A. (other forms were also identified as relevant, but were not as significant by comparison); (2) transactions with certain payment descriptions such as "loan," "refund," "repaid," or "return;" (additional payment descriptions were also identified as relevant, but were not as significant by comparison); (3) payments in EUR or USD (other currencies were also identified as relevant, but were not as significant by comparison); and (4) CPB-1 as the counterparty bank.

The Swedbank CCO reported the results of this expanded risk-based transaction analysis to the Swedbank CEO in a memorandum dated 20 September 2018 (the "**September 2018 CPB-1 Report**"). The September 2018 CPB-1 Report was closely held: a note on the front page directed that it was "*not to be spread to anyone without the express consent of the CEO*."

The September 2018 CPB-1 Report concluded that none of the customers of CPB-1 identified by the media are or were customers of Swedbank, but also explained that few customers had actually been named in the media. The September 2018 CPB-1 Report found that approximately 3,440 customers of the Baltic Subsidiaries had performed potentially suspicious transactions using the above four criteria with CPB-1 counterparties between 2007 and 2015. The total transaction flow was approximately €3.2 billion and $6.7 billion, respectively. According to the Report, as of September 2018, about 2,000 of the 3,440 were existing customers of the Baltic Subsidiaries, 552 of which had been designated as "high risk."

Group Compliance identified several specific risks in the Report:

- At least 74 then-current or former customers of the Baltic Subsidiaries, and 100 CPB-1 counterparties, were linked to the Panama Papers leak. Further, at least 176 customers transacted with 79 CPB-1 counterparties associated with a well-known Latvian proxy network with alleged criminal ties. The turnover of these transactions amounted to €45 million and $72 million.

- Several Baltic Subsidiary customers were also found to have been customers of CPB-1 at the same time or at different times.
- Current and former Baltic Subsidiary customers transacted with several companies linked to the Russian Laundromat and the Russian Mirror Trades schemes. Compliance also determined that at least 14 then-current customers had transacted with customers of CPB-1 that had been linked with the Azerbaijani Laundromat.
- 18 former and 11 then-current Baltic Subsidiary customers were profiled on the OCCRP's published list of "*Russian Laundromat Companies*." Between 2007 and 2015, the turnover of transactions for these 29 customers was approximately €56,000,000 and $16,000,000.

Swedbank's CCO also prepared materials to update the Swedbank Board about these findings, including a draft memorandum explaining Swedbank's processes to prevent money laundering and areas for improvement, which bore a legend at the top reading "*prepared for the Board of Directors of Swedbank AB*" (the "**Draft Board Memorandum**"), and a PowerPoint presentation summarizing the September 2018 CPB-1 Report (the "**Board PowerPoint**"). The CCO solicited feedback from Group Compliance employees involved in preparing the September 2018 CPB-1 Report, and one employee suggested that the CCO "*[t]hink about it/how you're going to identify – or in our case indicate, and leave your mark on, the deficiencies we have – both historically, which can explode in the Baltics in particular in the wake of [CPB-1] – and now. . .*" This employee also suggested adding the following text to the Draft Board Memorandum: "*Recent issues with [other banks], shows that failure within ML-risk could pose huge costs for the bank (fines and lawsuits) as well as for the shareholders (loss of share value).*" The CCO did not include this addition, but did add a footnote observing that "*[CPB-1]'s share price has been severely affected by the allegations on [money laundering/terrorist financing],*" and a brief description of the Baltic Banking off-boarding efforts – "*[a] special effort[] in 2017 . . . [i]nitiated and supported Baltic Banking in the off-boarding of a cluster of non-acceptable ML/TF companies, including doing investigations on employees to understand potential links. This was done with support from [an] external consultant and a very limited number of staff in Baltic Banking.*"

On 23 September 2018, the CCO sent the Draft Board Memorandum and the Board PowerPoint to the CEO. The CEO provided comments to the CCO on both documents, remarking that "*[it would be] good*" to clarify for the Board "*whether they should be really worried or not [. . .] There is a lot of emphasis on describing the risks and, I think, not enough on how we have worked with the issue.*" The CCO counseled caution: "*Well, we haven't worked with AML/Compliance so much, but we had some initiatives – I'm afraid there is a lot of old/historical [stuff] that no one knows, so I think we should be a little careful.*"

The CCO later added language to the Board PowerPoint that compared the suspicious transaction flow for Swedbank identified by Group Compliance against the suspicious transaction flow disclosed in the Public Report on CPB-1: (1) "*The turnover of identified questionable/suspicious clients (former/current) and/or counterparties [for the Baltic Subsidiaries] amounts to approx. EUR 3200m and approx. USD 6700m from 2007 till 2015*"; and (2) "*[CPB-1] report states turnover for 10000 clients for the same period to be EUR 200,000[m] (mostly USD& EUR)*," adding to the presentation notes that the understanding of the CPB-1 Report is that such flow is "*the total flow in [CPB-1] (not limited to flow to/from certain banks)*" and that it "*only covers the so called non-resident portfolio and it is unclear what this precisely comprises*." The earlier draft Board PowerPoint that the CCO shared with the CEO on 23 September 2018 did not draw this comparison. The Investigation did not find evidence that the Draft Board Memorandum was finalized or that either the memo or the underlying September 2018 CPB-1 Report were provided to the Board.

On 27 September 2018, the CCO did brief the Swedbank Board on the findings from Group Compliance's analysis using the Board PowerPoint. The Board PowerPoint provided an overview of the Public Report on CPB-1, and related media allegations; the methodology for Compliance's transactional review; a summary of Compliance's conclusions; and the proposed "*way forward*" that included further analysis of the 2,000 identified then-current customers of the Baltic Subsidiaries. The Board PowerPoint largely tracked the "*key takeaways*" from the September 2018 CPB-1 Report, regarding customers linked to Mossack Fonseca, other "*infamous proxy holders*" and the overall transaction flow.

However, the Board PowerPoint did not include some "*key takeaways*" from the September 2018 CPB-1 Report, and glossed over other salient details. The omissions included:

The finding that at least 17 Baltic Subsidiary customers, all of which were UK registered LPs/LLPs that had performed transactions with customers of CPB-1, were "*controlled by some of the most infamous offshore companies and proxy/nominee directors linked to organized corruption and money laundering*."

- The Board PowerPoint disclosed that 29 customers (out of which only 11 were then-current customers and 18 were former customers) of the Baltic Subsidiaries were identified as "*non-acceptable risk*," with the speaker's notes stating that these customers were "*directly matched against [the] list of the Russian laundromat [companies].*" But it did not include the detail from the September 2018 Report that some of these customers could be connected to schemes and criminal investigations reportedly linked to Russian and Ukrainian arms trafficking, the Magnitsky case, and to companies in North Korea and Syria.
- The September 2018 CPB-1 Report included a limitation, which stated that "*[i] t has not been possible at this stage to relate the numbers in this investigation to the numbers revealed in the CPB-1 Report*". The Board PowerPoint, however, drew a distinction between the $6.7 billion and €3.2 billion of potentially suspicious transaction volumes identified for customers of the Baltic Subsidiaries and the €200 billion flows uncovered at CPB-1.

In addition, several Board members present at the 27 September 2018 Board meeting recalled that the CEO and the CCO both emphasized that Swedbank and CPB-1 were very different; in particular, that CPB-1 was a non-resident-focused branch, while Swedbank Estonia was focused on domestic retail business. Other Board members recalled being given reassuring answers at the meeting and many of the Board members came away from the meeting with the impression that Swedbank was not exposed to significant risk arising from suspected money laundering at CPB-1. Swedbank senior managers who were present also stated that the presentation left the impression that the Bank had no significant exposure to the CPB-1 issues despite the transactions identified with CPB-1 counterparties. Thus, the general sentiment after the Board meeting was that there was no reason to worry about the Bank's exposure to CPB-1.

A senior manager from Group Legal and Swedish external counsel also gave presentations during the 27 September 2018 Board meeting. Group Legal presented an overview to the Board of CPB-1's operations, its non-resident customer portfolio and a timeline of events, based on the publicly released findings issued by CPB-1's head office. Neither the presentation by Group Legal nor the presentation by external counsel specifically addressed any legal risk to Swedbank arising from historical AML deficiencies on which the Board had been briefed.

In sum, Swedbank management did not adequately describe the material legal risks to Swedbank arising from the issues revealed in Swedbank's internal reviews of its own customers and the counterparty risk from CPB-1to the Swedbank

Board. Management's failure to effectively communicate to the Board the extent of Swedbank's potential exposure to material legal risk undermined the Board's ability to make informed decisions to manage the AML risks that the Bank confronted.

Off-Boarding Efforts Following CPB-1 Review

In the weeks following the Board presentation, Swedbank took steps to assess customers identified through the analysis that led to the September 2018 CPB-1 Report. These efforts were known internally as "*Project Nemo*." As part of Project Nemo, the Baltic Subsidiaries decided immediately to off-board 13 customers that were connected to various publicized money laundering investigations. All existing customers identified in the September 2018 CPB-1 Report for which decisions to off-board were not immediately made were subject to further review, including EDD of all relevant transactions between 2007 and 2019. These customers were assessed using updated risk appetite principles stipulating that Swedbank would not do business with:

- shell companies;
- companies that use shell persons or formal nominee shareholders or proxies;
- customers that have breached any ML/TF/sanctions-related laws, regulations or policies;
- customers that misuse their accounts for money laundering/terrorist financing purposes;
- customers that refuse to provide sufficient information or documentation;
- customers without legitimate links to the Bank's home markets; and
- virtual currency dealers.

Swedbank Estonia Employee Conduct Review

In addition, GSI Estonia conducted a separate review to identify any risks related to potential misconduct by current or former employees of Swedbank Estonia similar to that which had been reported at CPB-1. The purpose of the investigation was to retrospectively identify employees that may have been involved in improper behavior or otherwise exposed Swedbank Estonia to heightened risk. GSI Estonia issued a 27 September 2018 report containing its findings that was disseminated to the Swedbank Estonia CEO, the Swedbank CCO, and a senior manager within Baltic Banking. This report found no direct evidence of behavior or practices resembling those that allegedly occurred at CPB-1. The report did, however, note that Swedbank Estonia "*could be compromised or associated with large scale money laundering incidents*" from various risk areas, including: (1) employment relationships; (2) identified misbehavior by former/existing employees (including "*identified risk factors that could point in the direction of kick-backs*"); (3) public perception of former employee behavior; (4) relationships with customers linked to high risk persons; (5) limitations on monitoring capacities; and (6) potential public allegations of money laundering.

Although the GSI Estonia report did not thoroughly elaborate on the "*identified risk factors that could point in the direction of kick-backs*" for former or existing employees, it stated that a cash flow analysis was made regarding certain employees and in the case of one employee "*such additional cash flow is considered as unusual.*" The report also noted, with respect to another employee, that "*although there is no clear indication of the reason for such cash-in source of cash, as an example, in 2009[, the] predecessor of [GSI Estonia] conducted [an] internal investigation that was related to rumours about some IPB employees being involved in receiving personal monetary reward for the services that were provided by the bank (i.e. kickback)*" and that the employee in question "*was not able to give satisfying explanations on [their] cash transactions.*"

The Investigation has identified some historical communications indicating that former employees of Swedbank Estonia, including the primary RM for the HRC-1 Group, at times accepted gifts or apparently low-level gratuities from customers. For example, in chat messages from 2011, while discussing the requirements for certain customer documentation, one RM told a colleague that "*for 1000 [EUR] we'll open an account just by a phone call without any doc[uments]*" and observed that another colleague had "*trained me well – taught me* to '*grease the wheels to get them going*'" In 2014, the RM for the HRC-1 Group stated in a chat communication that the RM had been unwilling to accept a customer, but the customer had "*brought a nice bottle of Hennesy XO so I thought . . . not for nothing[,] it was a classic kick-back.*" In another chat from April 2015, another RM remarked that the RM would open an account for a HRNR customer that was ultimately owned by three Russian oligarchs, "*so that I have something be able to get out of here*."

2018 GIA Findings

At approximately the same time, in September 2018, GIA issued an audit report that found "*Major Improvement required*" for the "*[g]overnance and internal control in Customer Off-Boarding processes*" at the Baltic Subsidiaries. GIA noted that extensive customer off-boarding was conducted by the Baltic Subsidiaries in 2017 and their off-boarding processes continuously improved throughout 2018. Nonetheless, GIA found further improvements were required, for example: (i) documenting internal procedures to reflect actual practices; (ii) regular monitoring of KYC committee decisions about off-boarding; (iii) improving implementation of EDD decisions at Swedbank Lithuania and Swedbank Latvia to avoid incomplete termination of business relationships; and (iv) that GSI units at the Baltic Subsidiaries should establish requirements for off-boarding processes that result from transaction monitoring, to mitigate the risk of subjectivity and of mistakes in decisions.

GIA submitted its Q3 Internal Audit Report to both the Swedbank Board of Directors and its Audit Committee in advance of the Board and Committee meetings in late October 2018. This report identified "*deficiencies in controls and process[es] with the AML/CFT area*" across Swedbank. The report also stated that deficiencies in KYC, appropriate AML controls, and AML resources had persisted. The report made a "*Major Improvement Required*" finding with respect to customer off-boarding processes in the Baltic Subsidiaries, and with respect to that finding, stated that "*further improvements are required to ensure effective governance, AML risk management and internal control environment in order to protect Swedbank from being used for ML and TF purposes and to comply with existing external legal requirements.*"

In addition, a presentation from Swedbank's external auditor and distributed to the Audit Committee in October 2018 stated that "*as reported in previous quarters[,] AML is an area we want to bring to attention. AML is continuously an emerging risk, and in Q3 findings have been identified by both Internal Audit and Compliance*." Minutes from the 22 October Board meeting reflect that "*Anti-Money Laundering*" was the sole "*main theme area*" for Q3, and that a "*Key Finding in Q3 with unsatisfactory evaluation*" related to the finding that "*Swedish Banking has not secured that appropriate governance and controls have been established to assess the quality of [KYC] updates and data in the follow up*." Minutes from the Audit Committee meeting reflect no discussions on, or reaction to, the AML findings described in the quarterly report.

GIA issued another audit report in late October 2018 that assessed the implementation of the Nice Actimize Suspicious Activity Monitoring module ("**Nice Actimize SAM**") in the Baltic Subsidiaries. The audit noted that the Nice Actimize SAM was implemented in the Baltic Subsidiaries by 2018 to replace their semi-manual solutions for transaction monitoring. The audit assessed the set-up of Nice Actimize SAM in the Baltic Subsidiaries and found that "*Major Improvement*" was required due to "*stability and performance issues*" arising from "*hardware deficiencies, lack of human resources*

and the prioritization of new developments." There were delays in alert generation for suspicious transactions which necessitated the investigation of delayed alerts. GIA closed this finding on 4 February 2019. GIA further found that Swedbank Latvia needed to improve its assessment of human resource capacity, noting that the "*[i]mbalanced employees' workload could negatively impact the AML/CTF monitoring process.*" GIA closed this finding on 31 May 2019.

GIA summarized its findings in its Q4 2018 reports to both the Swedbank Board of Directors and its Audit Committee. The reports stated that the "*Nice Actimize SAM module has stability and performance issues when Baltic legal entities were included into system caused by*," among other factors, "*hardware deficiencies [and] lack of human resources*." The reports further stated that "*[w]eak governance of AML/CTF monitoring processes and insufficient IT controls might lead to the legal entities' disability [sic] to detect and investigate ML/TF suspicious transactions that might increase non-compliance, customer dissatisfaction and reputational risk*."

Reporting to the SFSA and the Board Regarding CPB-1

On 3 October 2018, the SFSA sent a detailed list of questions to the Swedbank CCO in preparation for a meeting on 16 October 2018, "*to discuss money laundering issues with a focus on your operations in the Baltics*." These included questions about Swedbank's customer base, AML policies and procedures, and internal controls and monitoring. One of the questions asked, "*To what extent have business relationships with customers that are considered as constituting an unacceptable risk been terminated?*"

On 5 October 2018, the SFSA followed up to ask Swedbank for the results of its internal review into CPB-1. Email communications reflect that, on that same day, the CCO responded that the SFSA would get "*an 'excerpt' from the presentation that was shown to the [B]oard of [D]irectors on September 27 concerning methods and conclusions*," but urged the SFSA not to "*rush to any conclusions based on the way some slides are formulated/can be interpreted*," since more detail would be provided at the upcoming meeting. Three days later, on 8 October, the CCO sent an excerpt of the Board presentation to the SFSA. Like the Board PowerPoint, the presentation excerpt sent to the SFSA provided a high-level summary of the investigation scope and results, including that 2,000 current customers had transacted with customers of CPB-1 and would be assessed on a case-by-case basis. It did not include a slide from the Board PowerPoint that detailed, among other things, the following about the Baltic Subsidiaries' customers: "*237 clients, mostly former have a positive match against the so called ICIJ list, whereof at least 74 are linked to Mossack Fonseca*."

In the materials prepared in advance of the 16 October 2018 meeting, which the CCO sent to the CEO on 14 October 2018, the proposed answer to the SFSA's 3 October question regarding termination of relationships with customers considered to constitute unacceptable risk was stated as, "*Swedbank does not accept ML/TF and regularly off-boards customers who are considered an unmanageable risk. (Difficult to pull up numbers, but a committee follows up on decisions.)*" The Investigation did not identify any written record of what was discussed at the 16 October 2018 meeting.

The investigations by Group Compliance and GSI which assessed the risks from links to the CPB-1 money laundering allegations were discussed again at a Swedbank Board Meeting on 22 October 2018. The minutes for this Board meeting reflect that the CEO briefly summarized the presentation to the Board at its 27 September 2018 meeting,

outlining what Swedbank had done in relation to the alleged money laundering at CPB-1. The minutes also provide that the CEO advised the Board "*that communication to analysts in conjunction with the presentation of Swedbank´s Q3 result, will include information about the internal thorough investigations that show that Swedbank's Baltic operations had no connections to the alleged ML in [CPB-1]*."

When asked about these minutes, the then-CEO informed Clifford Chance that this statement did not accurately reflect statements to the Board; instead, the then-CEO recalled telling the Board that Swedbank was taking steps to address those connections to CPB-1 that it had identified.

The minutes also reflect that the CEO told the Board that:

> *Swedbank has a market leading position in the Baltic market with strong focus on domestic customers, and a relatively low share of cross border payments, compared to competitors with significantly lower market share. A very large number of transactions have been analyzed based on different risk indicators and it can be noted that none of the companies that has been mentioned in the [CPB-1] case have been identified as current clients of Swedbank. Equally no former clients have been identified as having done transactions with [CPB-1] clients mentioned in the [CPB-1] case.*

While recognizing both "*internal and external challenges*" facing AML/CTF, the CEO advised the Board that "*Swedbank has continuously worked with AML and CTF actions with a systematic approach to detect suspicious transactions and business activities*." The minutes do not reflect any further discussion of the September 2018 CPB-1 Report, or the 27 September 2018 GSI Estonia report. But the minutes do reflect that the Chair of the Board "*thanked the participants for [a] very informative and good presentation, giving the Board of Directors a good insight in how Swedbank works with AML-related issues*," and then "*underscored the importance to have high urgency and attention to the issue*."

Swedbank Again Engages Grimstad AS

Earlier in October 2018, Swedbank again retained Grimstad AS, this time to assess whether GSI Estonia's employee conduct investigation had been "*objective and thorough*." This engagement was led by Swedbank's CCO. After the engagement began, Grimstad AS understood that its mandate was expanded to also conduct a broader review of historical AML deficiencies with respect to HRNR customers of Swedbank Estonia, as well as employee accountability. In mid-November, however, before any meaningful investigation could be conducted, the CCO directed Grimstad AS to deliver a report within three weeks. As a result, on 10 December 2018, Grimstad AS issued "*a draft preliminary status report*" that was largely based on the work it had performed in 2017 relating to Project Clear. The report was shared with the CCO and the CEO. However, in a recent interview with Clifford Chance, the former CEO stated that, while the CEO did recall receiving the report, the CEO did not read it because it was only a draft and the CCO had informed the CEO that Grimstad AS had only reported on findings from its 2017 investigation that Swedbank had already addressed.

Grimstad AS's draft report concluded that GSI Estonia's 27 September 2018 report did not describe any of the obvious breaches of AML obligations made by members of Swedbank Estonia's management team and its HRCAC. The main failings at Swedbank Estonia identified by Grimstad AS included accepting HRNR customers despite missing KYC information, not properly investigating or reporting "*obvious*" suspicious transactions involving HRNR customers, and facilitating a poor AML compliance culture. For example, Grimstad AS found no evidence that Swedbank Estonia had investigated numerous transactions that had suspicious indicators such as "*fictional loan agreements and repayments, false invoicing, the use of public known proxies*

and connection to several public[ly] known money laundering schemes." Grimstad AS further noted that some Swedbank Estonia employees, including RMs and senior management, accepted HRNR customers without meeting "*basic KYC principles and [even] protected some . . . HRNR customers from the Russian authorities, including tax authorities.*" These employees had "*accepted to hide the ultimate beneficial owners from the registration within the bank, which [led] to risks of failure to identify sanctioned individuals*."

Grimstad AS recommended that Swedbank take certain remedial actions, including informing the SFSA and EFSA of these historical deficiencies, and recommended continued investigative steps, such as: further fact-finding to identify current or former employees who were accountable, additional transactional analysis and sample testing for indicators of money laundering. However, according to Grimstad AS, neither this 2018 draft status report nor the draft report it delivered to Swedbank in July 2017 represented the results from completed investigations, nor were they intended to convey final analyses of the issues presented.

In January 2019, Group Compliance prepared a memorandum to Grimstad AS regarding its findings and objecting to some of its recommendations. Among other things, Group Compliance stated that it had already implemented some of Grimstad AS's recommendations. For example, Group Compliance stated that both the SFSA and the EFSA had been informed about the problematic customers off-boarded as a result of Project Clear, and with respect to employee accountability, Swedbank now recognized "*the legal, operational[,] and reputational risk that [Swedbank Estonia] management has actually put Swedbank and its reputation in – even though this might not have [been] understood at the time*." Nevertheless, Group Compliance observed that any further steps needed to "*be balanced so to at all times take the best interest of the Group and all of its stakeholders into consideration*."

Grimstad AS responded to Swedbank Compliance by letter in late January 2019, describing any investigative steps that it had taken as preliminary, but stating that it was apparent there was "*a risk that both Swedbank Group and individuals can be liable for criminal offences in the handling of several of the HRNR customers.*" On 19 February 2019, the CCO and another Group Compliance employee met with Grimstad AS to discuss the findings and potential next steps. A week later, Group Compliance sent another memorandum to Grimstad AS providing an overview of the AML-related remedial actions and initiatives that Swedbank had taken within Baltic Banking since Project Clear. Swedbank had no further substantive communications with Grimstad AS after sending that memorandum.

Exposure to Suspected Money Laundering at CPB-4

In late 2018 and early 2019, Group Compliance conducted an analysis of exposure to money laundering risk from CPB-4, a then-defunct Lithuanian bank that was involved in suspected money-laundering schemes. The Group Compliance investigation was prompted by a complaint dated 12 October 2018 from HCM to the Swedish Economic Crime Authority that accused another bank of facilitating money laundering in connection with transactions through CPB-4 and CPB-1.

The investigation included an analysis of transactions between Swedbank and its Baltic Subsidiaries and CPB-4 counterparties between 2007 and 2013. For Swedish Banking customers, the analysis was focused on international payments. For the Baltic Subsidiaries, the scope was focused on international and domestic Lithuanian payments exceeding €2,500.

For customers of Swedish Banking, the analysis identified that, between 2007 and 2013, 99 Swedbank customers had received 252 incoming payments (totaling Swedish Kr. 145 million) from CPB-4 counterparties that were "*questionable/suspicious*" using

pre-defined risk indicators. Twenty of these counterparties were explicitly mentioned in the 2018 HCM report.

For customers of the Baltic Subsidiaries, the review indicated that 400 customers (127 of which were then-current) had performed 3,746 questionable or suspicious transactions (totaling approximately €536 million)with 362 CPB-4 counterparties. Swedbank Group Compliance concluded its report by noting "*severe weaknesses*" in the "*historical SAR/STR reporting of suspicious transactions/activity to the FIU*," and determining that a majority of the questionable/suspicious transactions it encountered should have been reported.

Although the general nature of these findings was reported to the Swedbank RCC in late January 2019, much of the salient detail was not included. The CCO informed the RCC that Group Compliance had conducted a review of CPB-4, and that "*[a]ll current customers deemed to be outside the risk appetite in Swedish Banking and Baltic Banking have been off-boarded and/or FIU reported, the latter when deemed appropriate. The volumes and countries are as shown in the presentation. Former customers will be handled on a risk based approach*." The referenced presentation gave a general summary of the findings in the 2 January 2019 draft report, including the number and amount of questionable/suspicious transactions with CPB-4 counterparties in Swedish and Baltic Banking. The presentation to the RCC, however, did not include information regarding the number of CPB-3 counterparties with links to criminal schemes and proxy networks. Both the RCC and the Board presentation also omitted reference to the weaknesses in historical SAR reporting. On the same day, the CCO gave a more abbreviated briefing on CPB-4 to the Swedbank Board, without the specific transaction and customer data from the RCC presentation.

GIA Audits in January 2019

In early January 2019, GIA issued an audit report that graded the EDD process in Swedbank Estonia and Swedbank Lithuania as "*Major Improvement Required*." This report provided that in light of the modifications to Swedbank's risk-based approach, beneficial ownership, and CDD ushered in by the Fourth EU AML Directive, GIA performed an audit of the EDD process in Swedbank Estonia and Swedbank Lithuania, focused on testing completeness and EDD documentation and conclusions. The audit found that procedures and EDD memoranda templates in both Swedbank Estonia and Swedbank Lithuania should be strengthened and clarified with respect to source-of-funds identification, and source-of-wealth identification for PEPs and beneficial owners. GIA closed these findings in July and August 2019.

In January 2019, GIA submitted its Internal Audit Report for Q4 2018 to the Audit Committee of the Swedbank Board in advance of the Committee's 25 January 2019 meeting, which the Swedbank CEO attended. Among other things, the report discussed the findings from the October 2018 audit of the implementation of Nice Actimize SAM in the Baltic Subsidiaries and the findings from the January 2019 audit of the EDD process in Swedbank Lithuania and Estonia, both detailed above. Minutes of the Audit Committee meeting do not reflect any discussion on or reaction to these findings.

Minutes of a 28 January 2019 meeting of the Swedbank Board reflect agreement that "*[c]ompliance to AML regulations is a challenge for all financial institutions*," and that "*AML is a prioritized area . . . and there are several remediation projects on-going to strength[en] governance, processes, and competence*."

Board Reporting Regarding the Second Grimstad AS Engagement

On 28 January 2019, the Swedbank CCO also updated the RCC of the Swedbank Board on Swedbank's review of its exposure to the alleged money laundering at CPB-1 that was reported to the Board in September 2018. The CCO noted that the EDD

review of approximately 2,000 customers identified through the CPB-1 investigation had identified 340 customers for off-boarding as of January 2019, 140 of which had already been off-boarded. Further, the CCO explained that Swedbank had engaged an "external firm" to further assist the internal investigation relating to alleged money laundering involving CPB-1, but did not specifically identify Grimstad AS.

The minutes of the 28 January meeting reflect that the CCO informed the RCC that the external firm found "*no actual evidence of any collusion*," but identified the presence of "*some suspicious circumstances [] which have not been able to be fully substantiated.*" The PowerPoint slides that accompanied the presentation to the RCC included one slide about the CPB-1 internal review, which simply remarked that there was "*[n]o real evidence of criminality*" but that "*[one] former employee [was] currently linked to a current Russian PEP*." The meeting minutes further indicate that the CCO told the RCC that "*[t]he mere fact that someone could allege that there could have been wrong-doings of employees will always constitute a reputational risk*" for the Bank and therefore the CEO (who also attended the meeting) would handle the issue of employee accountability from a reputational risk perspective. The CCO did not outline any specific next steps relating to these issues.

That same day, the CCO also presented to the full Swedbank Board on AML issues. The minutes from the Board meeting indicate that the CCO reported that "*Swedbank has made a follow-up after the investigation and alleged money laundering of CPB-1's Estonian branch*," and the presentation was accompanied by an abbreviated version of the PowerPoint presentation used for the RCC meeting. Neither the Board minutes, nor the PowerPoint slides, indicate that the Board was informed of the involvement of Grimstad AS or its December 2018 findings. The Swedbank Board was not provided with Grimstad AS's December 2018 draft report or informed of its findings until March 2019.

B. Findings Regarding Swedbank's Risk Management and AML and Sanctions Compliance

The Investigation did not conclude based on the evidence available from Swedbank that the Baltic Subsidiaries engaged in money laundering. Such a finding would require, among other things, definitive knowledge of a customer's source of funds, which was not available. The Investigation did reveal, however, that Swedbank and its Baltic Subsidiaries were exposed to substantial money laundering risk arising from customer activity driven by the HRNR strategy and from long-standing deficiencies in AML controls, as set forth above (*see supra,* Section VII.A.).

It is apparent from these deficiencies that during the Investigation Period, Swedbank did not implement adequate controls to manage the risk that Swedbank or the Baltic Subsidiaries would be used by its customers for illicit purposes. In this regard, in practice, Swedbank did not adequately train its first line of defense to understand the importance of collecting appropriate KYC information regarding ultimate beneficial owners, source of customer funds, and legitimate business purposes of corporate structures and transactions. Nor did Swedbank take adequate steps to make sure that KYC and EDD policies were followed, that the information collected was properly analyzed for AML risk, that decisions to on-board and to maintain customers were based on adequate information regarding AML risk and that customer transaction monitoring was designed to address the AML risks presented by the high risk customer base.

As a result, the Investigation found that there were systematic circumstances—particularly, but not exclusively, in Swedbank Estonia—of accepting customers: (a) without beneficial ownership information or while knowing that the beneficial ownership information was incomplete or inaccurate; (b) without determining the legitimate business purpose for certain complex and opaque corporate structures or transactional

activity; or (c) while knowing that certain structures were intended by the customer to prevent third parties from learning the identity of beneficial owners. For example, Swedbank Estonia employees accepted without question customer entities referred to as "*wallet companies*," which were described in internal documents as having been set up to separate the source of the money from other companies, to minimize the risk of affiliation for the client. These circumstances extended in large part to LC&I's relationship with the HRC-1 Group.

At least until 2016, when the decision was made to de-risk the non-resident business, Swedbank Estonia and Swedbank Latvia chose not just to maintain, but to target and to pursue high risk business, including the HRNR portfolio, in the absence of adequate controls to properly identify, quantify and manage the risk. The Investigation did not conclude that, prior to 2016, Swedbank senior management was monitoring the Baltic Banking business in a way that would have adequately identified these risks or their scope. Beginning in 2016, due at least in part to the series of circumstances discussed above (*see supra,* Section VII.A.), Swedbank control functions did begin a broad series of internal reviews, some supported by external consultants, aimed at understanding the historical risk posed by the HRNR portfolio in the Baltic Subsidiaries, in light of the attendant significant AML compliance deficiencies.

GIA repeatedly flagged AML deficiencies, and many of the GIA-identified issues were timely closed. In subsequent audits, however, GIA then identified the same or similar deficiencies, a pattern that continued over the course of many years. GIA does not appear to have sounded any serious alarms for the deficiencies it did identify. But GIA also was not informed when Group Compliance identified significant AML deficiencies or off-boarded problematic customers, the most prominent example being Project Clear and the work of Grimstad AS. Swedbank senior management failed to share such information with GIA and the Board, giving the impression that everything was under control. Indeed, Swedbank senior management appears to have failed to appreciate the significance of the issues to the business and reputation of the institution, as until 2019 and the initiation of the Investigation, Swedbank did not seek a systematic and wholesale identification of the depth and root causes of the recurrent issues or to initiate a comprehensive remediation, as it has done beginning in 2019.

The compliance deficiencies extended to economic sanctions compliance controls. Beginning in 2005, US authorities brought a series of major enforcement actions against EU and other non-US based banks arising out of failures in OFAC sanctions compliance controls, which enforcement actions resulted in hundreds of millions, and some instances billions of dollars in penalties. While these actions were highly publicized and received considerable industry attention, Swedbank did not shore up its sanctions compliance with systematic automated customer and transaction screening in the Baltic Subsidiaries, for example, until 2017. Despite extensive public information regarding potential OFAC sanctions risk to banks involved in international payments through the US financial system, Swedbank senior management appears to have failed to appreciate the potential significance of these issues to the business and reputation of the institution until many years after peer Europe-based institutions had done so.

Further, the Investigation indicates that, throughout the Investigation Period, Swedbank senior management failed to ensure that the Swedbank Board was properly educated about and fully appreciative of the material legal and reputational risks that the historical compliance deficiencies posed to the institution. This failing was particularly acute during the period from 2016 through into early 2019, when Swedbank's control functions, with the support of external consultants, had identified to senior management their view of the seriousness of the historical deficiencies, conduct and attendant risks. During this period, Swedbank senior management failed to ensure that the Management Boards and Supervisory Councils of the Baltic Subsidiaries, particularly Swedbank Estonia, were adequately informed of findings with respect to money laundering risk and AML control deficiencies that affected the institution.

Finally, the Investigation did not find evidence before 2019 of a concerted effort by Swedbank to establish a broad culture of compliance within Swedbank or the Baltic Subsidiaries, or to instill an appropriate 'tone from the top' through to the client facing teams and control functions regarding the critical importance of AML and sanctions risk management and compliance.

As described further below (*see infra* Section VIII, *Remediation*), Swedbank and the Baltic Subsidiaries have made significant remedial efforts, primarily starting in 2016, to address the AML issues posed by HRNR and other high-risk customers, and to address and enhance compliance policies and procedures, AML controls and relevant IT systems. These efforts included steps to de-risk the HRNR portfolios by off-boarding substantial numbers of HRNR customers, including high risk customer groups that had generated substantial profits for the Bank. The remediation efforts also included establishing an AML program for the Baltic Subsidiaries in 2016 and implementing a Group-level policy on risk appetite in 2017, as well as enhancements to systematic sanctions controls. While off-boarding HRNR customers reduced risk, the efforts to remediate the historical AML framework were hampered by deficiencies in governance, unclear ownership of AML issues and failure to adequately prioritize AML and sanctions compliance.

Since early 2019, Swedbank and its Baltic Subsidiaries, with the support of the Swedbank Board, have: (a) embarked on a much more comprehensive approach and remediation plan to address and to strengthen the AML/CTF framework; (b) undertaken a review of Swedbank's corporate governance; (c) engaged external consultants to assist in remediation efforts; (d) increased AML/CTF resources; (e) taken certain employment actions; and (f) continued to off-board customers to further de-risk the customer portfolio. Swedbank also has new leadership, including a new CEO, a new CCO and a new Chairman of the Board.

C. Findings Regarding AML Risk Review

This section sets forth the analysis of relevant customers' transactions over the course of the AML Review Period. As set forth above (*see* Section IV, *supra*), Clifford Chance and FTI applied 21 automated detection algorithms to certain categories of customers' external transaction activity. The detection algorithms alert upon potentially suspicious patterns that deviate from what would be considered typical banking activity for individual and corporate customers. The detection algorithms do not indicate that alerted transactions were necessarily suspicious, but rather are designed to identify transactions with risk indicators similar to those that a transaction monitoring system would flag for further review. Clifford Chance and FTI focused this analysis on two categories of customers: (1) a broad set of AML Risk Identified Customers; and (2) a subset of those customers that fit Swedbank's definition of HRNR Customers.

The HRNR Customers include any customers that met Swedbank's definition for that population: non-resident legal entities registered outside the EU countries or Norway, and also those registered in Malta, Cyprus, the United Kingdom or Luxembourg. Swedbank's methodology for identifying HRNR customers only included customers ranked as high risk in Swedbank's internal risk ratings. Therefore, Clifford Chance and FTI included as HRNR Customers any non-resident legal entities listed as resident in one of the applicable countries in Swedbank's structured customer database and categorized as high risk by Swedbank at any time during the AML Review Period. Clifford Chance and FTI analyzed the activity of HRNR Customers to assess the extent to which customers meeting the definition of this population at any point during the AML Review Period had external transactions that alerted on one or more detection algorithms. The purpose of this analysis was to assess the extent of such customers' potentially suspicious activity and changes to that activity over time.

As described above, the broad set of AML Risk Identified Customers consists of customers that Clifford Chance and FTI identified as being connected to relevant conduct, networks and counterparties indicative of increased money laundering risk. AML Risk Identified Customers include:

- HRNR Customers as defined by Swedbank's own criteria;
- Additional legal entity customers resident in the same jurisdictions set out in the Bank's HRNR defined criteria but without reference to risk ratings;
- Additional legal entity customers resident in certain EU countries deemed by FTI to present a relatively higher risk of money laundering, namely Bulgaria, Czech Republic, Ireland and Romania;
- Legal entity customers that were owned by entities or natural persons resident outside the EU countries or Norway, or that were resident in Malta, Cyprus, the United Kingdom, Luxembourg, Bulgaria, Czech Republic, Ireland or Romania;
- Non-resident natural person customers that had at least €250,000 in external transactions in the AML Review Period;
- Transactions of customers with counterparties at six high risk financial institutions, including those referred to in the Report as CPB-1,[44] CPB-2, CPB-3, CPB-4 and CPB-5;
- Customers identified by using search terms. The search term sources include:
  - Customer names extracted from the Bank's Prior Reports concerning AML-related investigations or reviews;
  - Entities or individuals identified in Magnitsky-related complaints filed by HCM against Swedbank and Nordea;
  - Persons and entities identified in the course of the employee data review and employee interviews; and
  - Entities identified in the ICIJ Panama Papers database.

The population of HRNR Customers is subsumed within the broader set of AML Risk Identified Customers.

The following sets forth the results of the application of the detection algorithms to the HRNR Customers and the AML Risk Identified Customers, as well as key observations relating to those results.

It is important to reiterate that the fact that a customer was included in the HRNR or AML Risk population does not mean that customer necessarily engaged in suspicious or improper activity. In addition, the fact that a payment hit against one or more of the detection algorithms does not mean that the payment should have at the time been considered suspicious, nor is it evidence that a customer engaged in money laundering or other financial crime. Rather, the detection algorithms are designed to identify transactions that a well-functioning transaction monitoring system would flag for further review. Generally, considering automated detection algorithms on an industry-wide basis, typical false positive rates are above 90%.

While it would be possible for a financial institution with sufficient resources to resolve each alerted transaction, it is much more difficult and impractical to replicate that manual review process on a scale that encompasses several years of transactions for multiple subsidiaries within a reasonable investigative timeframe. Transaction monitoring systems weight the results of multiple detection algorithms to prioritize transactions indicative of high risk for manual review. As a manual review was not

[44] Transactions with CPB-1 were only considered until the end of Q1 2016, as that is the period of highest risk.

performed for this exercise, the below analysis highlights transactions that hit on any three or more detection algorithms (without weighting) to provide a more focused view of the money laundering risk arising from the transaction activity of the customer segment under review.

1. Estonia

a. HRNR Customers

The following table shows the number of active customers[45] identified as HRNR Customers by year, along with the total incoming and outgoing external transactions performed by those customers.[46]

	Estonia		
	Active HRNR Customers	Incoming €'M	Outgoing €'M
2007	1,904	8,869.2	8,757.8
2008	1,203	6,204.3	6,418.9
2009	1,025	5,618.7	5,592.2
2010	855	5,613.0	5,722.5
2011	714	8,762.4	8,656.3
2012	707	9,353.8	9,371.6
2013	768	7,886.9	7,960.1
2014	753	4,828.6	4,767.2
2015	790	4,260.3	4,172.9
2016	768	3,895.9	4,308.1
2017	418	1,108.6	1,524.8
2018	126	126.1	157.7
2019 Q1	109	26.7	13.4
Total	**2,668**	**66,554.6**	**67,423.4**

For the entirety of the period analyzed, the proportion of the overall Swedbank Estonia customer base that consisted of HRNR Customers was low: less than 0.2%. As the table demonstrates, both the number of active HRNR Customers and the value of external transactions decreased significantly over time, with a noticeable decrease after 2016.

The following table shows (i) the value of external payment inflows for HRNR Customers that alerted on three or more detection algorithms throughout the AML Review Period and (ii) the total external payment inflows for Swedbank Estonia, within the calendar year or portion of calendar year analyzed. In total (across all currencies), there was the equivalent of €5.2 billion of external payment inflows that alerted on three or more algorithms throughout the AML Review Period.

TOTAL INFLOW ALERTING ON THREE OR MORE ALGORITHMS IN €'MILLION (ESTONIA)

Category	Q2-Q4 2014	2015	2016	2017	2018	Q1 2019
HRNR Customer Transactions	1,491.1	1,648.1	1,549.3	459.1	6.8	0.2
Total Bank External Transactions - All Customer Transactions	26,283.4	33,871.5	35,296.3	35,761.8	37,098.3	7,462.7
HRNR Customer Transactions Alerted on 3 or more Algorithms as a Proportion of Total Transactions	5.7%	4.9%	4.4%	1.3%	0.02%	0.002%

Over the course of the AML Review Period, the proportion of total external payment inflows for all active Swedbank Estonia customers that consisted of external payment inflows for HRNR Customers alerting on 3 or more detection algorithms decreased from 5.7% in Q2-Q4 2014 to 0.002% in Q1 2019.

[45] Active Customers are defined as customers with an open account at some point during the year.

[46] All transaction values are presented in the equivalent Euro value of the transaction, regardless of the original currency. The transactions are converted at daily exchange rates stored within Swedbank's structured data.

The following table shows (i) the value of external payment outflows for HRNR Customers that alerted on three or more algorithms throughout the AML Review Period and (ii) the total external payment outflows for Swedbank Estonia, within the calendar year or portion of calendar year analyzed. In total (across all currencies), there was the equivalent of €7.7 billion of external payment outflows that alerted on three or more algorithms throughout the AML Review Period.

TOTAL OUTFLOW ALERTING ON THREE OR MORE ALGORITHMS IN €'MILLION (ESTONIA)

Category	Q2-Q4 2014	2015	2016	2017	2018	Q1 2019
HRNR Customer Transactions	2,013.2	2,231.2	2,393.2	967.5	60.1	3.3
Total Bank External Transactions - All Customer Transactions	25,515.6	33,481.6	34,661.1	35,537.6	36,864.3	7,552.2
HRNR Customer Transactions Alerted on 3 or more Algorithms as a Proportion of Total Transactions	7.9%	6.7%	6.9%	2.7%	0.2%	0.04%

Over the course of the AML Review Period, the proportion of total external payment outflows for all active Swedbank Estonia customers that consisted of external payment outflows for HRNR Customers alerting on three or more detection algorithms decreased from 7.9% in Q2-Q4 2014 to 0.04% in Q1 2019.

Thus, the value of the external payments alerting on three or more detection algorithms (both inflows and outflows) fell considerably over time. In particular, the total alerted transactions fell after 2016, when Swedbank Estonia off-boarded the HRC-1 Group and other high risk customers. **Appendix C** sets out all alerted transactions for customers in the HRC-1 and HRC-3 groups.

b. AML Risk Identified Customers

The following table shows (i) the value of external payment inflows for AML Risk Identified Customers that alerted on three or more algorithms throughout the AML Review Period and (ii) the total external payment inflows for Swedbank Estonia, within the calendar year or portion of calendar year analyzed. In total (across all currencies), there was the equivalent of €9.9 billion of external payment inflows that alerted on three or more algorithms throughout the AML Review Period, of which $6.8 billion was denominated in US Dollars.

TOTAL INFLOW ALERTING ON THREE OR MORE ALGORITHMS IN €'MILLION (ESTONIA)

Category	Q2-Q4 2014	2015	2016	2017	2018	Q1 2019
AML Risk Identified Customer Transactions	2,490.1	2,736.3	2,385.9	1,534.7	639.8	80.9
Total Bank External Transactions - All Customer Transactions	26,283.4	33,871.5	35,296.3	35,761.8	37,098.3	7,462.7
AML Risk Identified Customer Transactions Alerted on 3 or more Algorithms as a Proportion of Total Transactions	9.5%	8.1%	6.8%	4.3%	1.7%	1.1%

Over the course of the AML Review Period, the proportion of total external payment inflows for all active Swedbank Estonia customers that consisted of external payment inflows for AML Risk Identified Customers that alerted on three or more detection algorithms decreased from 9.5% in Q2-Q4 2014 to 1.1% in Q1 2019.

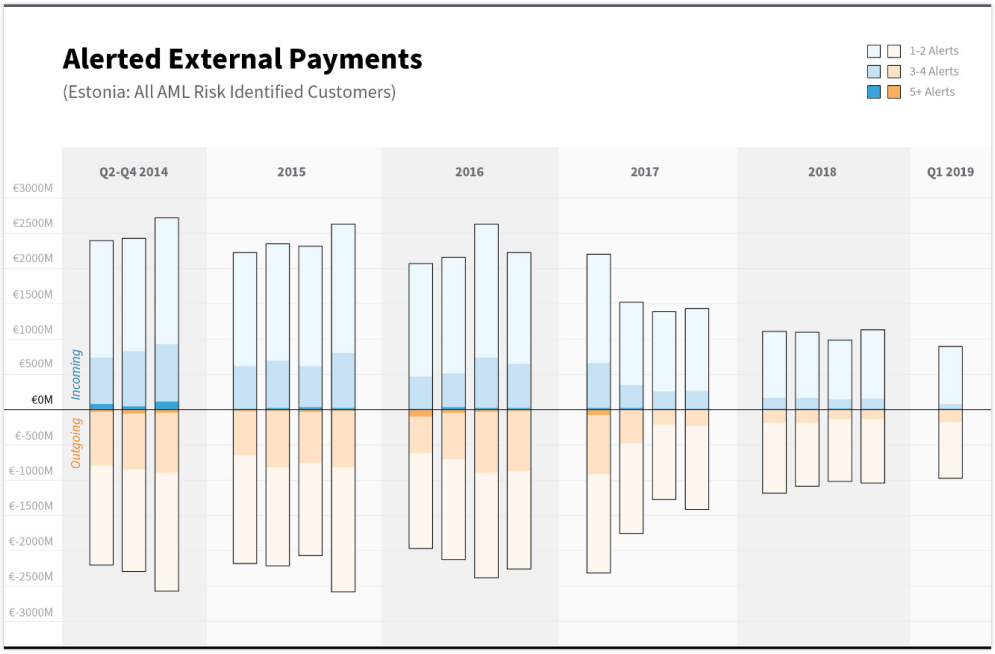
The following table shows (i) the value of external payment outflows for AML Risk Identified Customers that alerted on three or more algorithms throughout the AML Review Period and (ii) the total external payment outflows for Swedbank Estonia, within the calendar year or portion of calendar year analyzed. In total (across all currencies), there was the equivalent of €11.4 billion of external payment outflows that alerted on three or more algorithms throughout the AML Review Period, of which $6.6 billion was denominated in US Dollars.

TOTAL OUTFLOW ALERTING ON THREE OR MORE ALGORITHMS IN €'MILLION (ESTONIA)

Category	Q2-Q4 2014	2015	2016	2017	2018	Q1 2019
AML Risk Identified Customer Transactions	2,547.0	3,047.1	3,086.9	1,847.4	647.1	178.4
Total Bank External Transactions - All Customer Transactions	25,515.6	33,481.6	34,661.1	35,537.6	36,864.3	7,552.2
AML Risk Identified Customer Transactions Alerted on 3 or more Algorithms as a Proportion of Total Transactions	10.0%	9.1%	8.9%	5.2%	1.8%	2.4%

Over the course of the AML Review Period, the proportion of total external payment outflows for all active Swedbank Estonia customers that consisted of external payment outflows for AML Risk Identified Customers that alerted on three or more detection algorithms decreased from 10.0% in Q2-Q4 2014 to 2.4% in Q1 2019.

As discussed above, although some transactions alerted on only one scenario, other transactions alerted on multiple detection scenarios. The tables above set out the transactions which alert on three or more scenarios. The following chart sets out all of the alerted external payment inflows and outflows for all AML Risk Identified Customers during the AML Review Period, with shading to indicate the proportion of alerted transactions that triggered one to two alerts (light shading), three to four alerts (medium shading) and five or more alerts (dark shading). A table setting out the corresponding alerted values is set out at **Appendix D.1.**



As the chart demonstrates, the total level of alerted transactions (and also transactions alerting on three or more detection algorithms) decreased after 2016, consistent with the off-boarding of the HRC-1 Group and other high risk customers.

2. Latvia

a. HRNR Customers

The following table shows the number of active customers identified as HRNR Customers by year, along with the total incoming and outgoing external transactions performed by those customers.

	Latvia		
	Active HRNR Customers	Incoming EUR'M	Outgoing EUR'M
2007	570	957.7	943.6
2008	378	925.2	995.6
2009	358	435.1	460.5
2010	364	478.2	485.5
2011	383	538.4	538.0
2012	429	811.0	799.3
2013	520	921.4	887.4
2014	583	1,160.0	1,069.5
2015	560	1,657.5	1,621.0
2016	506	1,195.3	1,374.4
2017	63	44.3	52.3
2018	23	4.4	3.4
2019 Q1	20	1.2	0.9
	1,182	**9,129.6**	**9,231.6**

For the entirety of the period analyzed, the proportion of the overall Swedbank Latvia customer base that consisted of HRNR Customers was low: less than 0.1%. As the table demonstrates, the number of HRNR Customers decreased significantly after 2007 and again after 2016, and the value of the transactions decreased after 2008, and then again after 2016.

The following table shows (i) the value of external payment inflows for HRNR Customers that alerted on three or more detection algorithms throughout the AML Review Period and (ii) the total external payment inflows for Swedbank Latvia, within the calendar year or portion of calendar year analyzed. In total (across all currencies), there was the equivalent of €1.4 billion of external payment inflows that alerted on three or more algorithms throughout the AML Review Period.

TOTAL INFLOW ALERTING ON THREE OR MORE ALGORITHMS IN €'MILLION (LATVIA)

Category	Q2-Q4 2014	2015	2016	2017	2018	Q1 2019
HRNR Customer Transactions	298.7	782.3	357.0	7.3	0.04	0.0
Total Bank External Transactions - All Customer Transactions	18,848.9	25,762.7	25,211.4	25,298.0	26,419.1	5,697.2
HRNR Customer Transactions Alerted on 3 or more Algorithms as a Proportion of Total Transactions	1.6%	3.0%	1.4%	0.03%	0.0002%	0.0%

Over the course of the AML Review Period, the proportion of total external payment inflows for all active Swedbank Latvia customers that consisted of external payment inflows that alerted on three or more detection algorithms for HRNR Customers decreased from 3% in 2015 to 0% in Q1 2019.

The following table shows (i) the value of external payment outflows for HRNR Customers that alerted on three or more algorithms throughout the AML Review Period and (ii) the total external payment outflows for Swedbank Latvia, within the calendar year or portion of calendar year analyzed. In total (across all currencies), there was the equivalent of €1.6 billion of external payment outflows that alerted on three or more algorithms throughout the AML Review Period.

TOTAL OUTFLOW ALERTING ON THREE OR MORE ALGORITHMS IN €'MILLION (LATVIA)

Category	Q2-Q4 2014	2015	2016	2017	2018	Q1 2019
HRNR Customer Transactions	293.9	790.2	468.1	9.0	0.02	0.0
Total Bank External Transactions - All Customer Transactions	19,091.6	26,260.7	25,752.5	26,336.1	28,476.2	6,476.1
HRNR Customer Transactions Alerted on 3 or more Algorithms as a Proportion of Total Transactions	1.5%	3.0%	1.8%	0.03%	0.0001%	0.0%

Over the AML Review Period, the proportion of total external payment outflows for all active Swedbank Latvia customers that consisted of external payment outflows that alerted on three or more algorithms for HRNR Customers decreased from 3% in 2015 to 0% in Q1 2019.

Thus, the value and proportion of the alerted external payments (both inflows and outflows) fell considerably over time, particularly after 2016.

b. AML Risk Identified Customers

The following table shows (i) the value of external payment inflows for AML Risk Identified Customers that alerted on three or more algorithms throughout the AML Review Period and (ii) the total external payment inflows for Swedbank Latvia, within the calendar year or portion of calendar year analyzed. In total (across all currencies), there was the equivalent of €4.8 billion of external payment inflows that alerted on three or more algorithms throughout the AML Review Period, of which $2.6 billion was denominated in US Dollars.

TOTAL INFLOW ALERTING ON THREE OR MORE ALGORITHMS IN €'MILLION (LATVIA)

Category	Q2-Q4 2014	2015	2016	2017	2018	Q1 2019
AML Risk Identified Customer Transactions	910.1	1,763.0	1,134.9	591.7	341.6	51.3
Total Bank External Transactions - All Customer Transactions	18,848.9	25,762.7	25,211.4	25,298.0	26,419.1	5,697.2
AML Risk Identified Customer Transactions Alerted on 3 or more Algorithms as a Proportion of Total Transactions	4.8%	6.8%	4.5%	2.3%	1.3%	0.9%

Over the course of the AML Review Period, the proportion of total external payment inflows for all active Swedbank Latvia customers that consisted of external payment inflows for AML Risk Identified Customers that alerted on three or more detection algorithms decreased from 6.8% in 2015 to 0.9% in Q1 2019.

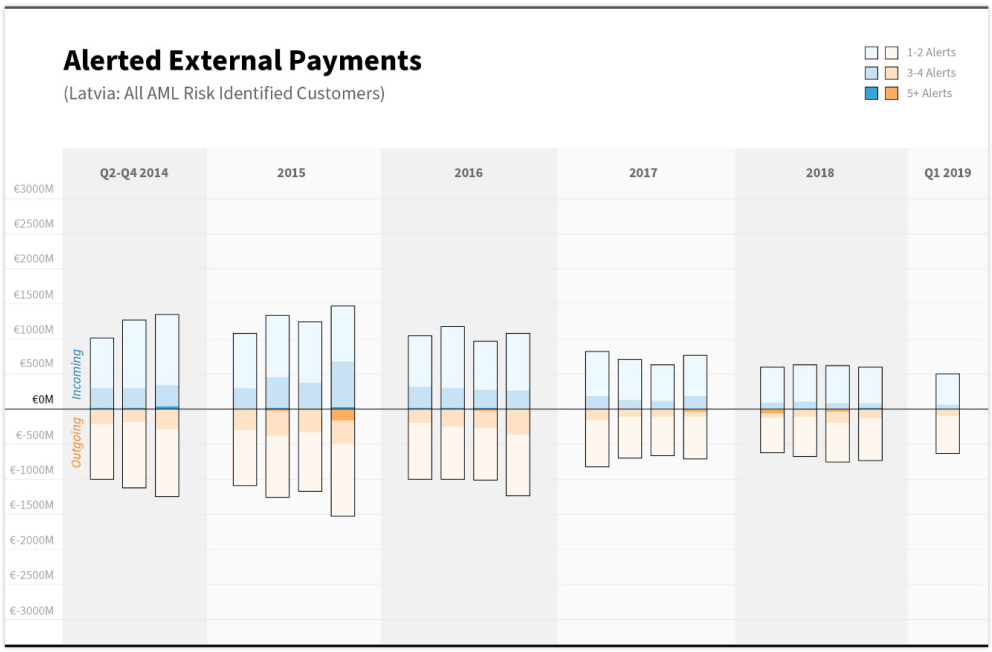
The following table shows (i) the value of external payment outflows for AML Risk Identified Customers that alerted on three or more algorithms throughout the AML Review Period and (ii) the total external payment outflows for Swedbank Latvia, within the calendar year or portion of calendar year analyzed. In total (across all currencies), there was the equivalent of €4.5 billion of external payment outflows that alerted on three or more algorithms throughout the AML Review Period, of which $2.4 billion was denominated in US Dollars.

TOTAL OUTFLOW ALERTING ON THREE OR MORE ALGORITHMS IN €'MILLION (LATVIA)

Category	Q2-Q4 2014	2015	2016	2017	2018	Q1 2019
AML Risk Identified Customer Transactions	694.1	1,540.4	1,113.3	515.8	576.6	96.8
Total Bank External Transactions - All Customer Transactions	19,091.6	26,260.7	25,752.5	26,336.1	28,476.2	6,476.1
AML Risk Identified Customer Transactions Alerted on 3 or more Algorithms as a Proportion of Total Transactions	3.6%	5.9%	4.3%	2.0%	2.0%	1.5%

Over the course of the AML Review Period, the proportion of total external payment outflows for all active Swedbank Latvia customers that consisted of external payment outflows for AML Risk Identified Customers that alerted on three or more scenarios decreased from 5.9% in 2015 to 1.5% in Q1 2019.

As discussed above, although some transactions alerted on only one scenario, other transactions alerted on multiple detection scenarios. The tables above set out the transactions that alert on three or more scenarios. The following chart sets out all of the alerted external payment inflows and outflows for all AML Risk Identified Customer subgroups during the AML Review Period, with shading to indicate the proportion of alerted transactions which triggered one or two alerts (light shading), three or four alerts (medium shading) and more than five alerts (dark shading). A table setting out the corresponding alerted values is set out at **Appendix D.2.**



3. Lithuania

a. HRNR Customers

The following table shows the number of active customers identified as HRNR Customers by year, along with the total incoming and outgoing external transactions performed by those customers.

	Lithuania		
	Active HRNR Customers	Incoming EUR'M	Outgoing EUR'M
2007	154	531.7	448.5
2008	79	409.8	453.2
2009	79	139.8	110.0
2010	85	355.9	309.4
2011	86	238.5	213.9
2012	98	346.2	311.4
2013	102	87.5	81.0
2014	109	108.0	91.5
2015	95	91.2	49.1
2016	87	87.4	35.3
2017	75	192.2	59.0
2018	64	258.7	114.4
2019 Q1	56	46.7	22.3
	225	**2,893.6**	**2,298.9**

For the entirety of the period analyzed, the proportion of the overall Swedbank Lithuania customer base that consisted of HRNR Customers was low: less than 0.01%.

The following table shows (i) the value of external payment inflows for HRNR Customers that alerted on three or more detection algorithms throughout the AML Review Period and (ii) the total external payment inflows for Swedbank Lithuania, within the calendar year or portion of calendar year analyzed. In total (across all currencies), there was the equivalent of €0.1 billion of external payment inflows that alerted on three or more algorithms throughout the AML Review Period.

TOTAL INFLOW ALERTING ON THREE OR MORE ALGORITHMS IN €'MILLION (LITHUANIA)

Category	Q2-Q4 2014	2015	2016	2017	2018	Q1 2019
HRNR Customer Transactions	1.9	7.2	4.5	63.4	59.5	12.5
Total Bank External Transactions - All Customer Transactions	34,712.0	28,799.6	29,740.8	32,873.8	38,793.4	8,734.7
HRNR Customer Transactions Alerted on 3 or more Algorithms as a Proportion of Total Transactions	0.01%	0.03%	0.02%	0.2%	0.2%	0.1%

Over the course of the AML Review Period, the proportion of total external payment inflows for all active Swedbank Lithuania customers that consisted of external payment inflows for HRNR Customers alerting on three or more detection algorithms was 0.1%, with the highest proportion being 0.2% in 2017 and 2018.

The following table shows (i) the value of external payment outflows for HRNR Customers that alerted on three or more algorithms throughout the AML Review Period and (ii) the total external payment outflows for Swedbank Lithuania, within the calendar year or portion of calendar year analyzed. In total (across all currencies), there was the equivalent of €0.1 billion of external payment outflows that alerted on three or more algorithms throughout the AML Review Period.

TOTAL OUTFLOW ALERTING ON THREE OR MORE ALGORITHMS IN €'MILLION (LITHUANIA)

Category	Q2-Q4 2014	2015	2016	2017	2018	Q1 2019
HRNR Customer Transactions	18.7	4.5	4.9	5.9	47.9	8.9
Total Bank External Transactions - All Customer Transactions	35,611.2	31,999.1	32,209.2	35,657.4	41,216.6	9,656.7
HRNR Customer Transactions Alerted on 3 or more Algorithms as a Proportion of Total Transactions	0.1%	0.01%	0.02%	0.0%	0.1%	0.1%

Over the course of the AML Review Period, the proportion of total external payment outflows for all active Swedbank Lithuania customers that consisted of external payment for HRNR Customers alerting on three or more detection algorithms was at or below 0.1%.

b. AML Risk Identified Customers

The following table shows (i) the value of external payment inflows for AML Risk Identified Customers that alerted on three or more algorithms throughout the AML Review Period and (ii) the total external payment inflows for Swedbank Lithuania, within the calendar year or portion of calendar year analyzed. In total (across all currencies), there was the equivalent of €3.2 billion of external payment inflows that alerted on three or more algorithms throughout the AML Review Period, of which $0.5 billion was denominated in US Dollars.

TOTAL INFLOW ALERTING ON THREE OR MORE ALGORITHMS IN €'MILLION (LITHUANIA)

Category	Q2-Q4 2014	2015	2016	2017	2018	Q1 2019
AML Risk Identified Customer Transactions	425.1	378.2	418.9	592.2	1,093.1	248.9
Total Bank External Transactions - All Customer Transactions	34,712.0	28,799.6	29,740.8	32,873.8	38,793.4	8,734.7
AML Risk Identified Customer Transactions Alerted on 3 or more Algorithms as a Proportion of Total Transactions	1.2%	1.3%	1.4%	1.8%	2.8%	2.8%

Over the course of the AML Review Period, the proportion of total external payment inflows for all active Swedbank Lithuania customers that consisted of external payment inflows that alerted on three or more detection algorithms for AML Risk Identified Customers was 1.8%.

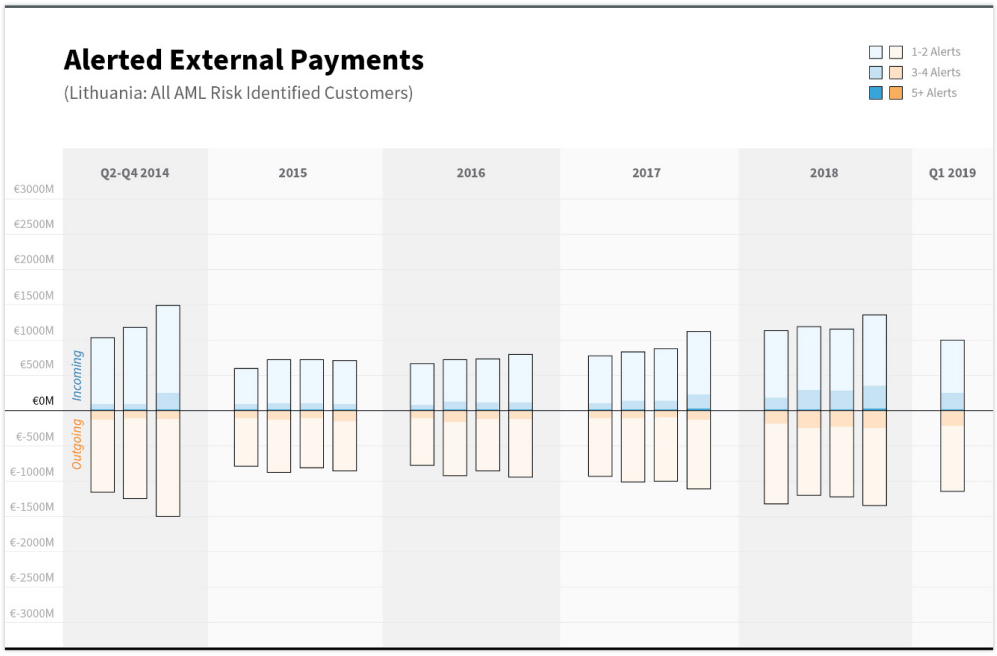
The following table shows (i) the value of external payment outflows for AML Risk Identified Customers that alerted on three or more algorithms throughout the AML Review Period and (ii) the total external payment outflows for Swedbank Lithuania, within the calendar year or portion of calendar year analyzed. In total (across all currencies), there was the equivalent of €3.0 billion of external payment outflows that alerted on three or more algorithms throughout the AML Review Period, of which $0.5 billion was denominated in US Dollars.

TOTAL OUTFLOW ALERTING ON THREE OR MORE ALGORITHMS IN €'MILLION (LITHUANIA)

Category	Q2-Q4 2014	2015	2016	2017	2018	Q1 2019
AML Risk Identified Customer Transactions	366.4	506.1	518.7	460.4	935.2	223.2
Total Bank External Transactions - All Customer Transactions	35,611.2	31,999.1	32,209.2	35,657.4	41,216.6	9,656.7
AML Risk Identified Customer Transactions Alerted on 3 or more Algorithms as a Proportion of Total Transactions	1.0%	1.6%	1.6%	1.3%	2.3%	2.3%

Over the course of the AML Review Period, the proportion of total external payment outflows for all active Swedbank Lithuania customers that consisted of external payment outflows for AML Risk Identified Customers that alerted on three or more detection algorithms was 1.6%.

As discussed above, although some transactions alerted on only one detection algorithm scenario, other transactions alerted on multiple scenarios. The tables above set out the transactions which alert on three or more scenarios. The following chart sets out all of the alerted external payment inflows and outflows for all AML Risk Identified Customer subgroups during the AML Review Period, with shading to indicate the proportion of alerted transactions which triggered 1-2 alerts (light shading), 3-4 alerts (medium shading), and 5+ alerts (dark shading). A table setting out the corresponding alerted values is set out at **Appendix D.3.**



D. Findings Regarding Swedbank's Public Disclosures about AML Compliance

The Investigation reviewed Swedbank's public statements regarding AML compliance, AML issues in the Baltics, CPB-1 and other related matters during the period of January 2014 through March 2019, in connection with an assessment of Swedbank's disclosures to investors about such matters. Disclosures to Swedbank investors during the period from October 2018 through March 2019 are of particular relevance for this analysis.

To begin with, investors can purchase Swedbank's ordinary shares, also known as A shares, which are listed on the Nasdaq OMX Stockholm. Investors are also able to invest in Swedbank through a sponsored Level 1 American Depositary Receipt ("**ADR**") program. Swedbank's ADRs are publicly traded in the United States on the OTC market, with one Swedbank ADR representing one Swedbank A share. Level 1 ADR issuers, like Swedbank, satisfy US disclosure requirements by publishing English language versions of their home market disclosures on their public website. In addition, Swedbank issues corporate fixed-income and debt securities through a series of funding programs, denominated in various currencies, including SEK, USD, and EUR.

We set forth below the relevant public statements or disclosures to investors by Swedbank or its executives that were reviewed by the Investigation, which is followed by an assessment of their sufficiency with respect to the matters identified in the Investigation.

1. Public Statements by Swedbank Regarding AML Risk and Compliance

a. Selected Relevant Public Statements Prior to October 2018

Swedbank made public statements related to AML compliance in the ordinary course of its public disclosure for years. These statements were largely general in nature or associated with specific events. Swedbank's disclosure related to AML issues evolved over time and increased in frequency and specificity over the Public Statements Review Period.

Discussion of Compliance Program/AML Compliance as a Priority

Most statements prior to October 2018 are of a generalized nature discussing Swedbank's overall compliance infrastructure. Below are representative statements from Swedbank's 2014 Annual Report, released on 17 February 2015:

> *To ensure that Swedbank complies with laws and regulations, we work to understand our customers, where their money comes from and the purpose of their relationship with the bank. This helps us to detect unusual behaviour. System support for monitoring domestic and international transactions and reconciliations of our customer database against sanction lists also reduce risks in our operations – both financial and brand related.*[47]

[47] Swedbank, 2014 Annual Report, at 15 (February 2015), https://online.swedbank.se/ConditionsE archive/download?bankid=1111&id=WEBDOC-PPE1340996. In addition, the 2014 Annual Report characterized anti-money laundering among its list of "[o]ther major issues in 2014" (id. at 46) and Bank management included anti-money laundering as a "[f]ocus area in 2014" (id. at 50). The Swedbank Board again characterized anti-money laundering among its list of "other major issues" in the 2015 Annual Report. Swedbank, 2015 Annual Report, at 50 (February 2016), https://online.swedbank.se/ConditionsEarchive/download?bankid=1111&id= WEBDOC-PPE1341044. AML was again among the Board's other major priorities in the 2016 Annual Report. Swedbank, 2016 Annual Report, at 42 (February 2017), https://online.swedbank.se/ConditionsEarchive/download?bankid=1111&id=WEBDOC-PPE1341227. "Know Your Customer (KYC) and Anti-money laundering (AML)" was cited as a management focus area in the 2016 Annual Report. Id. at 46.

Substantially similar statements appear in Swedbank's 2015 Annual Report:

> *To ensure that Swedbank complies with laws and regulations, we have to know our customers and understand where their money comes from and what the aim of their relationship with the bank is. This makes it easier to detect abnormal behaviour. Through our system support for monitoring transactions and by checking customer databases against sanctions lists, we reduce the risk that the bank will be used for money laundering or terrorist financing. . . . Five stages in our work to counter money laundering: 1. Risk assessment; 2. Customer knowledge; 3. Continuous monitoring; 4. Audits; 5. Reporting.*[48]

In its 2016 Annual Report, Swedbank stated that:

> *In payments, we constantly address key risks related to money laundering and terrorist financing. Through system support to monitor transactions, customer screening against sanction lists and the bank's Know Your Customer (KYC) process, we work continuously to minimise these risks in our business.*[49]

Moreover, Swedbank stated in its 2017 Annual Report that:

> *In addition to stress tests of our credit portfolio and sustainability risk analysis in our lending, it is important that we minimise risks in the payments area to combat money laundering and terrorism financing. Through the bank's Know Your Customer (KYC) process, we perform the statutory customer due diligence, and with system support we monitor transactions and screen customer databases against sanction lists.*[50]

The 2017 Annual Report further describes that "*[a]nti-money laundering and countering terrorist financing policy*" is an "*integral part of the annual report*,"[51] that "*[a]ll employees have a responsibility to live up to the bank's policies and guidelines to prevent corruption and money laundering*" and that "*[s]ince payment flows are part of our core business, it is important that we prevent illegal activities such as terrorist financing, money laundering*."[52]

Regulatory Event-Specific Public Disclosures

Swedbank's public statements also included information about AML-related regulatory developments in the Baltics. On 23 November 2016, Swedbank issued a press release disclosing that the Latvian Financial and Capital Market Commission issued examination findings related to the effectiveness of Swedbank's internal control systems for the prevention of money laundering in Latvia. Swedbank's press release stated that:

> *The findings include deficiencies in internal control systems, processes and documentation. Based on the audit results, the Commission and Swedbank Latvia have entered into an administrative agreement. The agreement includes a fine of EUR 1.36 million and a series of mitigating actions. Swedbank takes the findings in the Commission's audit very seriously. Swedbank is committed to actively working towards further improvement of our internal control system and elimination of any shortcomings and has cooperated fully with the Latvian authorities.*

Similarly, Swedbank issued a press release on 15 February 2018, disclosing the results of an inspection conducted by the Bank of Lithuania. The press release stated that:

48 2015 Annual Report, at 17.

49 2016 Annual Report, at 18.

50 Swedbank, Annual and Sustainability Report 2017, at 18 (February 2018), https://online.swedbank.se/ConditionsEarchive/download?bankid=1111&id=WEBDOC-PRODE30065852.

51 Id. at 174.

52 Id. at 180.

The findings include deficiencies in internal control systems for money laundering prevention, processes and documentation. Based on the results, Bank of Lithuania issued a warning to Swedbank and obliged to remedy identified deficiencies. Swedbank takes the findings by Bank of Lithuania very seriously. We would like to emphasize that AML and CTF is a prioritised matter for Swedbank. We are allocating significant efforts and resources to ensure AML/CTF compliance and we are committed to continuously improve our AML/CTF processes. . . . Swedbank has already initiated actions to implement a series of measures aiming to improve its internal control systems, to ensure relevant customer due diligence data and to enhance processes and routines. And thereby, the deficiencies pointed out by Bank of Lithuania, has partly already been corrected. A warning is the lowest level of sanction that the Bank of Lithuania can issue.[53]

b. The 3 October 2018 Bloomberg Article

As noted above, on 19 September 2018, CPB-1's Head Office published the *Public Report on CPB-1* and issued a press release regarding its findings. The findings in the Public Report on CPB-1 were widely reported by the global media and closely tracked by financial regulatory authorities.

On 3 October 2018, Bloomberg News published an article titled "*Estonia Banks Did $500 Billion in Cross-Border Flows*" that discussed the Public Report on CPB-1 and referenced other financial institutions active in the Baltics, including Swedbank. The Bloomberg article contained a statement by Swedbank that "*[w]e have worked continuously throughout the years together with authorities and correspondent banks, to secure that we have thorough systems and processes connected to AML*." The next day Swedbank issued a press release in response to the publication of the Bloomberg article stating that:

> *First of all, Estonia, Latvia and Lithuania are together with Sweden home markets to Swedbank. We run full banking operations and focus on domestic customers and business. As the market leader we have continuously worked with AML and have a systematic approach to assure that we detect suspicious transactions and business activities. In these efforts we work closely with authorities, regulators as well as with correspondent banks. We have always had zero tolerance against money laundering in all markets where we operate. As the market leader we have had a continuous dialogue with the governments and the regulators to strengthen the financial system and infrastructure, we see this as part of our responsibility.*
>
> *With regards to non-resident customers, Swedbank has a relatively low share[;] it represents less than 1.5% of all of Swedbank´s customers in the Baltic countries. However, in payment transactions is where money laundering is detected and this is where the focus should be.*
>
> *The ability to detect and act on suspicious transactions is key. The focus of our AML efforts is to secure systems and processes in order to scrutinize transactions and detect suspicious transactions rather than solely focus on the residency of the customer. Residency is part of the KYC and on-boarding process and Swedbank's policy is to bank customers with clear local business ties.*
>
> *Based on our approach we have throughout the years reacted on all signals, from our own channels as well as from external parties. We are not [a] USD clearer ourselves in those markets. There are currently no ongoing investigations into our bank from any of our regulators concerning AML-practices.*

[53] Swedbank, Bank of Lithuania issues inspection findings on Swedbank, Press Release (15 February 2018), www.swedbank.com/newsroom/press-releases.details.1D3675CAF955CB17.html. Swedbank also disclosed the Bank of Lithuania settlement in its 2017 Annual Report, at 25.

Despite the negative news flow on AML related issues in the Baltic countries, we welcome the development we have seen in recent years, where national and international authorities and politicians have been working intensively to increase transparency in their respective countries. We remain confident that the financial system in each country is sufficiently robust and the economies are strong and diversified enough to manage while the various measures are firmly being established and implemented.

Following the publication of the Bloomberg article the Estonian central bank published a press release that can be found here: https://www.eestipank.ee/en/press/bloomberg-has-mistaken-cross-border-payments-non-resident-flows-03102018[.][54]

On 4 October 2018, in an interview with Dagens Industri ("**DI**") conducted in Swedish, a senior manager in Group Communications stated that:

We have done our own review of the transactions that took place between us and [CPB-1], that is, transactions made by our customers with customers of [CPB-1], during 2007 to 2015. We have done this because of the reporting that has been in the media and the data that [CPB-1] has released. . . .

The review is finished, and we have worked just as we always do when we monitor transactions. In cases where we see warning signals, we act and report to the relevant authorities.

Did you find any transactions that you had missed?

We do not comment on the transaction monitoring we do. If there are instances of warning signs, then we act, and if necessary we report to the relevant authorities.

So you confirm that you have done this review but do not want to present the conclusions?

Also after this review, we feel comfortable with the customers we have in the Estonian market. These are ordinary households and ordinary companies where we have asked questions to ensure that they are connected to Estonia.

c. The Q3 Interim Report – 23 October 2018

Swedbank released its Q3 2018 Interim Report ("**Q3 2018 Interim Report**") and held a telephonic conference call with analysts on Tuesday, 23 October 2018 ("**Q3 2018 Telephone Conference**"). The Q3 2018 Interim Report stated:

Focus on domestic customers in all home markets

During the year, and particularly in the last quarter, growing attention has been paid to how banks are preventing money laundering and other financial crime. For Swedbank it has always been high on the agenda. With a market-leading position in all four of our home markets comes a responsibility to help develop and strengthen the financial system and financial infrastructure. We take responsibility by closely dialoguing with supervisory authorities and decisionmakers in each country. We have also worked systematically and proactively to monitor payment flows in order to detect potential fraud. Our corporate culture and business model are the main preventive measures, however. Swedbank is a values-driven bank. We have zero tolerance for

[54] Swedbank, Comment on Bloomberg Article, Press Release (4 October 2018) ("4 Oct. Press Release"), www.swedbank.com/newsroom/press-releases.details.825D2E8025C088A9.html

any type of criminal activity and have always taken decisive action when we received signals from within or outside our own organisation indicating suspicious transactions. Our focus has always been on domestic corporate customers and private customers in all our home markets. We have the same principles and framework throughout the Group with respect to money laundering, knowing the customer, and risk. Financial crime is evolving and can be unpredictable. We therefore continuously adapt our processes to ensure that we are protecting our customers and to further increase transparency in our home markets.[55]

Swedbank prepared a slide deck to go along with its presentation of the Q3 2018 Interim Report ("**Q3 2018 Results Presentation Slides**") with five slides under "*Swedbank in the Baltics*," containing information regarding Swedbank's customers in the Baltics, the levels of non-resident customers, Swedbank's payments market share and the level of Swedbank's cross-border payments. The Q3 2018 Results Presentation Slides also stated:

We have continuously worked with anti-money laundering

- *Systematic approach to assure detection of suspicious transactions and business activities*
- *Systematic approach to KYC and on-boarding process*
  - *Swedbank's policy is to serve customers with clear local business ties*
  - *Work closely with authorities, regulators as well as with correspondent banks*
- *Zero tolerance AML in all markets where we operate*
  - *Throughout the years reacted on all signals, from our own channels as well as from external parties.*
  - *Same governance, systems and processes to detect money laundering on all our markets*
- *No ongoing investigations from any of our regulators concerning AML-practices*[56]

The CEO stated in opening remarks for the Q3 2018 Telephone Conference:

The second thing is that on top of the fact that you need to develop your KYC constantly, you need to develop your systems and your processes. You know well that we are a low-risk bank, and this goes for this too. And I think that one of our strengths is that we are humble enough to realise that money laundering is something that is extremely complex. However much we do, we will never be able to detect everything ourselves. And this is why we work actively and reach out proactively to other banks – foreign banks as well as domestic – to the regulator, the police, etc. This is extremely important, and I sometimes get the question: do you think that you have everything in place to detect this? I think with the help from our friends and the proactive attitude that we have, I think we are in a really good shape.

[55] Swedbank, Q3 2018 Interim report January-September 2018, at 2 (23 October 2018), https://online.swedbank.se/ConditionsEarchive/download?bankid=1111&id=WEBDOC-PPE1341775.

[56] Swedbank, Swedbank's Third Quarter 2018 Results, at 7 (undated), https://online.swedbank.se/ConditionsEarchive/download?bankid=1111&id=WEBDOC-PPE1341777. This same slide also appears in Swedbank, Swedbank Investor Presentation, at 90 (December 2018) ("Q3 2018 Investor Presentation Slides"), https://online.swedbank.se/ConditionsEarchive/download?bankid=1111&id=WEBDOC-PPE1341768.

> *But the third thing, and the most important thing, is the fact that every time we detect a laundering attempt, we act, and we act forcefully. We investigate, and if there are things we don't like, we act immediately.*[57]

During the Q3 2018 Telephone Conference, Swedbank received a number of questions from the participants regarding AML issues in the Baltics. A research analyst asked about customers from Russia or the Commonwealth of Independent States. The CEO confirmed that 0.5 percent of the Baltic Subsidiaries' customers are from Russia or the CIS. The analyst then pointed out that 0.5 percent is approximately 15,000 customers, a similar number of customers to the amounts reported in the Public Report on CPB-1.[58]

Another research analyst asked about the 15,000 CIS customers and transaction flows, specifically asking Swedbank to confirm if it has "*looked at [its] client base back in 2008-15 to determine that [it] did not have what [CPB-1] was kind of classifying as suspicious clients? And I think they [CPB-1] looked at the residency and the source of funds*." The analyst further asked if Swedbank had done any kind of spot checking for a similar situation.[59]

In response, the CEO stated "*yes, just to answer your last question first, because that's very short: yes, we have*."[60] The analyst then asked the CEO to "*quantify what the outcome was*." The CEO replied: "*No, I can – yes, I can say to you that we didn't have any of the names that were in the [Public Report on CPB-1]; they had not been – they are not current clients of ours. And we've gone through the time from 2007 until now, and they haven't been. So we've checked for everything*."[61]

The CEO also spoke to the media on 23 October 2018, and in an appearance on CNBC, the CEO stated:

> *I think the important thing in this money-laundering case that we see one of our competitors have in Estonia is the fact that Swedbank is completely different. We run a retail bank in four countries. We focus on domestic corporates and domestic private individuals and that is a completely different setup. I also think that there is a difference in the fact that we are a low risk bank and that goes for AML and money laundering too. We work with KYC, we work with systems, we work with monitoring. But we are also humble enough to understand that this is a really, really complex issue so we reach out, we reach out to US banks, to domestic banks, to regulators, to the police and get all the help we can from everybody else.*

The CEO also reiterated in the CNBC interview that "*every time we see anything, we act and we act forcefully. And that, that we've done for years. And that is a big difference*."

On the same day, the CEO was quoted in Swedish in the Swedish newspaper TTELA as stating that: "*most important of all, every time we see something, we act, and that with force*." The article further quotes the CEO as explaining that "*[a]s a bank, you have to be aware that there is a risk*." The article then includes the question "*[b]ut you haven't seen anything more in the Baltics?*" to which the CEO is reported to have responded "*[n]o, we haven't*." The article then states the question "*[h]ow confident can you be that you don't have any dirty laundry in the Baltics?*" and a response by the CEO of "*[w]ith all that has come up in this story around [CPB-1], I can be absolutely sure, we have gone through everything.*"

In an interview with the newspaper Svenska Dagbladet on the same day, the CEO is reported to have stated that there was a "*huge difference*" between Swedbank's non-Estonian customers and those of CPB-1:

[57] Swedbank, Transcription: Swedbank Third Quarter Report 2018, at 3 (23 October 2018) ("Q3 2018 Telephone Conference Transcript"), https://online.swedbank.se/ConditionsEarchive/download?bankid=1111&id=WEBDOC-PPE1341801.

[58] Id. at 8.

[59] Id. at 11.

[60] Id.

[61] Id. at 11.

To be a Swedbank customer, you must have a physical link to the country. You must have a factory there, or a sales office or some other type of business. For example, if you are a private customer, you must have an employment in an Estonian company or be enrolled in a university.

You have reviewed your transactions with [CPB-1] 2007-2015, what did you find?

Yes. We found nothing. We have reviewed all customers who were included in the media reporting on [CPB-1] and none of them are, or have been, customers in Swedbank. Not a single one.

Isn't that strange?

No, it is not strange at all. All those customers are very much non-residents. They do not operate any business in Estonia. That they were not with us is not strange at all. . . .

You have 3.3 million customers in the Baltics, how do you know exactly what they are up to?

We monitor our customer register continuously. We divide them into risk classes and update once a year. So we know if customers change their behavior. If a foreign company stops manufacturing in Estonia, we see this immediately.

The CEO likewise was quoted as stating in an interview with DI on 23 October 2018 that Swedbank had "*gone through everything and there is nothing.*" The CEO added, "*[w]e have gone through all the names that you have seen in the media and in the [Public Report on CPB-1], and we have gone through it from 2007 and up until today, and there are none of them who have been customers in Swedbank*."

d. The 2018 Annual Report – 20 February 2019

Swedbank's 2018 Annual and Sustainability Report ("**2018 Annual Report**") was released on 20 February 2019,[62] the same day as the airing of the first of three episodes ("**20 February SVT Episode**") of the SVT *Uppdrag granskning* television program regarding Swedbank ("**SVT Program**").[63] The 2018 Annual Report made the following statements related to AML:

An important topic during the year was what banks are doing to prevent money laundering and other financial crime. For Swedbank, this issue has always been top of mind. With a market-leading position in all four of our home markets comes a responsibility to help strengthen the financial system and infrastructure. In our case, we maintain a close dialogue with supervisory authorities and decision-makers in each country. We have also worked systematically and proactively to monitor payment flows and detect potential irregularities. Our corporate culture and business model are the main preventive measures, however. Swedbank is a value-based bank. We have zero tolerance for any type of crime in our operations and have always acted resolutely when we receive indications from in- or outside the organisation of suspicious transactions. Our focus has always been on local corporate and private customers, in all our home markets. We apply the same principles throughout the Group with regard to money laundering, know-your-customer (KYC) and risk. Financial crime is ever-changing, however, so we will continue to adapt our processes to ensure that we protect customers and further increase transparency in our home markets.[64]

[62] Swedbank's Annual Report 2018 published, Press Release (20 February 2019), www.swedbank.com/newsroom/press-releases.details.F5515630FB30E09A.html.

[63] The second episode of the SVT report aired on 27 February 2019 and the third episode aired on 27 March 2019.

[64] Swedbank, 2018 Annual and Sustainability Report, at 6-7 (February 2019), https://online.swedbank.se/ConditionsEarchive/download?bankid=1111&id=WEBDOC-PRODE29146126.

Zero tolerance for money laundering

Swedbank is the leading bank for many households and businesses in its four home markets: Sweden, Estonia, Latvia and Lithuania. To maintain the bank's strong reputation, measures are taken continuously to combat corruption, money laundering and terrorist financing. An established "Know-Your-Customer" process, system support for monitoring transactions and reconciliations of customer databases against sanctioned lists are all in place to minimise these risks. Banks are obligated to report suspicions of market abuse such as insider trading, market manipulation and unlawful disclosure of inside information. According to the Anti-Money Laundering Act, banks are also obligated, without delay, to report suspicions of money laundering or terrorist financing to the Financial Intelligence Unit of the Swedish Police. Close cooperation with supervisory authorities and correspondent banks is necessary for this type of work. The fight against money laundering is global, as are the processes and systems. The bank has zero tolerance for money laundering in the markets where it is active and has taken action over the years when it sees any signs in its own channels and from outside partners. As a leading bank, Swedbank also has a responsibility to contribute to a continuous dialogue with supervisory authorities in order to strengthen the financial system and infrastructure. Extensive measures to fight corruption are integrated in the bank's business processes and in loan assessments, the supply chain, payment flows and investments. All employees receive mandatory online training to recognise transaction patterns, behaviours and situations that could constitute, or be associated with, money laundering and corruption.[65]

Internal rules

To prevent its payment systems from being exploited for criminal activity, Swedbank has built up a set of internal rules, processes and support functions to ensure that we comply with applicable laws and regulations in the area. Swedbank has an obligation to know all its customers, ***understand*** *where their money comes from and why they want a relationship with the bank, to better detect unusual behaviour.*

Through the a [sic] "Know Your Customer" process, system support to monitor transactions and reconciliations of customer databases against sanction lists, Swedbank minimises these risks.[66]

e. Other February-March 2019 Communications

(i) The SVT Programs

The 20 February SVT Episode featured footage of both the CEO and a senior manager in Group Communications, including the use of video clip flashbacks to statements made in the third quarter of 2018. These clips included video of the CEO being asked about Swedbank's investigation into transactions with CPB-1 and answering: "*[w]e looked into all the customers who were uncovered by [CPB-1] and none are customers in Swedbank*." The 20 February SVT Episode then showed a historical video clip of the *CEO being asked "[b]ut don't you also have international customers who, say, transfer money from Russia like the [CPB-1] customers?" In the clip, the CEO responded: "[n]ot customers who don't have any business activities in the country."*

The 20 February SVT Episode also contained segments from an interview of a senior manager in Group Communications. When asked how the CEO's remarks differentiating Swedbank from CPB-1 could be true, the senior manager stated that:

[65] Id. at 15-16.
[66] Id. at 202.

What we said last autumn, which is still true, is that we are working to prevent money laundering. One of the indicators we look at is exactly what you're talking about: checking that people and businesses have ties to our countries. Remember that money laundering is highly criminal activity, and one of the biggest challenges in our industry. Criminals keep changing their approach, and we need to adapt our systems. But one of our most important messages then and now is that when we see signs, we act on them.

SVT ran a second episode on 27 February 2019 which included additional video footage of the CEO stating in October 2018 that: "*[w]e are constantly monitoring everything that goes through the bank according to our risk plans. But what is important to me is that we act. You can rest assured that we're on top of things . . . Every time we see anything, we act, and we act forcefully*."

In this episode, SVT presented documents showing that well-known individuals from Russia and the CIS had Swedbank accounts. SVT asked a senior manager in Group Communications how the CEO "*went to the media last fall and said that you didn't have these types of scandals*," and the senior manager responded that the CEO was "*primarily talking about [] the names that figured in [CPB-1] and their business model*." The senior manager also stated that "*efforts to prevent money laundering are like a jigsaw puzzle. We, like you have done, look for risk indicators. And when we do that, naturally once you have all the pieces in place, we sometimes see that we could have acted on the first piece. But that's easy to say when the puzzle is finished*."

(ii) 20 February 2019 Telephone Conference

On 20 February 2019, Swedbank held a telephone conference call with industry representatives, including analysts and investors in response to the fallout from the 20 February 2019 SVT episode. On the call, the CEO stated:

So also as we've mentioned to many of you already, during the past ten years the activities have changed shape and form as the regulation regarding AML has developed and our own internal processes and approach has been strengthened and we act in a way that is helped by our monitoring systems in reply to all the suspicious transactions.

So at various points in time we've taken actions by actively off-boarding customers that no longer fulfill our requirements. As we mentioned in October, when [CPB-1] blew up, so to speak, on top of the fact that we have been monitoring suspicious activities continuously for a long time, we also initiated a look back, which I talked about to many of you, analysts, investors and also media. And in this look back what we did was that we talked to – we took in external help. We thought that it was good and useful for us to get external eyes on our own systems and everything that we found. And we used risk indicators on transaction data between [CPB-1] and Swedbank between seven and 15. And we concluded that what we saw was acted on and I think that this is important to repeat; that there's nothing new.

I also have questions today that when [CPB-1] first hit the media there was a number of customers – a small number, it was six or seven – mentioned and upon a question from media I replied that none of these are customers of Swedbank. That still holds. Since October, we've taken further actions. We continue to work with this. We continue to do deep dives into things that we see and that is actually nothing out of the ordinary as such.

(iii) Other Public Statements

In a 20 February SVT News article, the CEO defended statements made in October 2018, stating:

> *I referred to the customers who appeared in the [CPB-1] inquiry. A number of customers were revealed, I think it was eight, and I said then that they are not customers in Swedbank - and that is absolutely true. We are clean in that we act on everything we see, it is a very important message.*

The same article quoted a senior manager in Group Communications, who was interviewed for the SVT Program. The senior manager was asked how much suspected money laundering Swedbank had identified.

> *I can't answer that. Looking for suspicious transactions, or something we suspect may be a problem, is something that is going on every day in almost all banks.*
>
> ***So you haven't looked into how much, to what extent?***
>
> *Absolutely, but I can't share it with you.*
>
> ***Why not?***
>
> *Because we have decided that we are not talking about it. There are several reasons, there is bank secrecy, there is a disclosure prohibition so there are other reasons why we are not sharing this. But you can be absolutely certain that we are on top of this.*

Asked about regrets over "*how she has expressed herself around all questions about how much she knew*" in a 5 March 2019 TTELA interview, the CEO responded:

> *My ambition is to be open and straight . . . but what I also realize after the reporting last week is that the context, nuance and complexity are lost as well when I have expressed myself as I have done. . . . This is a large and complicated question . . . I think I have underestimated the importance of context. . . . I should have provided more context. Because what I said was not wrong. But I should have provided more context.*
>
> ***TT: Did you mean that after 2015 you haven't found anything more suspect?***
>
> *I don't really want to answer that, because now we have set up an investigation. We also have all the investigations by the authorities.*

Finally, a 22 March 2019 Wall Street Journal article quoted the CEO as saying that Swedbank should have provided more context when the CEO said in October that suspicious customers identified with CPB-1 did not have accounts at Swedbank: "*We should have taken a step back and explained that attempts of money laundering were happening all the time in all markets, and how we work through this systematically*."

2. Assessment of Public Statements or Disclosures to Swedbank Investors

When considered against the facts developed by the Investigation, certain disclosures or statements made during the period between October 2018 and March 2019 by Swedbank, its then-CEO and a senior manager in Group Communications, concerning Swedbank's historical AML compliance, current AML compliance, and exposure to CPB-1 and its customers, were either inaccurate or failed on multiple occasions to provide sufficient clarity and context.

a. Reaction to Money Laundering

Swedbank consistently made statements over the years and, in the Fall of 2018 and into 2019, with increasing frequency about its reaction to potential money laundering activity. For example, in a press release on 4 October 2018, Swedbank stated that it had "*throughout the years reacted on all signals, from our own channels as well as from external parties*."[67] Swedbank also used messaging like "*every time we see anything, we act and we act forcefully*." Sometimes, multiple messages along these lines were made during the same disclosure or event.[68]

Swedbank's efforts over the years to detect and react to money laundering issues are detailed in Section [VII.A.] of this Report. Detection efforts included enhancements to the Group's transaction monitoring and other systems discussed above, as well as the investigations and remediation programs conducted in Project Clear and Project Nemo. Swedbank's reactions to what it detected included, among other things, the termination of relationships with a substantial number of customers. While Swedbank did take steps to address and remediate AML issues, especially since 2016, the investigation revealed that Swedbank's historical AML efforts were not always adequate to mitigate money laundering risk.

b. Zero Tolerance for Money Laundering

Swedbank made statements that it had "*zero tolerance*" for money laundering in the 4 October Press Release, Q3 2018 Investor Presentation Slides,[69] and the 2018 Annual Report. [70] "*Zero tolerance*" messaging was also used during live presentations and interviews, including on the Q3 2018 Telephone Conference. [71]

The detection and remediation efforts explained in Section [VII] of this Report demonstrate Swedbank's intention to identify suspicious activity and to off-board suspicious clients. While Swedbank's efforts were at times inadequate or incomplete, our investigation did not conclude that Swedbank tolerated actual money laundering at the time the statements were made.

c. Systematic Approach to Detect Money Laundering

Swedbank made statements that it had a "*systematic approach to assure that we detect suspicious transactions and business activities*."[72] Other formulations of this message included that Swedbank worked "*systematically and proactively to monitor payment flows and detect potential irregularities*."[73]

As explained in Section [VII.A.] of this Report, Swedbank had in fact implemented manual and electronic processes and systems over the years to help it detect suspicious activity, although these processes and systems may not, in all respects, have met industry standards and did suffer deficiencies. Deficiencies in Swedbank's electronic processes and systems hindered Swedbank's ability to detect suspicious transactions and activities during the Public Statements Review Period. Notably, however, Swedbank often tempered statements regarding its detection methods with statements about the complexity of money laundering and the impossibility of detecting every attempt.[74] Swedbank could have added additional context about the limitations of its processes and systems, as they did not always meet industry standards and had significant deficiencies over the years.

[67] 4 Oct. Press Release.

[68] E.g., during the Q3 2018 Telephone Conference, Swedbank stated "every time we detect a laundering attempt, we act, and we act forcefully." Q3 2018 Telephone Conference Transcript, at 3. The Q3 2018 Results Presentation Slides used during the analyst call state "[t]hroughout the years reacted on all signals, from our own channels as well as from external parties." Q3 2018 Results Presentation Slides, at 7.

[69] Q3 2018 Investor Presentation Slides, at 90.

[70] 2018 Annual Report, at 6, 15.

[71] Q3 2018 Telephone Conference Transcript, at 7.

[72] 4 Oct. Press Release.

[73] 2018 Annual Report, at 6.

[74] See, e.g., Q3 2018 Telephone Conference Transcript, at 3.

d. Swedbank's Exposure to CPB-1 and its Customers

Swedbank regularly highlighted differences in business mix and scope between its Baltic Subsidiaries and CPB-1. These statements alone, based on the Investigation, were generally accurate. For example, in the Q3 2018 Investor Presentation Slides, Swedbank directly compared aspects of its business to CPB-1 and others. One slide titled "*Swedbank's payments market share shows a business model built on a domestic customer base*" compared Swedbank's market share by balance sheet in the Baltics (between 40% and 50% from 2008 through 2015) to those of certain peers (*e.g.*, CPB-1 at around 10%).[75] This slide also showed each bank's market share of outgoing cross-border payments. Swedbank's share of outgoing cross-border payments remained relatively stable at around 20% to 30%.

By contrast, CPB-1's share of outgoing payments increased from just under 30% in 2009 to over 40% in 2013 (despite a much lower balance sheet market share than Swedbank) before decreasing sharply in 2014 and 2015. This slide could have given the impression that Swedbank's market share of outgoing payments aligned more with the scope of its business in Estonia than the businesses of CPB-1 and others. Another slide emphasized Swedbank's low overall number of non-resident customers in the Baltics (*i.e.*, less than 1.5%).[76] This number contrasted with the approximately 2% – 4% numbers cited in the Public Report on CPB-1.

Between October 2018 and March 2019, Swedbank, its then-CEO, and a senior manager in Group Communications, made a number of statements related to Swedbank's internal investigation of its exposure to CPB-1 and CPB-1 counterparties. Swedbank and its executives provided insufficient context in statements, responses to questions about the scope of its investigation, and findings about its exposure to CPB-1 and its customers.

During October 2018, analysts and interviewers asked the CEO several questions about Swedbank's investigation in response to the Public Report on CPB-1 and whether Swedbank found evidence of suspicious activity similar to that described by CPB-1. Internal reports indicated that none of the six to eight CPB-1 customers identified in the media were customers of Swedbank. The CEO highlighted this fact. The CEO did not mention any of the other findings from the September 2018 CPB-1 Report.

The CEO confused this statement, however, by using imprecise language and overstating the work that had been performed when responding to questions. For example, asked if Swedbank had gone through its transactions with CPB-1 from 2007 through 2015, the CEO responded: *"Yes. We found nothing. We have reviewed all customers who were included in the media reporting on [CPB-1] and none of them are, or have been, customers in Swedbank. Not a single one."* Standing alone, the statement that Swedbank "*found nothing*" is incorrect in light of Swedbank's findings in its September 2018 CPB-1 Report. Asked about this statement by Clifford Chance, the CEO said that "*[y]es. We found nothing*" was intended to mean that no CPB-1 customers named in the media were customers of Swedbank. The CEO said that the statement was not intended to mean that Swedbank "*found nothing"* when it reviewed transactions with CPB-1 and CPB-1 counterparties from 2007 through 2015. While the CEO tried to clarify the scope of the initial statement in the remaining response, the CEO's use of imprecise language, and the word "*nothing*," could have left an impression that Swedbank did not have connections to CPB-1, including transactions between CPB-1 counterparties and Swedbank counterparties, and that Swedbank had identified no potential CPB-1-related exposure.

The CEO also failed at times to expressly limit statements to just the names identified "*in the media.*" When asked on the Q3 2018 Telephone Conference if Swedbank had conducted "*any kind of spot check*" for customers that CPB-1 was *"classifying as*

[75] Q3 2018 Investor Presentation Slides, at 88.
[76] Id. at 87.

suspicious clients" based on residency and source of funds, the CEO responded "*yes, we have.*"[77] This response was accurate. However, the CEO continued:

> *I can say to you that we didn't have any of the names that were in the [Public Report on CPB-1]; they had not been – they are not current clients of ours. And we've gone through the time from 2007 until now, and they haven't been. So we've checked for everything.*[78]

The reference here to "*names that were in the [Public Report on CPB-1]*" rather than to "*media reports*" (the intended message) is confusing, as the Public Report on CPB-1 did not name specific customers. Use of the phrase "*checked for everything*" also overstated the scope of Swedbank's review of its CPB-1-related exposure or was incomplete, without further information regarding the results of Swedbank's review. Overall, this response could have left an impression that Swedbank had examined its entire customer base from 2007 through 2018 to identify customers that CPB-1 was "*classifying as suspicious clients,*" which, without further disclosure of the results of Swedbank's internal reviews, was inaccurate. The CEO maintained, when interviewed by Clifford Chance, that the CEO intended to limit the statements about the results of Swedbank's review to its conclusion that none of the small number of CPB-1 customers named in the media were now, or ever had been, Swedbank customers.

In response to questions from an SVT interviewer about external experts reviewing transactions between Swedbank and CPB-1, the CEO stated *"[w]e looked into all the customers who were uncovered by [CPB-1] and none are customers in Swedbank.*" This statement could have given the impression that Swedbank knew the names of "*all customers*" uncovered in the CPB-1 investigation and had investigated them. However, as noted, CPB-1 never publicly identified the customers uncovered in the investigation, and there is no evidence that the CEO possessed a non-public list of CPB-1 customers.

Swedbank also provided insufficient context in statements about its own historical AML issues and off-boarding and whether it had historical issues like those uncovered at CPB-1. At the time, the CEO knew about Project Clear and Swedbank's historical customer off-boarding projects in the Baltics. Slides prepared by other Swedbank executives and shared with the CEO showed the significant impact on cross-border payment volumes in the Baltics caused by the off-boarding.

Statements attributed to the CEO by the media could have created an impression that Swedbank had no CPB-1-like exposure to AML-related issues. For example, according to TTELA, when asked during a media appearance how certain the CEO could be that Swedbank did not have any "*dirty laundry*" in the Baltic region, the CEO responded "*[w]ith all that has come up in this story around [CPB-1], I can be absolutely sure, we have gone through everything.*" The statement that TTELA attributed to the CEO could have left the inaccurate impression that Swedbank conducted a thorough review of its Baltic business and found no AML-related issues (systemic or otherwise) in its Baltic Subsidiaries similar to those disclosed in the Public Report on CPB-1. Contrary to this statement, Swedbank had conducted the review culminating in the September 2018 CPB-1 Report that found material connections to CPB-1 and its counterparties and AML deficiencies in its Baltic Banking operations. When questioned about the statement published by TTELA, the CEO believed that it originated from a teleconference with news organizations. The CEO maintained that the statement was intended to be limited only to Swedbank's review of its historical and current customer base against the few CPB-1 customers named in the media, and that the CEO was unfamiliar with the term "*dirty laundry.*"

[77] Q3 2018 Telephone Conference Transcript, at 11.
[78] Id.

E. Findings Regarding Swedbank's Communications with Banking Regulators

The Investigation did not conclude on the available evidence that Swedbank or the Baltic Subsidiaries knowingly provided false information to regulators. The Investigation did, however, identify some instances where Swedbank and the Baltic Subsidiaries may not have provided adequate context in their responses to regulatory requests, may have failed to provide updated information, or may have interpreted a request in an overly technical or narrow manner. In considering these instances, it is important to note that a bank typically has constant interaction with its regulators, and that the instances listed below should be fairly considered in the context of the overall dialogue over time:

(a) In November 2012, Swedbank Estonia responded to a question from the EFSA about increased payment movements for offshore customers by attributing the increase to a restructuring of the ownership of the HRC-1 Group. Swedbank Estonia assured the EFSA that it was aware of and was monitoring the restructuring and the transactions, and that it had obtained relevant documentation. The Investigation indicates that Swedbank Estonia was indeed aware of and monitoring the restructuring, and that it had obtained documents from the customer regarding the restructuring. The Investigation further found, however, that, as explained in Section VII.A., Swedbank Estonia generally did not in 2012 have (1) adequate documentation verifying the beneficial owners of the HRC-1 Group, or (2) an adequate understanding of the legitimate business purpose of the restructuring, nor had Swedbank Estonia (3) adequately implemented conduct risk-based monitoring of the HRC-1's Group's transactions.

(b) In April 2016, Swedbank Latvia responded to an FCMC request about Swedbank Latvia's internal audit plans for the past several years. The initial FCMC request sought "*Inspection plans from the Internal Audit Unit for 2014, 2015 and 2016, and the execution [results] of the plan for 2014 and 2015.*" In response to this request, Swedbank Latvia provided a general summary of the relevant GIA findings with two GIA reports from January 2015 and February 2016. The Investigation did not find evidence that Swedbank Estonia provided the FCMC at that time with a GIA report issued on 30 June 2015, which identified deficiencies in Swedbank Latvia's internal control systems for AML/KYC. The FCMC then conducted an on-site inspection in April 2016, and issued a report on 19 August 2016 that identified deficiencies in Swedbank Latvia's internal AML/CTF control system, noting its "*internal control system allows for the possibility of a client on whose economic activity the Bank has not acquired sufficient amount of information, to open an account and to do business on a large scale and within few months to close the account.*"

    Swedbank Latvia responded to the FCMC report in September 2016, and stated among other things that, "*[e]ven though Swedbank agrees with the importance of efficient internal control systems, and continuous improvements thereof, Swedbank urges the Commission to evaluate the fact that the irregularities have not increased the actual risk for money laundering or terrorist financing as extenuating circumstances.*" This statement appears not to have taken into account that certain deficiencies identified in the 30 June 2015 GIA report remained unresolved in October 2016, when a GIA report identified two "*overdue*" findings from the 2015 audit report relating to the quality of the existing transaction monitoring process, and the need to update internal regulations to improve non-resident account monitoring.

(c) In April 2016, Swedbank received two related requests from the SFSA in connection with the Panama Papers leak. On 12 April 2016, the SFSA issued a request referencing the "*so-called Panama documents and the information which has emerged from these concerning off-shore structures*," and asked Swedbank a number of questions including whether there were "*business areas of the bank, its*

branches or subsidiaries" that offered services or products to offshore structures. Swedbank responded to this request including information regarding the Baltic Subsidiaries.

On 22 April 2016, the SFSA made a follow-up request to Swedbank—using the same reference number as the 12 April request—seeking, among other things, (1) a list of all of *"Swedbank's Private Banking and LC&I customers"* that completed transactions to or from certain listed countries between 14 June 2014 and 19 April 2016, and (2) a list of "*legal persons*" which were, among other things, either (a) "*customers of Swedbank AB (Publ), Luxembourg Branch or Swedbank Management Company S.A.,*" domiciled in certain listed countries and had at least one beneficial owner "*with a business relationship with Swedbank*," or (b) had either "*assets exceeding 25 million SEK or equivalent with Swedbank"* or "*credit engagements (excluding credit cards) with Swedbank"* as well as "*at least one beneficial owner with fiscal domicile*" in one of certain listed countries.

On its face, the SFSA's 22 April request did not refer to Swedbank's "*branches or subsidiaries,*" as had the 12 April request, but rather used the term "*Swedbank*," except when referring to specific entities or businesses, such as "*Swedbank AB(Publ), Luxembourg Branch.*"

The contemporaneous internal communications indicate that, on or around 25 April 2016, LC&I in consultation with Group Compliance decided that with respect to the scope of the 22 April request, "*[t]he interpretation is that Swedbank = Swedbank AB, i.e. the questions also cover the branches but not the subsidiaries, except in question 4, where this is specified for Manco in Luxembourg.*" The Investigation did not identify evidence that this interpretation was discussed with the SFSA.

In addition, there was some discussion whether customers of the Baltic Subsidiaries to which Swedbank's LC&I business provided services should be included. As one LC&I employee explained to an employee in the Baltics, those customers "*formally belong to the legal entities in the Baltics even though they organizationally belong to LC&I in Swedbank. As the Swedish FSA asks only about clients belonging legally to Swedbank AB (Sweden) and its branches, the scope will not include these clients. In short, you are off the hook*."

Based on this interpretation of the question, Swedbank does not appear to have considered any customers from its Baltic Subsidiaries for its response, and did not in its response specify which entities were the sources of the responsive data.

In an internal email exchange in August 2016, two LC&I employees stated that Swedbank "*didn't report any Baltic customers to the SFSA in connection to Panama since the choice was made to interpret the questions as concerning Swedbank AB, on the other hand the question is whether the LC&I customers in the Baltics were controlled in the correct manner*."

(d) In January 2017, Swedbank responded to an SFSA verification letter dated 23 December 2016. The verification letter identified deficiencies in Swedbank's KYC for a number of customers, including HRC-1. Specifically, the SFSA stated that it "*appears as though the Bank has not assessed the risk associated with the fact that the customer's ownership structure changed strictly for the purpose of avoiding taxes*" and that "*Swedbank has not taken additional measures to reduce the bank's risk exposure to being exploited for money laundering.*" Swedbank submitted a response to the SFSA on 27 January 2017 that assured the SFSA that Swedbank had "*adequate procedures and processes in its operations . . . a good understanding of the customer, as well as the purpose and type of the business relationship.*"

During the drafting of this response, a Swedbank senior manager recognized that the response may be an overstatement, opining: "*I think this is a pretty*

strong statement in consideration of what is hiding behind [HRC-1] . . . What is our thinking here?" Although this comment was shared with a second Swedbank senior manager, the Investigation has not identified any evidence that it was shared with the CCO, who supervised the drafting of the response. The Investigation did, however, identify a communication between the CCO and the second senior manager in which the senior manager advised that the language of the response created "*a risk that we, in a possible continuation of the review, are unable to live up to what we write in the replies.*"

Swedbank also responded to the SFSA's criticism of the handling of HRC-1, stating "*that the change in the ownership structure was an adjustment to the proposed regulations in Russia and thus driven by changing tax regulations. The customer information that was received in this respect was clear and documented . . . [and] included a legal opinion from a Russian law firm.*" The Investigation has not identified any evidence that Swedbank provided the legal opinion to the SFSA and identified the following statement, "*the legal opinion referred to does not support our assessment . . . It may be difficult to explain [in case the SFSA] requests [it].*" In addition, the relevant legal opinion identified by Clifford Chance was very brief and did not address whether the ownership restructuring was permissible tax avoidance as opposed to tax evasion or otherwise support the propriety of the structuring.

(e) In April 2017, Swedbank Estonia responded to a series of EFSA questions about its AML compliance procedures in relation to non-resident and other high risk customers, which included a follow-up request for "*additional measures in order to assess your potential involvement with the Panama Papers case.*" Swedbank Estonia had previously informed the EFSA in April 2016 that it had identified 29 customers "*where Swedbank has identified a connection to the law office Mossack Fonseca.*" In May 2016, however, senior managers in Swedbank Estonia received an update that further research had identified 37 customers that used Mossack Fonseca as a registered agent (and there were another 56 natural persons referenced in the Panama Papers leak that were either customers or associated with customers). Swedbank Estonia's 12 April 2017 response repeated the 29 customers previously identified in April 2016, without providing the updated numbers from May 2016. Some senior managers at Swedbank Estonia, including its CEO, had received the updated numbers in May 2016, and later participated in the drafting of the 12 April 2017 response. The Investigation did not determine that the failure to provide the updated numbers was intentional.

F. Findings Regarding Employee Accountability

The Investigation also has examined relevant conduct of employees and senior management, including the Swedbank Board. In this regard, the Investigation considered who was responsible over time for the existence of the deficiencies in AML and sanctions controls in the Baltic Subsidiaries, primarily but not exclusively at Swedbank Estonia, and why the significant AML and sanctions control deficiencies that were identified by GIA, Compliance and other functions, as well as Swedbank's external auditors, nonetheless continued for many years.

The following sections focus first on an assessment of the various CEOs over the Investigation Period, followed by the Swedbank Board, and then generally on the actions the Bank has taken and is taking with respect to employees and employee accountability.

1. Assessment of the Swedbank CEOs

a. 2007 to 2009

At the outset of the Investigation Period, Swedbank was led by a CEO who assumed the role in 2004 and retired in 2009. In the period pre-dating the Investigation, the CEO and Swedbank were focused on the task of integrating the newly acquired Baltic Subsidiaries with the Group. By the Q2 2007 earnings call, the CEO reported that "*Baltic Banking on the other hand has had another very good result and managed to increase by 19% this quarter's result compared to the first quarter*." For Q1 and Q2 of 2007, the HRNR portfolio comprised over 15% of the incoming and outgoing external transactions of Swedbank Estonia.

By mid-2007, Swedbank was facing a challenge with Swedbank's then-operations in Russia (through its subsidiary OAO Swedbank, formerly OAO Hansabank). The regulatory action in Russia in June 2007 prompted the CEO of HBG to issue the 2007 Decree. As earlier discussed in detail (*see* Section VII, *supra*), the Decree mandated that no HBG entities could handle new or existing relationships with "*offshore*" customers that did not meet predefined criteria unless specifically authorized by the HBG Board,[79] and directed all HBG entities to review their existing portfolios. This resulted in significant off-boarding activity for Swedbank Estonia and Swedbank Latvia, although Swedbank Estonia exempted the HRC-1 Group from the Decree. Because the HRC-1 Group was exempted from the Decree, it remained a significant customer of Swedbank Estonia and anchored the subsequent expansion of Swedbank Estonia's HRNR customer portfolio.

In early 2009, the message communicated by the CEO to the Board, as reflected in the minutes from the 22 January 2009 Board meeting, was that the CEO "*concluded that [they] believ[e] that the bank has adequate routines on [AML].*" While the CEO's basis for this view is unclear, the Investigation has identified facts indicating that, at minimum, the Baltic Subsidiaries did not have adequate AML compliance controls at this time. However, because of the passage of time and the unavailability of witnesses from that time period, the Investigation was not able to determine the reasons for the discrepancy between the noted AML deficiencies at the Baltic Subsidiaries and the CEO's assurance to the Board that Swedbank's AML controls were adequate, nor was it able to assess the degree to which the CEO should have done more to ensure the sufficiency of AML controls.

b. 2009 to 2016

In 2008-2009, the attention of the CEO, Chairman and Board was mostly focused on the financial crisis and the retirement of the former CEO in April 2009. A new CEO was appointed, who served from 2009 until February 2016. This CEO began their tenure focused on credit risk, macroeconomic issues, and other items related to the financial crisis. In 2013 and 2014, the SFSA noted AML deficiencies in Swedish Banking and LC&I. The SFSA had commenced an investigation in early 2013 to examine procedures within LC&I, Swedish Banking, and Swedbank's Norway Branch. Among other findings, the SFSA found that LC&I and Swedish Banking had low risk awareness and did not sufficiently conduct risk assessments of customers. The SFSA also found numerous deficiencies in LC&I and Swedish Banking's KYC function, including a large amount of customers without proper KYC, missing KYC documentation and analysis and too many manual routines in the KYC process. Lastly, the SFSA found that LC&I and Swedish Banking had insufficient IT support and failed to screen beneficial owners against sanctions lists on a daily basis. In June 2014, the SFSA closed its investigation without sanction, provided that Swedbank perform various remedial activities set forth in its approved action plan. LC&I implemented several changes aimed at addressing the SFSA's findings, including improving the KYC function. Swedbank set up a "*Swedish-wide AML Programme*" that was responsible for "*the closing of all gaps*

[79] *See supra* at 56-57.

related to SFSA findings." Similar to the parallel LC&I AML project, the Swedish-wide AML Program made several improvements to the AML and KYC function within Swedish Banking.

When interviewed in connection with the Investigation, the then-CEO did not recall focusing on AML issues in the Baltics at the time because no particular serious deficiencies were brought to the CEO's attention. While GIA noted a number of AML deficiencies in the Baltic Subsidiaries during the CEO's tenure, the CEO did not recall receiving reports of such deficiencies, and did not recall receiving any other warning signals from within or outside Swedbank related to AML issues at the Baltic Subsidiaries. In 2015, Group Compliance began an assessment of AML controls in the Baltic Subsidiaries, the results of which were reported in March 2016 after the CEO had departed.

This CEO's lack of attention to AML issues in the Baltic Subsidiaries is noteworthy, as the recurrence of GIA findings of AML deficiencies—including repeated findings of inadequate training and KYC documentation—should have triggered more scrutiny by the CEO of AML risk in the Baltics. The CEO served during a period when the Bank's HRNR portfolio at the Baltic Subsidiaries was at its historical apex and the risk to Swedbank most acute. But the CEO was apparently unaware of the escalating risk, notwithstanding the fact that the SFSA focus on AML deficiencies in LC&I and Swedish Banking should have alerted the CEO to the possibility of AML risk in the Baltics and to the prospect of similar control deficiencies in that region. However, as the CEO and other former executives from that time period related, AML risk in the Baltics was simply not an area that Swedbank prioritized during those years.

c. 2016 to 2019

A new CEO was appointed in April 2016, who served until March 2019. The CEO had previously served as Head of GIA from 2009 through 2011, Head of Baltic Banking from 2011 through 2014, and Head of Swedish Banking from 2014 through 2016. The CEO started around the same time that the series of events described above (*see* Section VII.A*., supra* at 90-94) focused the Bank's attention on de-risking the Baltic Banking HRNR business for AML risk-management and reputational purposes. As has been described, under the CEO's tenure, Swedbank initiated numerous reviews and investigations into the Group's exposure to various AML scandals, primarily in the Baltics, that were identified through press reports, and, in conjunction with the Baltic Subsidiaries (especially Swedbank Estonia), initiated a broad de-risking exercise that over the course of approximately one year greatly reduced the Baltic Subsidiaries' HRNR customer base.

Nevertheless, during the CEO's tenure, the significant AML and sanctions control deficiencies that GIA, Group Compliance, external consultants retained by Swedbank and other Group functions had identified were not addressed with the resources and attention commensurate to the substantial legal and reputational risks such deficiencies posed to the institution. In addition, the Investigation determined that the CEO did not ensure that the Board was adequately educated or apprised of the significance of the legal and reputational risk to the institution arising from the AML and sanctions control deficiencies, particularly given the high-risk customer segment in the Baltics with which the CEO had some familiarity due to the CEO's prior roles and involvement in reviews of that portfolio as CEO. In addition, the Investigation did not identify evidence indicating that the CEO sufficiently emphasized AML compliance in setting the tone from the top, nor did the CEO ensure adequate coordination regarding AML compliance between control functions, between control functions and the business, or between Swedbank and its Baltic subsidiaries. These governance failings in practice impeded the efficacy of the AML-related remediation that had begun in 2016. Finally, the Investigation identified concerns with public disclosures made by Swedbank and the CEO, beginning in Q3 2018, regarding Swedbank's exposure to the type of AML issues being publicly reported by and about CPB-1.

2. Assessment of the Group Board and Board Chairman

The Board has overall responsibility "*for operations being conducted in accordance with current regulations and generally accepted practice. The Board sets basic compliance guidelines through a Compliance Policy*." The Board "*sets the financial goals and strategies; appoints, dismisses and evaluates the CEO; verifies that effective systems are in place to monitor and control operations and that laws and regulations are followed; and ensures transparency and accurate information disclosures*." The Board consists of nine members elected at the Annual General Meeting for one year. It also includes two employee representatives and their deputies in accordance with special agreements with the Financial Sector Union of Sweden and Akademikerföreningen.

Since at least 2013, the CCO has been required to provide: quarterly written reports and an overall assessment of Swedbank's Compliance risk across the Group to the Board and the Audit Committee of the Board; a written report outlining significant communication with regulators to be discussed at each Board meeting; and a yearly compliance plan encompassing key compliance risks and compliance activities for adoption by the Board. Starting in 2018, some of the Audit Committee's responsibilities were shifted to the RCC so that the Audit Committee could focus on handling financial reporting. With the shift, the Audit Committee received a yearly compliance report and the RCC received from Compliance and Group Operational Risk copies of: the yearly compliance plan; quarterly compliance reports; yearly operational risk plan; and quarterly operational risk reports.

The Audit Committee is tasked with identifying deficiencies "*in terms of governance, risk management and control*" by working with Swedbank's External Auditor, Head of GIA (who sits on the Committee) and the Group Executive Committee. The Audit Committee also receives and reviews the External Auditor's report as well as Internal Audit's quarterly reports. As noted above, while the External Auditor's reports did not focus in the main on AML deficiencies, they did on occasion comment on recommended improvements. For example, in Q2 2012, the External Auditor's report noted that "*Group AML needs to strengthen its AML structure.*" In Q2 2016, the External Auditor's Report found that "*there has not been a documented risk analysis performed since 2014 to evaluate if the controls are considered to be the most essential to mitigate current AML risks.*" In Q3 2018, the External Auditor's Report stated: "*[A]s reported in previous quarters, AML is an area we want to bring to attention. AML is continuously an emerging risk, and in Q3 findings have been identified by Internal Audit and Compliance.*" These reports, which did not highlight significant AML risk, were provided to the Board, the Audit Committee, and senior management, including the CEO.

GIA reports directly to the Board, and the Board is responsible for appointing and dismissing the Head of GIA. GIA had an obligation to report unsatisfactory findings to the committee chair and the CEO promptly. GIA would assign an unsatisfactory finding if a risk was too high compared to Swedbank's risk appetite; however, as a practical matter Swedbank's risk appetite was unclear for most of the Investigation Period. With respect to AML/CTF, GIA examined a variety of issues, including client on-boarding and off-boarding processes, training, PEP screening, transaction monitoring and sanctions screening. In general, unsatisfactory findings were required to be closed out within three months, while other findings could be closed out within six months or longer.

As noted in Section VII.A., generally throughout the Investigation Period GIA identified numerous deficiencies with respect to AML processes in the Baltic Subsidiaries. For example, a July 2008 GIA audit, reported to the Audit Committee in December 2008, rated Group-wide implementation of KYC processes overall as "*functioning*" but found a lack of definite criteria for AML training and shortcomings in addressing previous AML audits. A June 2012 GIA audit, sent to the Audit Committee in January 2013, found that Swedbank Lithuania failed to control the accuracy and completeness of

customer information entered into its customer database and Swedbank Estonia did not ensure that employees passed required AML trainings, rating both of these findings as "*Requires Improvement*." Another GIA audit in June 2013 found that the Baltic Subsidiaries failed to consistently identify PEPs among existing customers and, as in 2012, found insufficient AML training, again rating both of these findings as "*Requires Improvement.*" A June 2015 GIA audit, reported to the Audit Committee in July 2015, found that AML controls and transaction monitoring in the Baltic Subsidiaries required "*Major Improvement.*" While GIA had closed its 2013 finding with respect to deficiencies in identifying PEPs in late 2014, its June 2015 audit again found that the identification of PEPs among existing customers in the Baltic Subsidiaries "*Require[d] Improvements.*"

Minutes from Audit Committee meetings indicate that Audit Committee members regularly challenged the Bank on how AML issues were being handled and mitigated, and repeatedly emphasized the importance of an effective AML compliance program. For example, in 2016, the Audit Committee inquired about the progress of the Baltic Banking AML Program, and "s*tressed the importance of*" prioritizing AML issues and "*being in compliance with AML regulations.*" During another Audit Committee meeting in 2016, upon being informed about GIA's unsatisfactory findings related to AML in the Baltic Subsidiaries, the Audit Committee expressed "*regret[] to hear that Baltic Banking is not at the forefront as regards AML-issues.*" Further, in 2018 when informed about deficiencies related to transaction monitoring and AML/CTF documentation, the Audit Committee "*stressed the importance of strong AML/CTF management.*" Members of the Audit Committee recalled, however, an impression before 2019 that the AML risk in the Baltics was well managed, and that there was no sense of urgency about the identified breaches of the Group's policies or procedures. This was a recollection shared by members of the RCC.

Similarly, current and past Board members generally recalled believing that AML was not identified as a significant legal or reputational risk for Swedbank prior to 2019. According to interviews of Board members, based in significant measure on what they believed to be reassuring messages received from the CEO, the Board in more recent years generally had the impression that Group Compliance and GIA managed AML risk competently and professionally. Meeting minutes from the Investigation Period reflect a general sense of comfort with the progress made with respect to AML compliance in the Baltic Subsidiaries throughout the Investigation Period.

The Investigation indicates that, through GIA and CCO reports, and particularly through reporting to the Audit Committee, the Swedbank Board was apprised of the existence of persistent AML and sanctions control deficiencies in the Baltic Subsidiaries. Some of these deficiencies—particularly inadequate training and insufficient KYC documentation—were recurring over the years, even after having been previously reported as closed. The Investigation did not find evidence that either the Board, RCC or Audit Committee were adequately informed of the degree of legal and reputational risk posed by these deficiencies arising from the high-risk customer base that the Baltic Subsidiaries had serviced historically. Nevertheless, the Board was put on notice from 2015 through early 2017 by several GIA reports to the Board and Audit Committee of the prospect of regulatory sanctions or elevated reputational risk arising from identified deficiencies at the Baltic Subsidiaries with respect to weak sanctions screening data, insufficient KYC processes and transaction monitoring and defects in the payments screening process. Notwithstanding these warnings, the Board did not take action to manage AML risk in the Baltics commensurate with the degree of legal and reputational risk presented. The Investigation found little evidence of any substantive discussion of these issues at the respective Board or Audit Committee meetings. Thus, while the Board was not adequately apprised by management of the full extent of the risk posed by the AML deficiencies in the Baltics, the Board also did not act adequately to manage and control the AML risk of which it was made aware.

3. Assessment of Employee Conduct and Accountability

The Investigation identified a number of employees, including senior management level employees, whose acts and omissions caused, contributed to, or permitted to continue AML and sanctions control deficiencies and attendant risk to Swedbank and its Baltic Subsidiaries. These acts and omissions included serving as RMs to customers that presented unacceptable risk to Swedbank; serving as supervisors of those RMs and permitting such practices to continue; repeated approvals of customers and accounts by the HRCAC in Estonia despite missing or inadequate UBO information; and, as to senior managers in Swedbank and the Baltic Subsidiaries, failing to exercise appropriate oversight relating to AML controls. Over the course of the Investigation, Clifford Chance has shared this information with Swedbank for it to determine appropriate employment action, consistent with applicable law and policy. This has led to Swedbank ending the employment of a number of employees, including at senior management level, 11 of which have been publicly announced. An additional eight employees have separated from Swedbank during the course of the Investigation. Other employees have received warnings and financial sanctions, and all employees, as part of the ongoing enhancements to compliance, will undertake compliance-related training that includes, among other topics, AML and sanctions.

In addition to Swedbank's employment-related remedial steps during the course of the Investigation, a significant number of the employees primarily responsible for the historical deficiencies described here had left Swedbank or its Baltic Subsidiaries prior to the Investigation, as reflected in prior internal Swedbank reports:

- In 2007, two employees with responsibility for the IPB business that housed the HRNR Customer portfolio in Swedbank Estonia were terminated by Swedbank for conduct with respect to customers that either presented a conflict of interest or fell below Swedbank's employee conduct standards as set out in the Swedbank Code of Conduct. Further, in 2008-2009, when Swedbank Estonia disbanded the IPB, ten relevant employees either left or were asked to leave Swedbank.
- In 2017, in connection with the de-risking of the HRNR Customer business at the Baltic Subsidiaries and related Swedbank internal investigations, an additional six employees departed Swedbank, including in instances where Swedbank determined that the employees' conduct in servicing such customers fell below the standards expected of Swedbank employees.

Today, Swedbank is run by a new senior management team that was either external to Swedbank at the time or whom the Investigation has not identified as being involved in the historical issues. Beginning in 2019, Swedbank has installed, for example, a new CEO, CCO, Head of Baltic Banking, and CEO of Swedbank Estonia. In addition, Swedbank formed a new Anti-Financial Crime Unit ("**AFC**"), focused in part on AML and CTF prevention, with overall group responsibility for first-line AML processes in Swedbank. Moreover, Swedbank has a new Chairman, and the Board now is comprised of mostly new members as well.

G. Findings Regarding Swedbank's US Sanctions Compliance

In view of the five-year Sanctions Review Period and the 26.6 million In-Scope Messages, including over 1.8 million USD payments, included in the Filtering Exercise, the Transaction Review identified only a small number of apparent Subject Transactions, with the exception of 507 payments, totaling approximately $4.26 million payments, remitted between 30 December 2014 and 30 December 2016 by three shipping customers that had accounts at Swedbank Latvia whose owner appeared to operate these companies from Crimea even though the companies themselves were domiciled in offshore jurisdictions.

None of the Subject Transactions involved an SDN, and nearly all of them, by volume and value, occurred prior to 2017, the year that the Baltic Subsidiaries implemented ProScan.

1. Swedbank Estonia

a. Overview

FTI collected and analysed approximately 12 million SWIFT transaction messages processed by Swedbank Estonia. From that population, FTI identified approximately 338,000 In-Scope Messages that produced hits against the OFAC-related Search Terms. FTI then determined that approximately 7,100 of these messages contained true hits against the OFAC-related Search Terms. From the SWIFT messages that generated these hits, after searching for potential related messages, FTI assembled 3,037 Transaction Groups for the Legal Review, supplemented by an additional 185 Transaction Groups involving payments initiated by customers of Swedbank Estonia from IP addresses in an Embargoed Country.

In total, the Transaction Review determined, based on the available information, that Swedbank Estonia customers used an online banking platform to initiate 19 outgoing Subject Transactions, totaling approximately $100,000, as follows:

- 17 were remitted by a former individual customer of Swedbank Estonia who had a residency address in Estonia but, based on the KYC Data, also appeared to work from Iran during portions of the Sanctions Review Period, including when the customer sent these payments from an IP address in Iran.
- One was sent by a former individual customer of Swedbank Estonia from an IP address in Cuba. This customer had a residency addresses in Finland, but accessed the online banking platform via an IP address in Cuba numerous times over the Sanctions Review Period. The payment had no apparent connection to Cuba other than the customer's temporary presence there when sending the payment.
- The final payment was sent by a non-sanctioned corporate customer of Swedbank Estonia to a vessel crew member apparently located in Crimea. The resubmission analysis below discusses this Subject Transaction in detail.

Outgoing Subject Transactions (Volume)

Sanctions Program	2014	2015	2016	2017	2018	2019	Total
Crimea		1					1
Cuba				1			1
Iran		6	5	6			17
Total	**0**	**7**	**5**	**7**	**0**	**0**	**19**

Outgoing Subject Transactions (Value)

Sanctions Program	2014	2015	2016	2017	2018	2019	Total
Crimea		$1,261					**$1,261**
Cuba				$10,000			**$10,000**
Iran		$23,210	$44,593	$19,906			**$87,709**
Total	**0**	**$24,471**	**$44,593**	**$29,906**	**0**	**0**	**$98,970**

The Transaction Review also identified 35 apparent Subject Transactions, totaling approximately $222,000, incoming to customers of Swedbank Estonia. Thirty-four of them went to Swedbank Estonia's above-referenced Iran-exposed former individual customer, and appeared to involve compensation from a Finnish company's regional office in a third country for work that this individual undertook on the company's project in Iran and/or overlapped with periods when the online banking data appears to indicate that this individual was in Iran. The other incoming payment, for $10,300 and to a non-sanctioned corporate customer, contained a reference to a city in Iran in the free text field of the SWIFT payment message that Swedbank Estonia received from its US correspondent bank.

Incoming Subject Transactions (Volume)

Sanctions Program	2014	2015	2016	2017	2018	2019	Total
Crimea							**0**
Cuba							**0**
Iran		11	17	7			**35**
Total	**0**	**11**	**17**	**7**	**0**	**0**	**35**

Incoming Subject Transactions (Value)

Sanctions Program	2014	2015	2016	2017	2018	2019	Total
Crimea							**0**
Cuba							**0**
Iran		$66,298	$110,346	$44,861			**$221,506**
Total	**0**	**$66,298**	**$110,346**	**$44,861**	**0**	**0**	**$221,506**

b. Resubmission Analysis

The Transaction Review identified ten Relevant Transactions sent by Swedbank Estonia that were rejected or blocked by a counterparty bank for apparent OFAC-related reasons. The resubmission analysis determined that a non-sanctioned corporate customer of Swedbank Latvia resubmitted one such payment, for $1,260.83, through an online banking platform from an IP address in Estonia, that the Transaction Review classified as a Subject Transaction because (as noted above) it involved the wages of a crew member who appeared to be located in Crimea. Swedbank Latvia's customer removed a reference to "*Sevastopol*" in the original payment message before resubmitting the wage payment through an online banking platform. The Transaction Review did not identify any other such resubmissions through Swedbank Estonia.

2. Swedbank Latvia

a. Overview

FTI collected and analyzed approximately 7.8 million SWIFT transaction messages processed by Swedbank Latvia. From that population, FTI identified approximately 35,000 In-Scope Messages that produced hits against the OFAC-related Search Terms. FTI then determined that approximately 8,300 of these messages contained true hits against the OFAC-related Search Terms. From the SWIFT messages that generated those hits, after searching for potential related messages, FTI assembled 2,877 Transaction Groups for the Legal Review, supplemented by an additional 452 Transaction Groups

involving payments initiated by customers of Swedbank Latvia from IP addresses in an Embargoed Country and other payments by the same customers.

In total, the Transaction Review determined, based on the available information, that Swedbank Latvia customers used an online banking platform to initiate 522 outgoing Subject Transactions, totaling approximately $4.43 million, as follows:

- 507 of these payments, totaling approximately $4.26 million, involved three former shipping company clients of Swedbank Latvia domiciled in offshore jurisdictions whose owner (an individual) sent 410 of these payments from an IP address in Crimea on behalf of these companies after the imposition of US sanctions against Crimea on 19 December 2014. Based on the KYC Data for these three clients, we concluded that (a) the owner appeared to run these companies from Crimea and (b) other affiliated companies that were located in Crimea (not the ones that remitted the payments) participated in the operation of a vessel owned by one of the companies that remitted the payments. Each of the 507 payments, which dated between 30 December 2014 and 30 December 2016, appeared to have some connection to the operation of this vessel (*e.g.*, crew wages, bunkers). Swedbank Latvia terminated the accounts of these clients at the end of 2016.
  - Five of the 507 payments were resubmitted by the owner of these clients over an online banking platform, after a US intermediary bank rejected an earlier version of the same payment, apparently because the US intermediary bank had determined or suspected that the payment related to Crimea. The resubmitted payments went through different US correspondent banking channels than the rejected payments.
  - Another four of the 507 payments, plus two of the five that were resubmitted, attracted inquiries from a US correspondent bank regarding whether the payments involved Crimea. The reply sent by Swedbank Latvia did not indicate any connection to Crimea.[80]
- Apart from the 507 above-referenced payments, another five of the 522 outgoing Subject Transactions, totaling approximately $137,000, were sent by four individual customers of Swedbank Latvia from IP addresses in Crimea or Iran. These customers had residency addresses in Latvia, Russia and Uzbekistan, respectively. Based on their online banking activity during the Sanctions Review Period, one of these customers spent only one week in Crimea while the other three visited Crimea or Iran more frequently. But for the temporary presence of these customers in Crimea or Iran, the five payments otherwise appeared to have no connection to Crimea/Iran.
- The remaining ten of the 522 payments, totaling approximately $41,000, involved payments by non-sanctioned customers to counterparties or a beneficiary bank that were apparently located in Crimea, typically involving wage payments.
  - Three of these payments, sent during the first half of January 2015, included a reference to either "*Simferopol*" or to the BIC of a bank in Crimea in the payment message sent to US intermediary banks, but were still processed by them. The Transaction Review could not determine why the US correspondent banks that processed these payments failed to detect the Crimean references in the SWIFT messages,[81] although it could be because these payments occurred less than a month after the imposition of territory-wide sanctions against Crimea.

[80] Although the three shipping customers were not domiciled in Crimea, and particular vessel-related payments by them may not have involved voyages to or from Crimea, we classified these payments as Subject Transactions based on the apparent involvement of the owner and affiliated companies located in Crimea in the operation of the vessels owned by the three customers. Our open source research did not provide any further insight into the operations of the owner, the three customers or their affiliated companies in Crimea

[81] We note, however, that: (a) the Swedbank Latvia customer that remitted these payments was not located in Crimea or otherwise the subject of any OFAC sanctions; (b) the beneficiaries, crew members apparently located in Crimea, were not Swedbank customers; and (c) if a major US financial institution, presented with the same information about the beneficiary's location that Swedbank Latvia possessed, failed to identify the OFAC issue, Swedbank Latvia's own failure to identify the OFAC issue potentially may not be deemed a violation by Swedbank Latvia, because Swedbank Latvia did not cause its US correspondent bank to violate the OFAC sanctions in this context.

– As discussed further below, the other seven payments were resubmitted by non-sanctioned customers of Swedbank Latvia over the online banking platform without reference to Crimea after the rejection by a US intermediary bank of an earlier payment that had referenced Crimea.

Outgoing Subject Transactions (Volume)

Sanctions Program	2014	2015	2016	2017	2018	2019	Total
Crimea	2	263	252	3			**520**
Cuba							**0**
Iran		1	1				**2**
Total	**2**	**264**	**253**	**3**	**0**	**0**	**522**

Outgoing Subject Transactions (Value)

Sanctions Program	2014	2015	2016	2017	2018	2019	Total
Crimea	$16,598	$2,172,308	$2,108,130	$136,360			**$4,433,395**
Cuba							**0**
Iran		$272	$350				**$622**
Total	**$16,598**	**$2,172,579**	**$2,108,480**	**$136,360**	**0**	**0**	**$4,434,017**

The Transaction Review also identified one incoming Subject Transaction for $5,970 to an individual customer of Swedbank Latvia who had a residency address in Crimea.

Incoming Subject Transactions (Volume)

Sanctions Program	2014	2015	2016	2017	2018	2019	Total
Crimea					1		**1**
Cuba							**0**
Iran							**0**
Total	**0**	**0**	**0**	**0**	**1**	**0**	**1**

Incoming Subject Transactions (Value)

Sanctions Program	2014	2015	2016	2017	2018	2019	Total
Crimea					$5,970		**$5,970**
Cuba							**0**
Iran							**0**
Total	**0**	**0**	**0**	**0**	**$5,970**	**0**	**$5,970**

b. Resubmission Analysis

The Transaction Review identified 38 Relevant Transactions sent by Swedbank Latvia that were rejected or blocked by either Swedbank Latvia or a counterparty bank for apparent OFAC-related reasons. As noted above, the Crimea-based owner of the three shipping company clients domiciled in offshore jurisdictions resubmitted five of these payments, totalling $69,215, over an online banking platform.

In addition, the resubmission analysis determined that three different non-sanctioned corporate customers of Swedbank Latvia resubmitted another seven of the rejected payments (for crew wages or expenses), totaling approximately $30,000, through an online banking platform that the Transaction Review classified as Subject Transactions, because the beneficiary and/or beneficiary bank were apparently located in Crimea. In six of these cases, the customers removed references to "*Sevastopol*," "*Kerch*," "*Evpatoria*" and/or "*Simferopol*," in the original payment messages before resubmitting them through the online banking platform. In the remaining case, the original payment generated a request for information from the beneficiary bank's US correspondent bank seeking information about the location of the beneficiary of the payment. In response, Swedbank Latvia, presumably based on information provided by its customer, provided an address in Sevastopol, which caused the beneficiary bank's US correspondent bank to reject the payment. After attempting to re-send the same payment with the same routing (*i.e.*, the same beneficiary bank and US correspondent banks) and having that payment again rejected, the customer changed the routing to a different beneficiary bank, such that other US correspondent banks processed the payment.

3. Swedbank Lithuania

a. Overview

FTI collected and analysed approximately 6.8 million SWIFT transaction messages processed by Swedbank Lithuania. From that population, FTI identified approximately 145,000 In-Scope Messages that produced hits against the OFAC-related Search Terms. FTI then determined that approximately 2,100 of these messages contained true hits against the OFAC-related Search Terms. From the SWIFT messages that generated those hits, after searching for potential related messages, FTI assembled 808 Transaction Groups for the Legal Review, supplemented by an additional 50 Transaction Groups involving payments initiated by customers of Swedbank Lithuania from IP addresses in an Embargoed Country.

In total, the Transaction Review determined, based on the available information, that two customers of Swedbank Lithuania used an online banking platform to initiate five outgoing Subject Transactions, totaling approximately $2,400, as follows:

- One of these payments, for $400, was sent by an individual customer with a residency address in Lithuania over an online banking platform from an IP address in Crimea while the customer appeared to be visiting there.
- The four remaining payments were sent by a non-sanctioned corporate customer to pay vessel crew members who apparently were in Crimea. As discussed further below, each of these payments was resubmitted by the customer over an online banking platform without reference to Crimea after the rejection by Swedbank Lithuania (two payments) or a US intermediary bank (two payments) of an earlier payment that had referenced Crimea.

The Transaction Review did not identify any incoming Subject Transactions received by customers of Swedbank Lithuania.

Outgoing Subject Transactions (Volume)

Sanctions Program	2014	2015	2016	2017	2018	2019	Total
Crimea			1		4		**5**
Cuba							**0**
Iran							**0**
Total	**0**	**0**	**1**	**0**	**4**	**0**	**5**

Outgoing Subject Transactions (Value)

Sanctions Program	2014	2015	2016	2017	2018	2019	Total
Crimea			$400		$2,009		**$2,409**
Cuba							**0**
Iran							**0**
Total	0	0	$400	0	$2,009	0	**$2,409**

b. Resubmission Analysis

The Transaction Review identified nine Relevant Transactions sent by Swedbank Lithuania that were rejected or blocked by either Swedbank Lithuania or a counterparty bank for apparent OFAC-related reasons. The resubmission analysis determined that a non-sanctioned customer of Swedbank Lithuania resubmitted four such payments, for crew wages, through an online payment platform, valued at approximately $2,000, that the Transaction Review classified as Subject Transactions because the beneficiary crew member was apparently located in Crimea. The customer removed references to "*Sevastopol*," "*Kerch,*" *"Krym*," "*Crimea*" and "*Evwpatorya*," respectively, that it had included in the four original payment messages before resubmitting them through the online banking platform.

VIII. REMEDIATION

Swedbank has focused over the past year on transforming its approach to AML/CTF and sanctions compliance, creating new roles, appointing new personnel, increasing resources, revising and strengthening policies and procedures, and taking steps to de-risk its customer portfolio including in the Baltic Subsidiaries. These efforts are in some ways a continuation of de-risking and remediation efforts in which Swedbank has engaged since 2016, when Swedbank, like other European banks with HRNR customer portfolios in the Baltics, increasingly recognized the risks that such a portfolio presented and tried to mitigate those risks.

A. Swedbank's Remediation Efforts before 2019

Swedbank's de-risking and remediation efforts since 2016 include, for example:

- In 2016, Group Compliance and Baltic Banking established an AML program for the Baltic Subsidiaries with updated procedures for payments screening, transaction monitoring, KYC and risk classification. The Baltic Subsidiaries also took steps to de-risk their HRNR portfolio, off-boarding substantial numbers of HRNR customers, and, in Swedbank Estonia, deciding to terminate relationships with HRC-1 and HRC-3, despite their status as major profit generators. At Swedbank Estonia, the off-boarding exercise was designed to eliminate (1) HRNR customers registered in "*low tax rate jurisdictions . . . whose beneficiary has a weak connection*" to Estonia; (2) other HRNR customers with "*a weak link*" to Estonia and whose beneficial owner was registered in "*low tax rate areas*"; and (3) any accounts of HRNR financial institutions.
- In 2017, Swedbank implemented a new Group-level policy on risk appetite that required, among other things, a documented process to ensure that any residual AML/CTF risk was consistent with the Group's risk appetite. Swedbank Latvia and Group Compliance also agreed to terminate customer relationships with HRC-5 and HRC-6.
- In 2018, Swedbank expended considerable effort examining counterparty risk from other financial institutions in the Baltics, identifying hundreds of customers to off-board because they were inconsistent with the Group's risk appetite.

In connection with these de-risking efforts, Swedbank conducted internal audits and retained external consultants. For example, in February 2017, Swedbank engaged Grimstad AS to assist with the off-boarding of HRC-1 and to assess related AML risks and employee conduct issues within Swedbank Estonia. This initiative, in which Grimstad AS worked closely with certain members of Group Risk and Group Compliance, became known as "Project Clear." Ultimately, Project Clear identified 208 customers that Swedbank Estonia proceeded to off-board.

Also beginning in 2017, Swedbank initiated several internal reviews to assess its exposure to potential money laundering through CPB-1. In late 2018, Swedbank took steps to address the findings from these reviews and to identify customers that engaged in potentially suspicious transactions with CPB-1 counterparties. These efforts were known internally as "Project Nemo."

Thus, at the time of Clifford Chance's engagement in February 2019, Swedbank already had initiated efforts to address shortcomings in its AML/CTF policies and procedures. To some extent, Swedbank's efforts were driven by public disclosures about billions of dollars of suspicious transactions with links to various money laundering scandals.

But Swedbank was also motivated by internal forces that viewed an HRNR portfolio as inconsistent with Swedbank's roots as a savings bank with a predominantly low risk retail banking customer base.

As the foregoing chronology demonstrates, Swedbank's de-risking efforts since 2016 were inhibited by persistent deficiencies in Swedbank's governance, lack of clear and consistent ownership over AML/CTF and sanctions controls and insufficient attention to AML/CTF and sanctions issues.

B. Swedbank's Remediation Efforts since 2019

Since February 2019, when Clifford Chance's engagement began, Swedbank has taken additional remedial steps, including: (1) formation and implementation of a remediation plan with 152 remedial actions, many of which Swedbank reports have already been completed; (2) engagement of additional external consultants to assist in its remediation efforts; (3) review of corporate governance; (4) ongoing efforts to off-board additional high risk customers who do not meet Swedbank's risk appetite; (5) efforts to increase the resources devoted to AML/CTF monitoring and compliance in Swedbank's first and second lines of defense; and (6) employment actions. In addition, in July 2019 the Board established a working group, now the Corporate Governance Committee, which is the Board's advisory body to monitor the Bank's work with the ongoing investigations among other responsibilities.

1. Swedbank's Remediation Plan

Swedbank's Group-wide AML/CTF remediation plan ("**Remediation Plan**"), also referred to internally at Swedbank as the Group AML/CTF Activity List, is a consolidated effort conceived of and executed primarily by the AFC unit, which Swedbank formed in April 2019 to focus on AML/CTF, fraud prevention, cyber security, information security and physical security, and which includes GSI as part of the first line of defense. The AFC recognized the need for a consolidated, coordinated effort. This was because each of the Business Areas and Group Functions (as defined *supra* Section VI) had disparate remedial tasks to accomplish, as a result of earlier findings and recommendations from internal control functions, internal reviews and reviews by external consultants, and those tasks were not always prioritized, well-coordinated or carried out consistently.

As described in greater detail below, the AFC collected all of the tasks in a single consolidated Remediation Plan, and the tasks are now being completed at the Business Area and Group Function level, tracked by the AFC, verified as completed by Group Compliance and audited for by GIA, with ultimate reporting to the CEO and the Board. The Remediation Plan has also expanded over time to include additional findings and recommendations made by Clifford Chance as part of the Investigation, and by external consultants. The Remediation Plan involves Swedbank's three lines of defense: (1) the AFC; (2) Group Compliance; and (3) GIA, as well as (4) an external consultant.

Preparation of the Remediation Plan. To develop the list of action points that make up the Remediation Plan, AFC asked the Business Areas and Group Functions to identify the remediation tasks that needed to be completed. Based on the responses, in October 2019, the AFC prepared an initial list of 132 action points, which was expanded, based on further discussions with Business Areas and Group Functions and on issues identified by Clifford Chance and external consultants, to 152 points in December 2019. Swedbank expects the list to continue to grow as various financial regulators issue their findings.

As part of Clifford Chance's review and analysis of historical investigative reports collected from Swedbank's Compliance and GIA functions, Clifford Chance assessed the status of Swedbank's prior remediation efforts with respect to AML and sanctions risk management. Clifford Chance provided Swedbank with summaries and assessments

of high-priority remediation measures, including: (1) relevant tasks and time periods; (2) Swedbank functions responsible for implementing these recommendations; (3) the current status; and (4) Clifford Chance's recommended follow-up actions. Swedbank reviewed these recommendations and expanded the Remediation Plan to include additional points where the recommendations were not already covered in the Plan.

Examples of key action items include the following actions at the AFC level:

- retaining an external consultant on an annual basis to conduct an independent assessment of Swedbank's AML/CTF framework;
- improving Swedbank's governance over AML/CTF functions by ensuring that responsibilities are clearly defined, instructions and reporting lines are clear, and resources are adequate;
- updating Swedbank's AML/CTF framework by revising and updating Group policies, directives and instructions on various topics, including economic sanctions, KYC, investigations, FIU reporting and training;
- updating Swedbank's AML/CTF risk management, such as by developing key risk and key performance indicators to assess improvements to the framework and test the risk appetite;
- increasing competence and resources—with additional funding and new hires—to enhance the Bank's ability to investigate suspicious customers and behaviors;
- increasing capacity in transaction-monitoring scenario development and developing next generation tools and technologies to increase efficiency in detecting financial crime; and
- updating the sanctions screening system to achieve efficiency enhancements in the sanctions screening process.

Within Swedish Banking, the Remediation Plan includes the following key action items:

- planning and executing targeted KYC initiatives to address outstanding KYC issues and increase KYC quality, including measures to address KYC backlogs;
- developing and implementing a new risk classification model that consists of a set of rules-based scenarios combined with a predictive model to increase quality; and
- developing of transaction monitoring scenarios in Swedish Banking.

Within LC&I, the Remediation Plan includes the following key action items:

- improving and expanding the risk-based transaction monitoring system by developing additional scenarios and by including monitoring of securities transactions and an automated solution for sanctions screening of counterparties; and
- updating KYC processes and KYC quality by enhancing the quality of CDD and EDD, improving KYC controls and screening in the Trade Finance process, and reviewing and updating internal routines.

Within Baltic Banking, the Remediation Plan includes the following key action items:

- reviewing and providing feedback on the updated AML/CTF framework being developed by the AFC;
- reviewing the AML/CTF risk management framework and applying a risk-based approach to mitigate money laundering and terrorist financing exposure effectively and efficiently, which includes agreeing on KYC principles and making a series of improvements to the CDD and EDD processes; and
- improving transaction screening and monitoring tools by developing additional scenarios.

Most of these representative action items have further sub-items that count toward the total number of action items in the Remediation Plan.

Management of the Remediation Plan. The AFC is responsible for managing the milestones in the Remediation Plan, following up with the Business Areas and monitoring progress of all milestones. To do this, the AFC conducts one-on-one meetings with each of the Business Areas on a monthly basis to identify and monitor the status of the action items. The first such meetings occurred in September 2019. The AFC tracks the status of all action items and provides a report to Group Compliance each month.

Validation of Completed Action Items. Group Compliance analyzes the information provided by the Business Areas and Group Functions and validates any milestone that the AFC designates as closed. Group Compliance prioritizes higher-risk milestones, and categorizes each milestone based on the complexity required to validate it. Thus, high-complexity validation "*requires analysis, testing and, if applicable, model validation*"; moderate-complexity validation "*requires analysis of evidencing materials/ information*"; and low-complexity validation relies on "*evidencing materials and/or information without further analysis*." Group Compliance then meets with the Business Area and to develop a validation plan. For high-complexity milestones, the validation may include monitoring exercises and a scoping memo; for low-complexity milestones, Group Compliance may only include notes on the list circulated by the AFC.

After the assessment, Group Compliance will either (1) validate the AFC's assessment in all material aspects, or (2) conclude that the milestone requires further action. If the latter, the Business Area will need to address the issue and then Group Compliance will re-validate.

Group Compliance plans to provide the AFC with updates of its assessments on at least a quarterly basis and will report to the GRCC when milestones are completed or delayed. Group Compliance will also report to the Board of Directors and the CEO on a quarterly basis, providing a summary report of milestones that are validated and those that require further action.

GIA Assessment. After Group Compliance validates the milestone, GIA conducts a separate assessment. GIA essentially audits Group Compliance's validation of the business activities on a risk-basis and then determines whether to validate Group Compliance's work or revert to the first line of defense.

Focusing primarily on whether it concurs with the criteria that Group Compliance used for its assessment, GIA will: (1) validate the review by Group Compliance; (2) coordinate with Group Compliance to determine whether GIA should consider a different scope; or (3) conduct a specific audit of the milestone. As part of the process, GIA meets with Group Compliance, the AFC, Baltic Banking, Swedish Banking and LC&I monthly to understand the milestone and the basis for closing the milestone out.

Once GIA completes its assessment, GIA reports its findings to the Board.

Finally, as part of its ongoing work, Swedbank's external auditor—one of the "Big Four" accounting firms—reviews the status of the Remediation Plan. As part of that assessment, the external auditor is currently conducting a governance audit, jointly with GIA, to determine whether the AFC has effectively implemented the Remediation Plan.

Status of Remediation Plan. As of mid-January 2020, according to a report provided by the AFC to the GRCC, the total number of closed milestones was 67 out of 152, with 47 of the 67 closed in Q4 2019. Among the notable milestones closed in Q4 2019 were:

- increasing and enhancing transaction monitoring within Baltic Banking by adding 25 transaction monitoring scenarios;

- updating the Group AML/CTF framework;
- initiating a project to support the Business Areas and Group Functions in implementing the updated AML/CTF framework;
- implementing a new risk classification model for Swedish Banking with rule-based scenarios and a predictive model; and
- rolling out digital KYC to 3.6 million private customers in Swedish Banking.

In the same presentation to the GRCC, the AFC noted that it expected up to 30 additional milestones to be closed in Q1 2020, focusing on continued efforts to implement the Group AML/CTF framework. The AFC also reported that certain milestones had been delayed and could not be closed within deadlines set in 2019, including milestones related to the development of transaction monitoring scenarios in Swedish Banking, certain improvements to the EDD process in Swedish Banking and LC&I and efforts to clear KYC backlogs in Swedish Banking.

Group Compliance is in the process of assessing all of the closed milestones. On 27 January 2020, Group Compliance reported to the Board and the CEO that it had validated 21 of the 67 closed milestones, and had concluded that three milestones required further action. As an example of the latter, Group Compliance noted that the risk appetite statement was not sufficiently detailed and had not been updated since spring of 2019, before the Board of Directors and CEO were replaced.

GIA is currently performing an audit of the Remediation Plan and will begin to review closed milestones in Q2. Anticipating the demands of the Remediation Plan, the Board of Directors in January 2020 approved an increase in GIA's full-time employees ("**FTE**") to 70.

2. Engagement of External Consultants

As part of its Remediation Plan, Swedbank has engaged a number of external consultants to assist with various remediation efforts, which include the following:

- *Review of Compliance*: Swedbank's Group Compliance function has engaged a consultant to analyze Swedbank's overall structure to manage and control compliance risks and to assess whether Swedbank's Compliance function is aligned with industry standards. Based on this analysis, the consultant will assist Swedbank in developing a Target Operating Model with a focus on the Compliance function, including how to effectively manage Compliance risks within Swedbank.
- *Review of Swedbank's Culture*: Swedbank's Group HR function is working with an external consulting firm to develop its ability to understand, assess and improve the culture of Swedbank's businesses. The goal of the review is to create a roadmap for achieving Swedbank's cultural goals.
- *Review of Swedbank's Transaction Monitoring System*: In 2019, Swedbank engaged an external consultant to conduct a maturity assessment of its transaction monitoring system. This includes an assessment of Swedbank's current transaction monitoring system and any planned transaction monitoring systems against the Bank's EMEA and Nordic peers.
- *AML/CTF Program Review:* Swedbank plans to engage a consultant to assess the current state of Swedbank's policies, procedures, systems and controls, including their implementation. The consultant will identify any gaps by measuring against regulatory requirements and industry best practices. The consultant will help Swedbank address any such gaps and then conduct assessments to confirm that gaps have been addressed and that Swedbank's policies, procedures, systems and controls remain effective.

3. Corporate Governance Review Project

Swedbank's Corporate Governance Review Project was initiated by Swedbank's Board in December 2019 and is designed to ensure that Swedbank, as a Parent Company, has a sound and effective corporate governance model in place across the Group that is clear, consistent and in line with best practices, taking into consideration the Group's size, complexity and strategy. Swedbank's CEO has overall responsibility for the Project and is supported by a Steering Group that is chaired by the Group's Chief Legal Officer ("**CLO**") and includes the CCO, the CRO, the Deputy CLO, the Head of Baltic Banking and the Head of Swedish Banking, with other participants to be determined. The Project Leader is from the CFO's office or an external resource. The Project Manager is a Senior Legal Counsel. As part of the Project, the Bank will review the managing boards, the supervising councils and the committees and will consider the relationship between the parent, its subsidiaries and sister companies, as well as the challenges of navigating the potentially conflicting regulations in Sweden and the Baltics relating to steering and control. The ultimate goal of the Project is to recommend improvements that will foster adequate reporting, escalation, decision-making, responsibility and accountability within the Group with respect to both the legal and the organizational structure.

4. Continued De-Risking of Swedbank's Customer Portfolio

To assist Swedbank in its ongoing efforts to de-risk its customer portfolio—a process that, as explained above, has been underway for several years—Clifford Chance and Swedbank have developed a protocol to review current customers for possible off-boarding. Clifford Chance reviewed recommendations from Swedbank's off-boarding initiatives since 2016, as documented in the Compliance and GIA reports, and worked with Swedbank to establish the current status of higher risk clients or client groups identified as part of those initiatives. Higher risk clients or client groups that remained customers of Swedbank became part of a population of customers under review.

To carry out the review, Swedbank has set up a team from the Baltic Subsidiaries ("**Current Customer Review Team**") to review the customers identified by Clifford Chance for possible off-boarding or, if the customer risk can be managed in a manner consistent with Swedbank's risk appetite, for applying restrictions or monitoring to the customer's future activity. Such risk-mitigating measures may include limits on certain products and services, additional EDD or full or partial blocks on certain funds transfers.

Where Clifford Chance has identified a customer of interest with open accounts at the Baltic Subsidiaries, the name and unique identifier of the customer is provided to the Current Customer Review Team, along with reasons for the identification of the customer. Pending the outcome of the review, the customer is placed on enhanced transaction monitoring and, if Swedbank determines that the customer engages in suspicious activity while subject to the enhanced monitoring, Swedbank suspends the account and considers appropriate reporting to the FIU. For each customer, the Current Customer Review Team researches and assesses its risk profile. Each assessment includes a recommendation for future action relating to the customer. Clifford Chance then reviews the recommendation and provides comments, after which Swedbank finalizes its decision and implements the recommendation.

5. Increasing Resources

Swedbank has been working to significantly increase its AML/CTF resources across all three lines of defense and in all three Business Areas.

6. Employment Actions

Finally, as discussed above in Section VII.F. regarding Employee Accountability, Swedbank has taken steps to remove employees and to appoint other employees to new roles in order to strengthen and demonstrate its commitment to AML/CTF and sanctions compliance. Among other actions, since Clifford Chance began the Investigation in February 2019, Swedbank has replaced its CEO, its Chairman of the Board and its CCO.

APPENDIX A

Key terms used in this report

AFC	Swedbank Group Anti-Financial Crime Unit established in 2019
AFCIS	Baltic Banking's Anti-financial Crime and Investigation Services Unit
AML	Anti-Money Laundering
AML Review Period	March 2014 to March 2019
AML Risk Identified Customers	Customers of interest to the Investigation as defined in Section IV.F., including the HRNR Customers
Baltic Banking	Baltic Banking Business Area of Swedbank AB
Baltic Subsidiaries	Swedbank Latvia, Swedbank Estonia, Swedbank Lithuania, collectively
BARCC	Business Area Risk and Compliance Committee
the Board	Swedbank AB Board of Directors
Business Areas	Swedish Banking, LC&I and Baltic Banking
CAE	Chief Audit Executive
CCO	Head of Compliance/Chief Compliance Officer
CDD	Customer Due Diligence
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CPB	Counterparty Bank, as in CPB-1, CPB-2, CPB-3, CPB-4, and CPB-5
Counterparty Risk Customers	Customers which transacted with counterparties who were customers of higher-risk financial institutions such as CPB-1, CPB-2, CPB-3, CPB-4, and CPB-5
EDD	Enhanced Due Diligence
EFSA	Estonian FSA (a.k.a. FI)
Estonian FIU	Estonian Police Financial Intelligence Unit (Rahapesu andmebüroo unit in the Police and Border Guard Board)
FCMC	Latvian Financial and Capital Market Commission
GCC-E	Swedbank's Group Credit Committee-Executive

GDPR	General Data Protection Regulation
Group Framework	Swedbank Group's compliance policies and procedures
GEC	Swedbank Group Executive Committee
GRCC	Group Risk and Compliance Committee
GIA	Swedbank Group Internal Audit
GSI	Swedbank Group Security and Investigations
Group Functions	The central divisions within Swedbank that support Swedbank's CEO and various business operations in relation to matters such as risk, IT and compliance
HBG	Hansabank Group
HRC	High Risk Customer, as in HRC-1, HRC-2, HRC-3, HRC-4, HRC-5, or HRC-6
HRCAC	Swedbank Estonia High-Risk Customer Acceptance Committee (HRCAC) or HRNR committee
HRNR Customer	High Risk Non-Resident Customers as defined by Swedbank's own criteria (i.e. non-resident legal entities registered outside the EU countries or Norway, and those registered in Malta, Cyprus, the United Kingdom or Luxembourg) with a high risk rating
ICIJ	International Consortium of Investigative Journalists
In-Scope Transactions	USD SWIFT payments processed by the Baltic Subsidiaries during the five-year period 22 March 2014 to 22 March 2019
IPB	Swedbank Estonia International Private Banking Department
LB	Lietuvos Bankas (Bank of Lithuania)
LC&I	Large Corporate & Institutions Business Area of Swedbank AB
KYC	Know Your Customer
KYC Data	Know-your-customer unstructured information collected by the Baltic Subsidiaries
NAK	Swedbank Latvia non-resident customer acceptance committee
MLRO	Money Laundering and Risk Officer
OFAC	Office of Foreign Assets Control
OFAC-Restricted Customers	Customers that were potentially the subject of OFAC sanctions as defined in Section IV.I.

Oligarch	A term that broadly refers to private sector persons in control of sufficient economic resources to influence national politics
PEP/RCA	Politically Exposed Person/Relatives and Close Associates
Primary AML Risk Identified Customers	A subset of AML Risk Identified Customers which constitute the customer groups representing the most direct risks of money laundering activity based on knowledge gained through the Investigation
Project Clear	An internal review and offboarding effort then conducted by Swedbank in 2007 to address the risks associated with the HRC-1 Group in Estonia
Public Statements Review Period	January 2014 through March 2019
RM	Relationship Manager
RCC	Risk and Capital Committee of the Swedbank Board
SFSA	Swedish Financial Supervisory Authority (Finansinspektione)
Sanctions Review Period	22 March 2014 through 22 March 2019
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
Structured Data	Data that is organized in clearly-defined fixed fields within a database, so that its elements can be made addressable for more effective processing and analysis, such as data tables or spreadsheets
Subject Transactions	USD SWIFT payments processed by the Baltic Subsidiaries during the five-year period 22 March 2014 through 22 March 2019 reviewed by the Investigation for compliance with OFAC blocking sanctions or country embargoes
Swedbank	Swedbank AB (publ)
Swedbank Estonia	Swedbank AS (Estonia)
Swedbank Latvia	Swedbank AS (Latvia)
Swedbank Lithuania	Swedbank AB (Lithuania)
Swedish Banking	Swedish Banking Division of Swedbank AB
the Investigation	Clifford Chance's Investigation
the Investigation Period	January 2007 through March 2019
the Report	Clifford Chance's Report
UBO	Ultimate Beneficial Owner

APPENDIX B

BOARD MEMBERS AND CEOs OF SWEDBANK AB 2015 - 2019

Board of Swedbank AB 2015 -2019				
2015	**2016**	**2017**	**2018**	**2019**
Anders Sundström (Chairman)	Lars Idermark (Chairman)	Lars Idermark (Chairman)	Lars Idermark (Chairman)	Lars Idermark (Chairman)[82]
Lars Idermark	Ulrika Francke	Ulrika Francke	Ulrika Francke	Göran Persson (Chairman)[83]
Ulrika Francke	Bodil Eriksson	Bodil Eriksson	Bodil Eriksson	Ulrika Francke[84]
Göran Hedman	Göran Hedman	Bo Johansson	Bo Johansson	Bodil Eriksson
Anders Igel	Peter Norman	Peter Norman	Peter Norman	Bo Johansson
Pia Rudengren	Pia Rudengren	Annika Poutiainen	Annika Poutiainen	Peter Norman[85]
Karl-Henrik Sundström	Siv Svensson	Mats Granryd	Mats Granryd	Annika Poutiainen[86]
Siv Svensson	Karl-Henrik Sundström	Siv Svensson	Siv Svensson	Mats Granryd
Maj-Charlotte Wallin	Camilla Linder (Employee Representative)	Magnus Uggla	Magnus Uggla	Siv Svensson[87]
Camilla Linder (Employee Representative)	Roger Ljung (Employee Representative)	Camilla Linder (Employee Representative)	Anna Mossberg	Magnus Uggla
Roger Ljung (Employee Representative)		Roger Ljung (Employee Representative)	Camilla Linder (Employee Representative)	Anna Mossberg
			Roger Ljung (Employee Representative)	Kerstin Hermansson[88]
				Bo Magnusson[89]
				Josefin Lindstrand[90]

CEOs of Swedbank AB 2009 – 2019	
March 2009 – February 2016	Michael Wolf
February 2016 – 28 March 2019	Birgitte Bonnesen

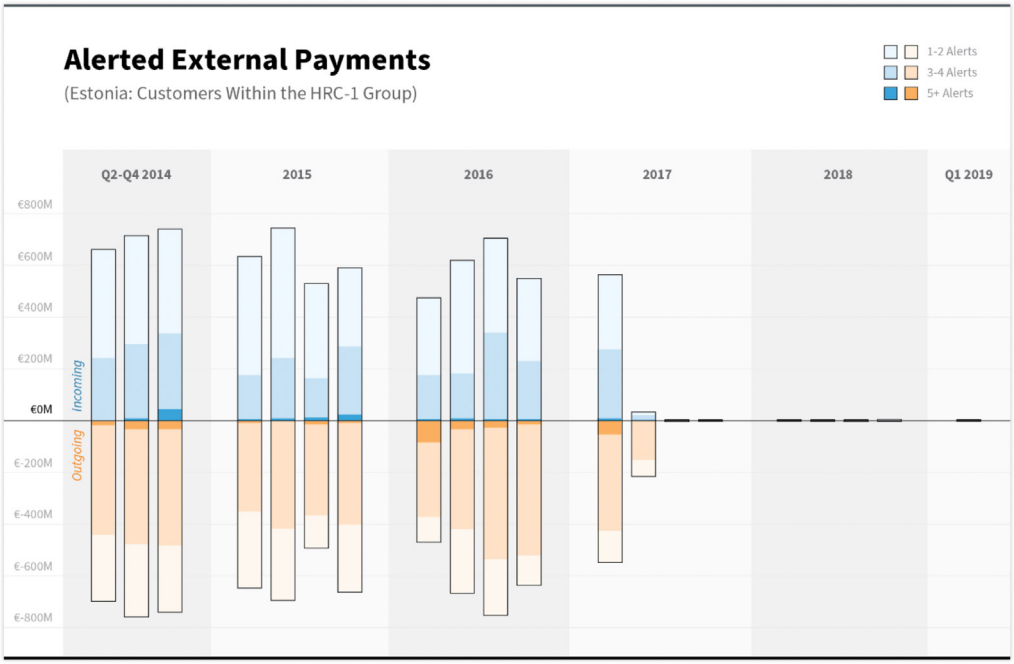
[82] Resigned 5 April 2019
[83] Appointed at extraordinary general meeting 19 June 2019
[84] Resigned 19 June 2019
[85] Resigned 19 June 2019
[86] Resigned 9 January 2019
[87] Resigned 19 June 2019
[88] Appointed at Annual General Meeting 28 March 2019
[89] Appointed at extraordinary general meeting 19 June 2019
[90] Appointed at extraordinary general meeting 19 June 2019

APPENDIX C

DETAILS ON SPECIFIC CUSTOMER GROUPS IN ESTONIA

A. HRC-1 GROUP

The alerted transactions relating to the customers within the HRC-1 Group are set out below, with shading to indicate the proportion of alerted transactions which triggered 1-2 alerts (light shading), 3-4 alerts (medium shading), and 5+ alerts (dark shading).:



A large proportion of alerted transactions for the HRC-1 Group relate to one company, HRC-1 (€5.1 billion incoming (66% of incoming alerted transactions) and €3.3 billion outgoing (42% of outgoing alerted transactions)). However, the vast majority of activity pertaining to this customer group ceased after Q1 2017 as the members of the HRC-1 Group were offboarded.

The following tables set out the underlying numbers for the above chart:

TOTAL INFLOW FOR HRC-1 GROUP CUSTOMERS ALERTING ON ANY ALGORITHMS IN €'MILLION (ESTONIA)

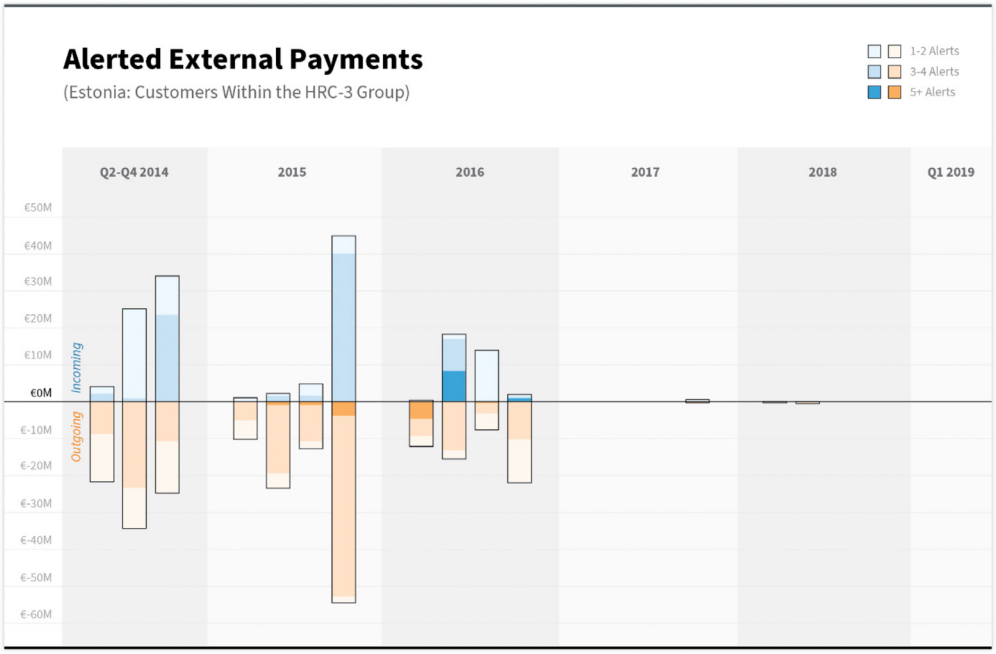
Number of Alerts	Q2-Q4 2014	2015	2016	2017	2018	Q1 2019
1-2 Alerts	1,237.0	1,622.4	1,413.6	299.9	0.8	0.1
3-4 Alerts	818.9	821.2	898.1	283.4	0.0	0.0
5 or more Alerts	55.3	47.4	30.8	9.5	0.0	0.0
Total	**2,111.3**	**2,491.0**	**2,342.6**	**592.8**	**0.8**	**0.1**

TOTAL OUTFLOW FOR HRC-1 GROUP CUSTOMERS ALERTING ON ANY ALGORITHMS IN €'MILLION (ESTONIA)

Number of Alerts	Q2-Q4 2014	2015	2016	2017	2018	Q1 2019
1-2 Alerts	793.5	957.3	675.5	186.6	5.0	0.6
3-4 Alerts	1,321.6	1,505.3	1,690.3	525.0	0.5	0.0
5 or more Alerts	83.8	33.8	160.2	54.2	0.0	0.0
Total	**2,198.9**	**2,496.4**	**2,526.0**	**765.7**	**5.5**	**0.6**

B. HRC-3 GROUP

The alerted transactions relating to the customers within the HRC-3 Group are set out below, with shading to indicate the proportion of alerted transactions which triggered 1-2 alerts (light shading), 3-4 alerts (medium shading), and 5+ alerts (dark shading):



As this chart demonstrates, the vast majority of activity pertaining to this customer group ceased after 2016 as the members of the HRC-3 Group were offboarded.

The following tables sets out the underlying numbers for the above chart:

TOTAL INFLOW FOR HRC-3 GROUP CUSTOMERS ALERTING ON ANY ALGORITHMS IN €'MILLION (ESTONIA)

Number of Alerts	Q2-Q4 2014	2015	2016	2017	2018	Q1 2019
1-2 Alerts	36.3	9.4	15.7	0.6	0.0	0.0
3-4 Alerts	26.7	43.3	9.5	0.0	0.0	0.0
5 or more Alerts	0.0	0.0	9.2	0.0	0.0	0.0
Total	**63.0**	**52.7**	**34.4**	**0.6**	**0.0**	**0.0**

TOTAL OUTFLOW FOR HRC-3 GROUP CUSTOMERS ALERTING ON ANY ALGORITHMS IN €'MILLION (ESTONIA)

Number of Alerts	Q2-Q4 2014	2015	2016	2017	2018	Q1 2019
1-2 Alerts	38.0	13.0	21.6	0.0	0.4	0.0
3-4 Alerts	42.7	82.2	30.8	0.0	0.2	0.0
5 or more Alerts	0.0	5.6	5.0	0.0	0.0	0.0
Total	**80.7**	**100.8**	**57.4**	**0.0**	**0.6**	**0.0**

APPENDIX D

ALERTED TRANSACTIONS IN THE BALTIC SUBSIDIARIES

1. Alerted Transactions in Estonia

The following table shows the value of external payment inflows for AML Risk Identified Customers which alerted on any algorithms throughout the AML Review Period. In total (across all currencies), there was the equivalent of €37.9 billion of external payment inflows which alerted on any algorithms throughout the AML Review Period.

TOTAL INFLOW FOR AML RISK IDENTIFIED CUSTOMERS ALERTING ON ANY ALGORITHMS IN €'MILLION (ESTONIA)

Number of Alerts	Q2-Q4 2014	2015	2016	2017	2018	Q1 2019
1-2 Alerts	5,037.1	6,782.2	6,686.4	5,010.8	3,683.1	818.0
3-4 Alerts	2,253.5	2,647.5	2,293.4	1,475.1	625.7	80.3
5 or more Alerts	236.7	88.8	92.5	59.6	14.1	0.6
Total	**7,527.3**	**9,518.5**	**9,072.3**	**6,545.4**	**4,322.9**	**898.9**

The following table shows the value of external payment outflows for AML Risk Identified Customers which alerted on any algorithms throughout the AML Review Period. In total (across all currencies), there was the equivalent of €37.0 billion of external payment outflows which alerted on any algorithms throughout the AML Review Period.

TOTAL OUTFLOW FOR AML RISK IDENTIFIED CUSTOMERS ALERTING ON ANY ALGORITHMS IN €'MILLION (ESTONIA)

Number of Alerts	Q2-Q4 2014	2015	2016	2017	2018	Q1 2019
1-2 Alerts	4,541.5	6,001.5	5,654.3	4,921.8	3,691.3	792.0
3-4 Alerts	2,409.8	2,942.5	2,888.5	1,740.8	621.3	175.5
5 or more Alerts	137.2	104.6	198.4	106.7	25.8	2.9
Total	**7,088.5**	**9,048.6**	**8,741.2**	**6,769.2**	**4,338.4**	**970.3**

2. Alerted Transactions in Latvia

The following table shows the value of external payment inflows for AML Risk Identified Customers which alerted on any algorithms throughout the AML Review Period. In total (across all currencies), there was the equivalent of €18.8 billion of external payment inflows which alerted on any algorithms throughout the AML Review Period.

TOTAL INFLOW FOR AML RISK IDENTIFIED CUSTOMERS ALERTING ON ANY ALGORITHMS IN €'MILLION (LATVIA)

Number of Alerts	Q2-Q4 2014	2015	2016	2017	2018	Q1 2019
1-2 Alerts	2,705.2	3,335.5	3,106.4	2,316.4	2,084.6	439.6
3-4 Alerts	867.5	1,726.0	1,107.2	586.1	334.4	51.1
5 or more Alerts	42.6	37.1	27.6	5.6	7.1	0.2
Total	**3,615.3**	**5,098.5**	**4,241.3**	**2,908.2**	**2,426.1**	**490.9**

The following table shows the value of external payment outflows for AML Risk Identified Customers which alerted on any algorithms throughout the AML Review Period. In total (across all currencies), there was the equivalent of €19.1 billion of external payment outflows which alerted on any algorithms throughout the AML Review Period.

TOTAL OUTFLOW FOR AML RISK IDENTIFIED CUSTOMERS ALERTING ON ANY ALGORITHMS IN €'MILLION (LATVIA)

Number of Alerts	Q2-Q4 2014	2015	2016	2017	2018	Q1 2019
1-2 Alerts	2,685.5	3,531.5	3,155.1	2,409.5	2,239.7	539.9
3-4 Alerts	686.9	1,311.8	1,049.4	439.3	419.2	90.6
5 or more Alerts	7.2	228.6	63.9	76.5	157.4	6.2
Total	**3,379.6**	**5,071.8**	**4,268.4**	**2,925.3**	**2,816.3**	**636.7**

3. Alerted Transactions in Lithuania

The following table shows the value of external payment inflows for AML Risk Identified Customers which alerted on any algorithms throughout the AML Review Period. In total (across all currencies), there was the equivalent of €18.7 billion of external payment inflows which alerted on any algorithms throughout the AML Review Period.

TOTAL INFLOW FOR AML RISK IDENTIFIED CUSTOMERS ALERTING ON ANY ALGORITHMS IN €'MILLION (LITHUANIA)

Number of Alerts	Q2-Q4 2014	2015	2016	2017	2018	Q1 2019
1-2 Alerts	3,255.6	2,362.1	2,482.6	2,995.9	3,720.5	744.8
3-4 Alerts	424.5	353.8	402.4	563.5	1,050.3	243.4
5 or more Alerts	0.6	24.5	16.5	28.7	42.8	5.5
Total	**3,680.7**	**2,740.4**	**2,901.6**	**3,588.1**	**4,813.6**	**993.7**

The following table shows the value of external payment outflows for AML Risk Identified Customers which alerted on any algorithms throughout the AML Review Period. In total (across all currencies), there was the equivalent of €21.2 billion of external payment outflows which alerted on any algorithms throughout the AML Review Period.

TOTAL OUTFLOW FOR AML RISK IDENTIFIED CUSTOMERS ALERTING ON ANY ALGORITHMS IN €'MILLION (LITHUANIA)

Number of Alerts	Q2-Q4 2014	2015	2016	2017	2018	Q1 2019
1-2 Alerts	3,561.7	2,844.2	3,008.0	3,614.4	4,192.0	932.5
3-4 Alerts	362.2	498.6	505.3	456.3	927.6	222.7
5 or more Alerts	4.2	7.5	13.5	4.1	7.6	0.4
Total	**3,928.1**	**3,350.2**	**3,526.7**	**4,074.8**	**5,127.2**	**1,155.7**

APPENDIX E

Local Implementation of EU AML Directives

The information and tables set forth below were prepared in consultation with local counsel in each of Sweden and the Baltics, to describe the implementation of the EU Directives into local legislation in Sweden, Estonia, Latvia and Lithuania.

A. Implementation in Sweden

On 1 August 2017, the Swedish AML Act (Sw. *lag (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism*) (the "**AML Act**") entered into force. Due to the relatively large number of amendments that were needed for the adequate implementation of the 4AMLD, the legislature proposed to repeal and replace the previous Swedish AML Act of 2009 with a new act, for purposes of accessibility and transparency. The preparatory work notes that the 4AMLD is a minimum harmonization directive and that Sweden as a member state may adopt or retain more stringent provisions in the field covered by the 4MLD to prevent money laundering and terrorist financing, so long as such regulations are within the limits of EU law. It is also noted that the 4MLD does not prevent member states from adopting regulations that are not covered by the Directive. Notwithstanding these possibilities for deviation, the AML Act mostly followed the provisions of 4MLD.

The majority of the provisions in 5MLD have been implemented in Swedish law by way of amendments to the AML Act, the Swedish Act on Registration of Beneficial Owners (Sw. *lag (2017:631) om registrering av verkliga huvudmän)* and relevant sectoral legislation as of 1 January 2020. A new act on a national account and safe-deposit boxes system will enter into force on 10 September 2020 to fulfill the requirements of art. 32a 5MLD.

The following additions and amendments to AML/CTF law in Sweden have been made in response to 4MLD and 5MLD.

No.	Legislation	Legal basis	Main provisions
1.	The AML Act Entered into force: 1 August 2017	4MLD	Legal framework regarding AML/CTF was revised entirely. Key changes included: • expansion of the definition of obliged entities; • expansion of the definition of PEPs; • increased focus on the risk-based approach, and requirements to consider a risk-based approach when conducting KYC, CDD, SDD, EDD and transaction monitoring; • less possibilities to rely only on simplified due diligence measures, and setting normal risk KYC/CDD as a standard.

No.	Legislation	Legal basis	Main provisions
2.	Amendments to the AML Act Enters into force: 1 April 2020	4AMLD	• clarifications regarding the obligation for the Financial Police to, where practicable, provide obliged entities with feedback on the effectiveness of, and follow-up on, reports of suspected money laundering or terrorist financing (SARs) to obliged entities (art. 46.3 4MLD). Such feedback and follow-up is to be provided in a timely manner; • clarification on certain parts of the definition of PEP (art. 3 4MLD); • clarification on CDD measures to be taken by entities conducting life or other investment-related insurance business (art. 13.5 4MLD).
3.	The Swedish Act on Registration of Beneficial Owners Entered into force: 1 August 2017	4MLD	• adoption of a new act in order to fulfill the requirements of art. 30–31 4MLD regarding holding of central register of information on each legal entity's and trust's beneficial ownership as well as obliged entities' obligation to disclose beneficial ownership information.
4.	The governmental regulation regarding measures against money laundering and terrorist financing (the **"AML regulation"**) Entered into force: 1 August 2017	The AML Act	• notification requirements for certain obliged entities requiring that such entities (mainly non-financial businesses) register with the Swedish Companies Registration Office (the **"SCRO"**). The SCRO shall keep a register over all such obliged entities required to register; • establishment of a department within the Swedish Police to act as the coordinator of the national response to the risks of money laundering and terrorist financing, fulfilling the requirements of art. 7 4MLD; • authorization for **SFSA**, together with certain administrative authorities and bodies, to issue regulations with more detailed requirements following from the AML Act.[91]
5.	The SFSA's regulations regarding measures against money laundering and terrorist financing (**"FFFS 2017:11"**)	The AML Act	• as elaborated under item 4, certain administrative authorities are empowered to legislate within their relevant supervisory areas. For obliged entities within the financial sector, the SFSA is the relevant supervisory authority. The SFSA's regulations include detailed provisions regarding, inter alia, the general risk assessment, education for employees and measures to be taken in order to verify identity; • obligations of the Money Laundering Reporting Officer as well as, where applicable, the Specially Appointed Executive and the control functions.
6.	Amendments to the AML Act Entered into force: 1 January 2020	5MLD	• more stringent CDD measures in relation to customers associated with high-risk third countries; • further limitations on the possibility to use CDD in relation to anonymous payment instruments. • increased protection for "whistle blowers".[92]

[91] Such authorization includes a delegation of legislative power to adopt provisions in relation to the obliged entities operating in different commercial fields, and may include provisions on, inter alia, the further content and scope of the general risk assessment, the risk classification of customers and the measures that may constitute simplified due diligence.

[92] Notably, the new Directive (EU) 2019/1937 of the European Parliament and of the European Council on the protection of persons who report breaches of EU law (whistle-blower directive) is not expected to precipitate additional requirements in the AML Act.

No.	Legislation	Legal basis	Main provisions
7.	Amendments to the Act on Registration of Beneficial Owners Entered into force: 1 January 2020	5MLD	• clarification regarding beneficial ownership of trusts and other types of legal arrangements (art. 31 5MLD).
8.	The Swedish Act on Account and Safe-Deposit Boxes System Enters into force: 10 September 2020	5MLD	• adoption of a new act to fulfill the requirements of art. 32a 5MLD regarding establishing a centralized automated mechanism/register for identification of any holder of payment accounts, banks accounts or safe-deposit boxes.
9	Amendments to FFFS 2017:11 Entered into force: 1 January 2020	The AML egulation, The SFSA's regulations regarding amend-ments to FFFS 2017:11 (FFFS 2019:28)	• provisions regarding the identification and analysis of threats towards employees, a new method for electronic identification of customers and the obligation for obliged entities to archive for ten years documentation made in connection with reporting to the Swedish Security Service.

B. Implementation in Estonia

In Estonia, the Money Laundering and Terrorist Financing Prevention Act (the **"AML/CTF Law"**) was in force until 2008 and consisted of only 30 provisions (including the implementing provisions of the act). Although strict rules relating to beneficial owners existed at that time, there was no legal obligation to identify beneficial owners unless there was suspicion. The EFSA had issued very brief and general guidelines on additional measures to prevent money laundering by credit institutions and financial institutions in 2002, and did not provide detailed AML guidelines until 2009.

A new version of the AML/CTF Law entered into force in 2008 and remained in force until 2017. Although the main structure of the act remained fairly intact during that time period, the content and interpretation of the norms and the obligations applicable to credit institutions changed significantly based on the evolving EFSA guidelines.

In 2014, the EFSA enacted more detailed AML/CTF guidelines, introducing new AML/CTF standards setting out, *inter alia*, recommendations on monitoring and screening and usage of IT solutions in the AML/CTF area.

The most recent EFSA AML guidelines entered into force on 1 March 2019, tripling in volume and setting a high bar on the obligations applicable to credit institutions.

The following is the overview of the pre-2017 AML regime:

No.	Legislation	Legal basis	Main provisions
1.	AML/CTF Law Adopted: 25 November 1998 Entered into force: 1 July 1999 Main amendments entered into force: 1 January 2004	1MLD and 2MLD	• general procedure for CDD; • procedure for identification of a beneficial owner in case there is a suspicion; • list of data that has to be registered; • obligation to appoint a compliance officer (contact person of FIU); • duty to report in case of suspicion of ML/TF.
2.	AML guidelines of the EFSA *"Additional measures to prevent money laundering by credit and financial institutions"* Entered into force: 1 August 2002	AML Law	• procedure for CDD; • general recommendation to update customer data regularly; • recommendations on applying KYC principle; • recommendations on establishing internal security measures; • duty to report in case of suspicion of ML.
3.	AML/CTF Law Adopted: 19 December 2007 Entered into force: 28 January 2008	3MLD	• general procedure for CDD; • procedure for simplified and enhanced CDD; • procedure for identification of beneficial owner; • variations of due diligence measures applied by credit institutions and financial institutions (e.g., face to face identification); • definition of PEP; • procedure for registration and preservation of data; • obligation to establish an AML policy; • obligation to appoint a compliance officer (contact person of FIU); • duty to report in case of suspicion of ML/TF.

No.	Legislation	Legal basis	Main provisions
4.	AML guidelines of the EFSA *"Additional measures to prevent money laundering and terrorist financing in credit and financial institutions"* Adopted: 22 October 2008 Entered into force: 1 April 2009	AML/CTF Law	• very general recommendation to monitor transactions; • recommendations on establishing internal rules (AML policy); • recommendations on compliance officer; • procedure for CDD; • recommendations on risk-based approach and categories of ML/TF risk ; • procedure for identification of a beneficial owner; 2009 AML guidelines did not include the following: • detailed recommendations on monitoring and screening of transactions; • recommendations on the different lines of defense in the AML/CTF area; • recommendations on the organizational set-up of AML/CTF compliance (except for the obligation to have a contact person in place for the FIU, independent from the business); • detailed recommendations to use IT systems and automated systems in monitoring and screening activities; • detailed recommendations to store data electronically or centrally; • recommendations to analyze related parties of the client or conduct negative media screening.
5.	AML guidelines of the EFSA "*Measures to prevent money laundering and terrorist financing in credit and financial institutions"* Adopted: 3 July 2013 Entered into force: 1 January 2014	AML/CTF Law	• procedure for organizational setup • recommendations on establishing internal rules (AML policy); • recommendations on compliance officer; • procedure for CDD; • recommendations on risk-based approach and categories of ML/TF risk ; • procedure for identification of a beneficial owner; • recommendations on monitoring and screening, • recommendation to use IT technical solutions in the AML/CTF area; 2014 AML guidelines did not include the following: • recommendations on the different lines of defense in the AML/CTF-area; • detailed recommendation to store data electronically or centrally; • detailed recommendations to analyze related parties of the client or conduct negative media screening.

The AML/CTF Law that was adopted on 26 October 2017 and entered into force on 27 November 2017 set out the Estonian AML regime. During the course of the implementation of 4MLD, the following major amendments to Estonian laws and regulations have been introduced by the Estonian Parliament, Minister of Finance and the EFSA:

No.	Legislation	Legal basis	Main provisions
1.	AML/CTF Law Adopted: 26 October 2017 Entered into force: 27 November 2017	4MLD	• procedure for enhanced CDD; • categories of ML/TF risk and relevant risk characteristics; • minimum extent of enhanced CDD at inception of business relationship with a customer; • minimum requirements for enhanced CDD performed during the business relationship; • procedure for identification of a beneficial owner; • procedure for enhanced monitoring of customer's transactions and relationship; • requirements for risk appetite; • requirements for risk assessment.
2.	Regulation of Minister of Finance *"Requirements and procedure for identification of persons and verification of person's identity data with information technology means"* Adopted: 23 May 2018 Entered into force: 28 May 2018	AML/CTF Law	• identification of persons and verification of person's identity data with information technology means (without meeting face to face).
3.	Advisory Guidelines of Estonian Financial Supervision Authority *"Organizational solutions and preventive measures for credit and financial institutions to take against money laundering and terrorist financing"* Adopted: 26 November 2018 Entered into force: 1 March 2019	AML/CTF Law	• procedure for organizational setup; • procedure for enhanced CDD; • categories of ML/TF risk and relevant risk characteristics; • minimum extent of enhanced CDD at inception of business relationship with a customer; • minimum requirements for enhanced CDD performed during business relationship; • procedure for identification of a beneficial owner; • procedure for ongoing monitoring and screening of customer's transactions and relationship; • requirements for risk appetite; • Requirements for risk assessment.

No.	Legislation	Legal basis	Main provisions
4.	Amendments to the Money Laundering and Terrorist Financing Prevention Act 5MLD is being implemented in two stages. First set of amendments was adopted on: 11 December 2019 Will enter into force: 10 March 2020 Second set of amendments initiated: 19 December 2019 (still under ongoing discussions in Estonian Parliament)	5MLD	First set of amendments includes stricter rules for virtual currency providers (shall be treated in the same way as financial institutions).The main changes to be introduced by the second set of amendments concern the following: • introducing new obligated persons; • amending the definition of PEPs; • amending the definition of beneficial owners; • procedure for protection of whistleblowing.

C. Implementation in Latvia

From June 1998 until August 2008, the AML/CTF regime mainly consisted of the law *"On the Prevention of Laundering of Proceeds Derived from Criminal Activity"* and relevant regulations of the Cabinet of Ministers of the Republic of Latvia (transposing 1MLD and 2MLD into Latvian law). The initial wording of the law set out provisions relating to (i) identification of clients; (ii) reporting of unusual and suspicious financial transactions; (iii) refraining from conducting suspicious transactions and suspending such transactions; (iv) development of internal control systems; (v) duties of supervisory and control authorities; (vi) information relating to the predecessor of the Latvian Financial Intelligence Unit, the Control Service; and (vii) international cooperation.

The years leading up to Latvia's joining the EU in 2004 brought rapid and significant changes to the AML/CTF regime. As a result of a growing need for reform of the AML/CTF regime, the existing laws and regulations were subsequently replaced in 2008 by the Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing (the **"AML/CTF Law"**), which transposed the 3MLD into Latvian law.

The AML/CTF Law was adopted on 17 July 2008 (and entered into force on 13 August 2008). The 4MLD, 5MLD and FATF guidance resulted in various additions and amendments to the AML/CTF Law and other laws and regulations, as set out below:

No.	Legislation	Legal basis	Main provisions
1.	Amendments to the AML/CTF Law Adopted: 26 May 2016 Entered into force: 29 June 2016	4MLD	• obligation to develop a policy for assessing the suitability of the employee and member of the management board responsible for the compliance with the requirements of the AML/CTF Law, and a procedure for division of tasks.

No.	Legislation	Legal basis	Main provisions
2.	Amendments to the AML/CTF Law Adopted: 26 October 2017 Entered into force: 9 November 2017	4MLD	• accessibility of the information necessary for the fulfillment of the requirements of the obliged entities from the Register of Enterprises of the Republic of Latvia; • obligation to perform risk assessment and to create an internal control system, as well as to update the risk assessment and to improve the internal control system; • obligation to conduct CDD; • CDD measures and risk factors; • identification of natural persons, legal persons and legal arrangements; • determination of the beneficial owner and ascertaining the conformity of the determined beneficial owner; • reporting obligation and obligation to determine the beneficial owner; • obligation of a legal person to disclose its beneficial owner; • availability of the information regarding beneficial owners; • supervision of business relationships and occasional transactions; • enhanced and simplified CDD; • non-participation of the customer in the onsite identification procedure in person; • correspondent banking relationship of credit institutions; • exemptions from CDD; • recognition and acceptance of the results of CDD; • storage, updating and destruction of CDD documents; • provision of the CDD documents and information to the Latvian FIU, supervisory and control authorities; • liability for violations in the field of prevention of ML/TF , and competence in imposing sanctions and implementing supervisory measures.

No.	Legislation	Legal basis	Main provisions
3.	FCMC regulations No. 2 *"Regulations for Enhanced Customer Due Diligence"* Adopted: 9 January 2018 Entered into force: 16 January 2018 Expired on: 1 December 2019 with the entry into force of FCMC regulations No. 135	AML/CTF Law; 4MLD	• procedure for enhanced CDD; • categories of the risk of ML/TF and relevant risk characteristics; • minimum extent of enhanced CDD at inception of business relationship with a customer; • minimum requirements for enhanced CDD performed during business relationship; • special measures of enhanced CDD ; • requirements for maintaining electronic database for information about non–resident customers; • procedure for enhanced monitoring of customer's transactions.
4.	FCMC regulations No. 3 *"Regulatory provisions for credit institutions and licensed payment and electronic money institutions on enhanced customer due diligence"* Adopted: 9 January 2018 Entered into force: 16 January 2018 Expired on: 1 December 2019 with the entry into force of FCMC regulations No. 135	AML/CTF Law; 4MLD	• enhanced CDD procedures; • risk segments and their corresponding risk factors of ML/TF; • minimum scope of enhanced CDD upon establishing a business relationship with the customer; • minimum requirements for enhanced CDD , performed during a business relationship; • special enhanced CDD measures; • requirements for maintenance of electronic databases of customer information subject to EDD ; • enhanced monitoring procedures of customer transactions.
5.	Cabinet of Ministers of the Republic of Latvia regulations No. 392 *"Procedure by which the Obliged Entity of the Law on the Prevention of Money Laundering and Terrorism Financing Performs the Remote Identification of a Customer"* Adopted: 3 July 2018 Entered into force: 6 July 2018	AML/CTF Law; 4MLD	• restrictions on the application of the remote identification of a customer; • rights and obligations of the obliged entity of the AML/CTF Law regarding the remote identification of a customer; • performance of video identification; • use of technological solutions in the remote identification of a customer.

No.	Legislation	Legal basis	Main provisions
6.	Amendments to the Law on International Sanctions and National Sanctions of the Republic of Latvia ("**Sanctions Law**") Adopted: 21 June 2018 Entered into force: 12 July 2018	Initiative by the Ministry of Foreign Affairs of the Republic of Latvia; FATF Recommendations 2012	• purpose and scope of application of the Sanctions Law; • imposition of sanctions in the fields of public procurements and public-private partnerships; • obligation to conduct sanctions risk assessment and to establish an internal control system; • liability for violations in the field of the requirements of international and national sanctions; • procedures for the use of fines; • statute of limitations.
7.	FCMC regulations No. 1 *"Regulatory Provisions for the Money Laundering and Terrorism Financing Risk Management"* Adopted: 3 January 2019 Entered into force: 12 January 2019	AML/CTF Law; 4MLD	• ML/TF risk management and internal control system for ML/TF risk management; • ML/TF risk management strategy; • responsibility of officials and employees of a credit institution; • supervision of ML/TF risk exposure.
8.	FCMC regulations No. 13 *"Regulatory Provisions for the Management of Sanctions Risk"* Adopted: 29 January 2019 Entered into force: 12 February 2019	Sanctions Law FATF Recommendations 2012	• assessment of sanctions risk and internal control system for the management of sanctions risk; • conditions and requirements in relation to the sanctions imposed by EU or NATO member states.

No.	Legislation	Legal basis	Main provisions
9.	Amendments to the AML/CTF Law Adopted: 13 June 2019 Entered into force: 29 June 2019	5MLD; FATF Recom-menda-tions 2012	• obligation of other persons in relation to provision of information regarding suspicious transactions; • accessibility of the information necessary for the fulfilment of the requirements of the AML/CTF Law to the obliged entities and supervisory and control authorities from the information systems of the Republic of Latvia; • general conditions for processing of personal data; • requirements for a member of the senior management and the employee responsible for the compliance with the requirements of the AML/CTF Law and conformity assessment of the applicant; • prohibition to maintain anonymous accounts and anonymous individual strong-boxes; • determination of the beneficial owner and ascertaining the conformity of the determined beneficial owner; • reporting obligation and obligation to determine the beneficial owner; • obligation of a legal person to disclose its beneficial owner; • availability of the information regarding beneficial owners; • supervision of business relationships and occasional transactions and liability of the obliged entities; • business relationship with a customer from a high-risk third country; • reporting on suspicious transactions; • submission of threshold declarations; • exchange of information between credit institutions and financial institutions; • obligation to store information and disclosure of information to the supervisory and control authorities of credit institutions and financial institutions; • exchange of information and cooperation between the supervisory and control authorities of credit institutions and financial institutions; • reporting of violations of the AML/CTF Law (or potential violations) to the supervisory and control authority and prohibition to cause unfavorable consequences.

No.	Legislation	Legal basis	Main provisions
10.	Amendments to the Sanctions Law Adopted: 13 June 2019 Entered into force: 4 July 2019	Initiative by the Ministry of Foreign Affairs of the Republic of Latvia; FATF Recom-menda-tions 2012	• proposition of international sanctions; • financial and civil legal restrictions; • imposition of sanctions in the fields of public procurements and public-private partnerships; • imposition of sanctions in the field of EU funds and other foreign financial assistance; • entry into agreements in the field of public or private law and making of payments when sanctions are imposed; • obligation to conduct sanctions risk assessment and to establish an internal control system; • liability for violations in the field of the requirements of international and national sanctions; • discharge of the liability of a person; • Sanctions Coordination Council; • reporting obligation.
11.	Cabinet of Ministers of the Republic of Latvia regulations No. 281 *"Regulations on Unusual Transaction Indicator List and Procedure for Reporting Unusual and Suspicious Transactions"* Adopted: 2 July 2019 Entered into force: 10 July 2019 Expired on: 17 December 2019 with the entry into force of Cabinet of Ministers of the Republic of Latvia regulations No. 408	AML/CTF Law 5MLD	• indicators of unusual transactions; • information to be included in the suspicious transaction report; • reporting procedure.

No.	Legislation	Legal basis	Main provisions
14.	FCMC regulations No. 125 *"Regulations on Independent Audit of Internal Control System for Prevention of Money Laundering and Terrorism and Proliferation Financing"* Adopted: 8 August 2019 Entered into force: 16 August 2019	AML/CTF Law; 4MLD	• scope and regularity of the audit; • procedure for conducting the audit. .
15.	FCMC regulations No. 135 *"Regulations on Customer Due Diligence, Enhanced Customer Due Diligence and Development of Risk Scoring System"* Adopted: 21 August 2019 Entered into force: 1 December 2019	AML/CTF Law 4MLD 5MLD	• development of risk scoring system; • requirements and procedure for conducting CDD and enhanced CDD; • requirements for enhanced customer and transactions monitoring.
16.	Cabinet of Ministers of the Republic of Latvia regulations No. 407 *"Regulations on Procedure for Submitting and Contents of Threshold Declaration"* Adopted: 27 August 2019 Entered into force: 17 December 2019	AML/CTF Law	• when to submit a threshold declaration; • information to be included in the threshold declaration; • submission procedure.

No.	Legislation	Legal basis	Main provisions
17.	Cabinet of Ministers of the Republic of Latvia regulations No. 408 *"Regulations on Procedure for Reporting Suspicious Transactions"* Adopted: 27 August 2019 Entered into force: 17 December 2019	AML/CTF Law	• information to be included in the suspicious transaction report; • reporting procedure.

D. Implementation in Lithuania

The first *"Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania"* (the **"AML Law"**) was adopted on 19 June 1997 and entered into force on 1 January 1998. Originally consisting of 20 Articles, the AML Law established: (i) the definition of money laundering and the prevention of money laundering; (ii) authorities responsible for implementation of AML measures—i.e. the Tax Police (since 2002, the Financial Crime Investigation Service at the Ministry of the Interior of the Republic of Lithuania (the **"FCIS"**)), the Bank of Lithuania, the Customs Department under the Ministry of Finance and the Government of the Republic of Lithuania—and the competence of these authorities; (iii) legal framework applicable to credit institutions, financial institutions and other entities in cases of suspicion of money laundering; and (iv) thresholds upon which the CDD procedures need to be performed.

Major changes to the AML Law were introduced in 2004. The revised AML Law provided for the concept of terrorist financing and a more detailed description of money laundering. From 1997 through 2004, the list of authorities responsible for the prevention of money laundering and terrorist financing was expanded to include such institutions as the Security Department of the Republic of Lithuania, the Lithuanian Bar Association and others. The number of subjects that were required to monitor suspicious transactions and/or monetary operations also increased, to include as obliged entities auditors, attorneys-at-law and assistant attorneys-at-law. These obliged entities were required to perform CDD procedures if the amount of a transaction and/or monetary operation exceeded the threshold stipulated by the AML Law and to adhere to other obligations established therein.

In 2008, the prevention measures outlined in the AML Law were expanded to cover terrorist financing. The AML Law of 2008 additionally introduced: (i) the definition of terms such as close associate, business relationship, shell bank, beneficial owner; (ii) the concept and procedure of simplified and enhanced CDD and beneficial owner due diligence; (iii) provisions regulating co-operation with other EU countries in the field of money laundering and terrorist financing prevention and (iv) procedures for reporting of suspicious or unusual transactions and/or monetary operations to the FCIS.

The amended AML Law, transposing the 4MLD into Lithuanian law, entered into force on 13 July 2017 (except for the provisions regulating disclosure of beneficial ownership information, which entered into force on 1 January 2019). The amendments were mostly drafted as per the provisions of 4MLD and revised Lithuania's AML/CTF regulation in its entirety.

The following additions and amendments to AML/CTF law in Lithuania were made in response to 4MLD, as set out below:

No.	Legislation	Legal basis	Main provisions
1.	AML Law Adopted: 29 June 2017 Entered into force: 13 July 2017	4MLD	Legal framework regarding AML/CTF was revised entirely. Key changes were the following: • broadening the definition of obliged entities; • broadening the definition of PEPs; • extended remote identification regulation; • changes in CDD regulation (including provision of exhaustive list of events when simplified CDD can be carried out and extended list of cases for enhanced CDD); • introduction of requirements for disclosure of beneficial ownership; • differentiation and application of individual sanctions.
2.	AML Law Adopted: 30 June 2018 Entered into force: 12 July 2018	Initiative of the Parliament	• minor amendments with respect to definition of PEPs.
3.	AML Law Adopted: 30 June 2018 Entered into force: 11 November 2018	Initiative of the Parliament	• minor amendments, including with respect to definition of customer, monetary operation and inclusion of state and municipality institutions and the Bank of Lithuania in the list of entities in respect of which simplified CDD can be applied.
4.	AML Law Adopted: 30 June 2018 Entered into force: 1 January 2019	Initiative of the Parliament	• minor amendments with respect to beneficial ownership disclosure of trusts.

In addition, the implementing AML/CTF regulation was revised by the Bank of Lithuania and the FCIS, namely:

No.	Legislation	Legal basis	Main provisions
1.	Order No V-7 of the Director of the Financial Crime Investigation Service at the Ministry of the Interior of the Republic of Lithuania of 17 January 2017 on instructions to prevent money laundering and/or terrorist financing designated to financial institutions not indicated in Article 4(1) of the Law on Prevention of Money Laundering and Terrorist Financing Adopted: 17 January 2017 Entered into force: 19 January 2017	AML Law	Legal framework regarding AML/CTF was established for financial institutions not indicated in Article 4(1) of the AML Law (obliged entities), i.e.: • risk assessment regulation; • customer and beneficial owner identification measures; • monitoring of customer business relationship; • provision of information to the FCIS; • retention of data; • other obligations (such as adoption of internal policies and procedures, implementation of international sanctions, etc.).
2.	Order No V-129 of the Director of the Financial Crime Investigation Service at the Ministry of the Interior of the Republic of Lithuania of 4 September 2017 on approval of rules for the management of registration journals of monetary operations, transactions and customers Adopted: 4 September 2017 Entered into force: 16 September 2017 (as amended on 13 April 2018)	AML Law	Established the legal framework for keeping of journals (registers) in accordance with the AML Law, i.e.: • information to be included in the journals (registers); • journals (registers) handling and retention procedures.

No.	Legislation	Legal basis	Main provisions
3.	Order No 1V-701 of the Minister of Interior of 16 October 2017 on approval of the description regarding suspension of suspicious monetary operations or transactions and provision of information regarding suspicious monetary operations or transactions to the Financial Crime Investigation Service at the Ministry of the Interior of the Republic of Lithuania and the description regarding information on monetary operations and transactions amounting to or exceeding €15,000 or equivalent in foreign currency submission to the Financial Crime Investigation Service at the Ministry of the Interior of the Republic of Lithuania Adopted: 16 October 2017 Entered into force: 17 October 2017	AML Law	Established the legal framework for suspension and reporting of suspicious monetary operations and transactions, i.e.: • submission of information to FCIS; • information submission requirements; • co-operation with FCIS.
4.	Order No V-131 of the Director of the Financial Crime Investigation Service at the Ministry of the Interior of the Republic of Lithuania of 12 September 2017 on approval of the description of the procedure of certification and submission of the copy of the personal identity document Adopted: 12 September 2017 Entered into force: 16 September 2017	AML Law	Established the legal framework for procedure for certification of the personal identity document.

No.	Legislation	Legal basis	Main provisions
5.	Order No V-314 of the Director of the Financial Crime Investigation Service at the Ministry of the Interior of the Republic of Lithuania of 30 November 2016 on approval of technical requirements applicable to customer identification process where the identity of the customer is identified remotely using electronic equipment allowing live stream Adopted: 11 October 2017 Entered into force: 18 October 2017	AML Law	Amended the legal framework for remote customer identification to correspond to the implementation of the 4MLD into national law.
6.	Order No V-240 of the Director of the Financial Crime Investigation Service at the Ministry of the Interior of the Republic of Lithuania of 5 December 2014 on approval of the possible list of criteria for recognition of money laundering and suspicious monetary operations or transactions Adopted: 8 November 2017 Entered into force: 16 November 2017	AML Law	A non-exhaustive list of criteria for recognition of AML/CTF has been supplemented to correspond to the implementation of the 4MLD into national law.
7.	Order No V-20 of the Director of the Financial Crime Investigation Service at the Ministry of the Interior of the Republic of Lithuania on criterion for determining large constant and regular customer-specific monetary operations Adopted: 24 January 2018 Entered into force: 26 January 2018	AML Law	It was stipulated that the criterion for establishing that the customer is constantly and regularly carrying out large monetary operations is when the customer has been in business for at least one year and the actual amount of cash receipts or payments in the last two quarters of the calendar year or financial year exceeds €300,000 or its equivalent in foreign currency.

No.	Legislation	Legal basis	Main provisions
8.	Decision of the Director of the Supervision Service of the Bank of Lithuania No 241-174 of 23 July 2018 regarding Application of Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions, adopted by the European Insurance and Occupational Pensions Authority, European Securities and Markets Authority and European Banking Authority Adopted: 23 July 2018 Entered into force: 23 July 2018	Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions	The decision established that the Bank of Lithuania and the financial market participants providing services in the Republic of Lithuania shall follow the recommendations stipulated in the guidelines.

In addition, regulation changes have been introduced with respect to the registration of beneficial ownership. As of 1 January 2019, beneficial ownership information must be collected and stored within all legal entities established in Lithuania and submitted to the Information System of Legal Entities Participants (**"JADIS"**). Amendments to JADIS regulations were adopted on 8 February 2019 and entered into force on 9 February 2019:[93]

No.	Legislation	Legal basis	Main provisions
1.	Order No 1R-231 of the Minister of Justice of the Republic of Lithuania of 11 October 2013 on the Approval of the Rules of the Information System for the Participants of Legal Entities Adopted: 8 February 2019 Entered into force: 9 February 2019	AML Law	Legal framework regarding submission of beneficial ownership data to JADIS and gaining of access to respective information thereof has been established, i.e.: • submission of information to JADIS system; • information submission procedure and requirements; • disclosure of beneficial ownership information.

[93] Although JADIS regulations have been updated and are in force, the JADIS system has not yet been technically updated. Therefore, for the time being it is not possible to submit beneficial ownership information. The respective technical amendments are expected to commence this coming year.

Amendments to the AML Law, transposing the 5MLD into Lithuanian law, entered into force on 10 January 2020. The amendments were mostly drafted as per the provisions of 5MLD.

The following additions and amendments to the AML Law were made in response to 5MLD, as set out below:

No.	Legislation	Legal basis	Main provisions
1.	AML Law Adopted: 3 December 2019 Entered into force: 10 January 2020 (some of the provisions will enter into force later this year or even next year)	5MLD	Key changes are the following: • broadening definition of the obliged entities (e.g., real estate agents are considered as such, but only in cases where the rent amounts to €10,000 or more); • introduction of the obligation of the state institutions to provide the FCIS with the information necessary for drawing up and updating the list of important public duties in the Republic of Lithuania; • expanded list of cases where customer and beneficial owner due diligence must be performed (in relation to transactions/monetary operations in virtual currency); • introduction of the possibility to collect the data about the customer directly from state information systems and registers; • expanded list of cases where information must be submitted to the FCIS (in relation to transactions/ monetary operations in virtual currency); • extended and more detailed information storage procedures; • expanded list of cases where enhanced CDD needs to be applied; • prohibition against financial institutions issuing anonymous passbooks or anonymous safe-deposit boxes, opening anonymous accounts or accounts under fictitious names; • introduction of additional provisions on cooperation of Lithuanian authorities with foreign authorities and the grounds on which the authorities may refuse to cooperate (e.g., if the cooperation interferes with criminal intelligence actions) and the circumstances under which non-cooperation is prohibited (e.g., the request concerns tax matters); • introduction of measures to reduce the risk posed by natural persons or legal entities established in high risk third countries, which are identified as such by the European Commission (e.g., restriction of business relations or transactions with persons residing in such countries); • conditions established for credit and electronic money institutions to derogate from the usual means of identification where there is a low risk of money laundering and terrorist financing; • prohibition on access to information about the customer or beneficial owner by third parties established in high risk third countries for the purpose of the prevention of money laundering and terrorist financing; • expanded list of cases where cash amounts need to be declared and the FCIS must be notified of the money being transported; • prohibition against starting a business relationship or executing one-off monetary operations, when beneficial ownership information has not been submitted to JADIS or the information is incorrect or misleading.

The implementing AML/CTF regulation was also revised by the FCIS, namely:

No.	Legislation	Legal basis	Main provisions
1.	Order No V-314 of the Director of the Financial Crime Investigation Service at the Ministry of the Interior of the Republic of Lithuania of 30 November 2016 on approval of technical requirements applicable to customer identification process where the identity of the customer is identified remotely using electronic equipment allowing live stream Adopted: 28 January 2020 Entered into force: 1 February 2020	AML Law	The requirement with respect to passport cover photo as well as the requirement that the customer's shoulders are visible during the identification have been removed.
2.	Order No V-240 of the Director of the Financial Crime Investigation Service at the Ministry of the Interior of the Republic of Lithuania of 5 December 2014 on approval of the possible list of criteria for recognition of money laundering and suspicious monetary operations or transactions Adopted: 10 January 2020 Entered into force: 15 January 2020	AML Law	A non-exhaustive list of criteria for recognition of AML/CTF has been supplemented.

APPENDIX F

FATF GUIDANCE

I. Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing - High Level Principles and Procedures [94]

First published in June 2007, this guidance aims to set out the key elements of an effective risk-based approach and identifies the types of issues that financial institutions may wish to consider when applying a risk-based approach.

The guidance notes that adopting a risk-based approach implies the adoption of a risk management process for dealing with money laundering and terrorist financing. This process encompasses recognizing the existence of the risk(s), undertaking an assessment of the risk(s) and developing strategies to manage and mitigate the identified risks. The guidance states that financial institutions should identify higher risk customers; products and services, including delivery channels; and geographical locations.

The guidance states that financial institutions should implement appropriate measures and controls to mitigate the potential money laundering risks of those customers that are determined to be higher risk as the result of the institution's risk-based approach. These measures and controls may include:

- increased awareness by the financial institution of higher risk customers and transactions within business lines across the institution;
- increased levels of KYC or EDD;
- escalation for approval of the establishment of an account or relationship;
- increased monitoring of transactions; and
- increased levels of ongoing controls and frequency of reviews of relationships.

The guidance further states that in order for financial institutions to have an effective risk-based approach, the risk-based process must be imbedded within the internal controls of the institution. Senior management are responsible for ensuring that the financial institution maintains an effective internal control structure, including suspicious activity monitoring and reporting. The guidance notes that strong senior management leadership and engagement in AML is an important aspect of the application of the risk-based approach. Senior management must also create a culture of compliance, ensuring that staff adhere to the financial institution's policies, procedures and processes designed to limit and control risks.

II. Risk-Based Approach Guidance for the Banking Sector

In 2014 the FATF supplemented its previous guidance with additional guidance on the application of a risk-based approach to AML compliance. The Guidance states that financial institutions should identify, assess and understand the ML/TF risks to which they are exposed and take AML/CTF measures commensurate to those risks in order to mitigate them effectively.

Risk Assessment:

Financial institutions should conduct a risk assessment, which forms the basis of their compliance framework and should enable the bank to understand how, and to what extent, it is vulnerable to ML/TF.

[94] https://www.fatf-gafi.org/

In identifying and assessing the ML/TF risk to which they are exposed, the guidance states that banks should consider a range of factors that may include:

- the nature, scale, diversity and complexity of their business;
- their target markets;
- the number of customers already identified as high risk;
- the jurisdictions the bank is exposed to, either through its own activities or the activities of customers, especially jurisdictions with relatively higher levels of corruption or organized crime, and/or deficient AML/CTF controls and listed by FATF;
- the distribution channels, including the extent to which the bank deals directly with the customer or the extent to which it relies (or is allowed to rely on) third parties to conduct CDDand the use of technology;
- the internal audit and regulatory findings; and
- the volume and size of its transactions, considering the usual activity of the bank and the profile of its customers.

Customer Due Diligence:

Banks should develop and implement policies and procedures to mitigate the ML/TF risks they have identified through their individual risk assessment. CDD processes should be designed to help banks understand who their customers are by requiring them to gather information on what they do and why they require banking services. The initial stages of the CDD process should be designed to help banks assess the ML/TF risk associated with a proposed business relationship, determine the level of CDD to be applied and deter persons from establishing a business relationship to conduct illicit activity.

Ongoing Customer Due Diligence/Monitoring:

Ongoing monitoring means the scrutiny of transactions to determine whether those transactions are consistent with the bank's knowledge of the customer and the nature and purpose of the banking product and the business relationship. Monitoring also involves identifying changes to the customer profile (for example, their behavior, use of products and the amount of money involved), and keeping it up to date, which may require the application of new, or additional, CDD measures. Monitoring transactions is an essential component in identifying transactions that are potentially suspicious.

Monitoring should be carried out on a continuous basis or triggered by specific transactions. It could also be used to compare a customer's activity with that of a peer group. It need not require electronic systems, although for some types of banking activity, where large volumes of transactions occur on a regular basis, automated systems may be the only realistic method of monitoring transactions. However, where automated systems are used, banks should understand their operating rules, verify their integrity on a regular basis and check that they address the identified ML/TF risks.

Reporting:

If a bank suspects, or has reasonable grounds to suspect, that funds are the proceeds of crime or are related to terrorist financing, it shall report its suspicions promptly to the relevant FIU. Banks should have the ability to flag unusual movement of funds or transactions for further analysis. Banks should have appropriate case management systems so that such funds or transactions are scrutinized in a timely manner and a determination made as to whether the funds or transaction are suspicious.

Internal Controls:

Adequate internal controls are a prerequisite for the effective implementation of policies and processes to mitigate ML/TF risk. Internal controls include (i) appropriate governance arrangements where responsibility for AML/CTF is clearly allocated; (ii) controls to monitor the integrity of staff, in accordance with the applicable local legislation, especially in cross-border situations; and (iii) the national risk assessment, where compliance and controls test the overall effectiveness of the bank's policies and processes to identify, assess and monitor risk.

Governance:

The successful implementation and effective operation of a risk-based approach to AML /CTF depends on strong senior management leadership and oversight of the development and implementation of the risk-based approach across the bank.

Assessment of Controls:

Banks should take steps to be satisfied that their AML/CTF policies and controls are adhered to and effective. To this end, their controls should be monitored on an ongoing basis by the bank's compliance officer. In addition, the adequacy of and compliance with banks' AML/CTF controls should be reviewed by an audit function.

CLIFFORD

CHANCE

Washington, D.C.
Clifford Chance
2001 K Street NW
Washington, DC 20006 - 1001
USA
Tel +1 202 912 5000
Fax +1 202 912 6000

New York
Clifford Chance
31 West 52nd Street
New York, NY 10019-6131
USA
Tel +1 212 878 8000
Fax +1 212 878 8375

Abu Dhabi
Clifford Chance
9th Floor, Al Sila Tower
Abu Dhabi Global Market Square
PO Box 26492
Abu Dhabi
United Arab Emirates
Tel +971 (0)2 613 2300
Fax +971 (0)2 613 2400

Amsterdam
Clifford Chance
IJsbaanpad 2
1076 CV Amsterdam
PO Box 251
1000 AG Amsterdam
The Netherlands
Tel +31 20 7119 000
Fax +31 20 7119 999

Barcelona
Clifford Chance
Av. Diagonal 682
08034 Barcelona
Spain
Tel +34 93 344 22 00
Fax +34 93 344 22 22

Beijing
Clifford Chance
33/F, China World Office 1
No. 1 Jianguomenwai Dajie
Chaoyang District
Beijing 100004
China
Tel +86 10 6535 2288
Fax +86 10 6505 9028

Brussels
Clifford Chance
Avenue Louise 65 Box 2
1050 Brussels
Belgium
Tel +32 2 533 5911
Fax +32 2 533 5959

Bucharest
Clifford Chance Badea
Excelsior Center
28-30 Academiei Street
12th Floor, Sector 1
Bucharest, 010016
Romania
Tel +40 21 66 66 100
Fax +40 21 66 66 111

Casablanca
Clifford Chance
57, Tour CFC, Casa Anfa,
Hay Hassani, Casablanca 20220
Morocco
Tel +212 520 008 600
Fax +212 520 008 640

Dubai
Clifford Chance
Level 15
Burj Daman
Dubai International Financial Centre
PO Box 9380
Dubai
United Arab Emirates
Tel +971 4 503 2600
Fax +971 4 503 2800

Düsseldorf
Clifford Chance
Königsallee 59
40215 Düsseldorf
Germany
Tel +49 211 43 55-0
Fax +49 211 43 55-5600

Frankfurt
Clifford Chance
Mainzer Landstraße 46
60325 Frankfurt am Main
Germany
Tel +49 69 71 99-01
Fax +49 69 71 99-4000

Hong Kong
Clifford Chance
27th Floor
Jardine House
One Connaught Place
Hong Kong
Tel +852 2825 8888
Fax +852 2825 8800

Istanbul
Clifford Chance
Kanyon Ofis Binasi Kat 10
Büyükdere Cad. No. 185
34394 Levent
Istanbul
Turkey
Tel +90 212 339 0001
Fax +90 212 339 0098

London
Clifford Chance
10 Upper Bank Street
London, E14 5JJ
United Kingdom
Tel +44 20 7006 1000
Fax +44 20 7006 5555

Luxembourg
Clifford Chance
10 boulevard G.D. Charlotte
B.P. 1147
L-1011 Luxembourg
Grand-Duché de Luxembourg
Tel +352 48 50 50 1
Fax +352 48 13 85

Madrid
Clifford Chance
Paseo de la Castellana 110
28046 Madrid
Spain
Tel +34 91 590 75 00
Fax +34 91 590 75 75

Milan
Clifford Chance
Via Broletto, 16
20121 Milan
Italy
Tel +39 02 806 341
Fax +39 02 806 34200

Moscow
Clifford Chance
Ul. Gasheka 6
125047 Moscow
Russian Federation
Tel +7 495 258 5050
Fax +7 495 258 5051

Munich
Clifford Chance
Lenbachplatz 1
80333 Munich
Germany
Tel +49 89 216 32-0
Fax +49 89 216 32-8600

Newcastle
Clifford Chance Newcastle Limited
Partnership House, Regent Farm
Road,
Gosforth, Newcastle upon Tyne,
NE3 3AF
Tel +44 20 7006 1000
Fax +44 20 7006 5555

Paris
Clifford Chance
1 rue d'Astorg
CS 60058
75377 Paris Cedex 08
France
Tel +33 1 44 05 52 52
Fax +33 1 44 05 52 00

Perth
Clifford Chance
Level 7, 190 St Georges Terrace
Perth, WA 6000
Australia
Tel +618 9262 5555
Fax +618 9262 5522

Prague
Clifford Chance
Jungmannova Plaza
Jungmannova 24
110 00 Prague 1
Czech Republic
Tel +420 222 555 222
Fax +420 222 555 000

Rome
Clifford Chance
Via Di Villa Sacchetti, 11
00197 Rome
Italy
Tel +39 06 422 911
Fax +39 06 422 91200

São Paulo
Clifford Chance
Rua Funchal 418 15th Floor
04551-060 São Paulo SP
Brazil
Tel +55 11 3019 6000
Fax +55 11 3019 6001

Seoul
Clifford Chance
22nd Floor, D1 Tower,
17, Jongno-3 gil,
Jongno-gu, Seoul 03155
Korea
Tel +82 2 6902 8000
Fax +82 2 6902 8001

Shanghai
Clifford Chance
25/F, HKRI Centre Tower 2
HKRI Taikoo Hui
288 Shi Men Yi Road
Shanghai 200041
People's Republic of China
Tel +86 21 2320 7288
Fax +86 21 2320 7256

Singapore
Clifford Chance
12 Marina Boulevard
25th Floor Tower 3
Marina Bay Financial Centre
Singapore 018982
Tel +65 6410 2200
Fax +65 6410 2288

Sydney
Clifford Chance
Level 16
No. 1 O'Connell Street
Sydney NSW 2000
Australia
Tel +612 8922 8000
Fax +612 8922 8088

Tokyo
Clifford Chance
Palace Building, 3rd floor
1-1, Marunouchi 1-chome
Chiyoda-ku, Tokyo
100-0005
Japan
Tel +81 (0)3 6632 6600
Fax +81 (0)3 6632 6699

Warsaw
Clifford Chance
Norway House
ul. Lwowska 19
00-660 Warszawa
Poland
Tel +48 22 627 11 77
Fax +48 22 627 14 66

*Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.
Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.