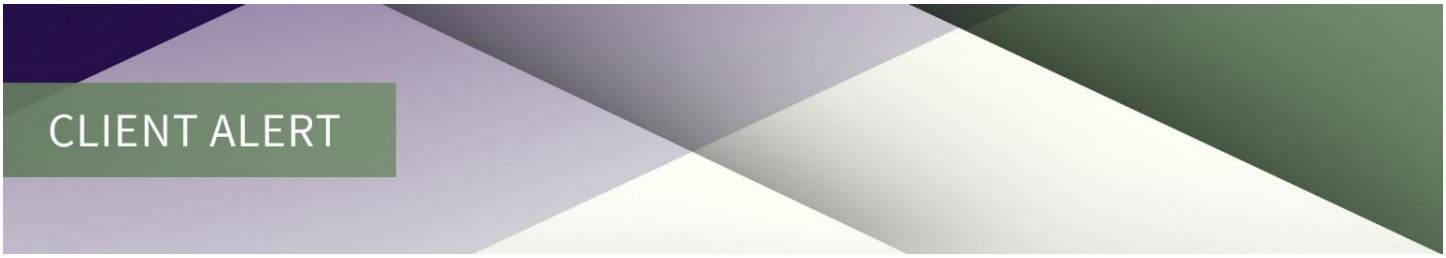

FinCEN and OFAC Advisories Highlight the Compliance Risks of Ransomware Attacks

October 12, 2020

AUTHORS

David Mortlock | Elizabeth Bower | Daniel K. Alvarez | Richard M. Borden
William J. Stellmach | Michael J. Gottlieb | Ahmad El-Gamal

On October 1, 2020, the U.S. Department of Treasury's Financial Crimes Enforcement Network ("FinCEN") and Office of Foreign Assets Control ("OFAC") released advisories highlighting, respectively, the reporting requirements for suspicious activity associated with ransomware as well as the sanctions-related compliance risks associated with facilitating ransomware payments on behalf of victims. The advisories cite the 37 percent increase in reported ransomware attacks and 147 percent annual increase in losses from ransomware attacks reported by the Federal Bureau of Investigation's 2018 and 2019 Internet Crime Reports as causes for significant concern. In light of these statistics, the departments sought to provide guidance on the regulatory risks to financial institutions and other entities arising from transactions or other activities in the wake of a ransomware attack.

Importantly, the advisories reaffirm and emphasize the prohibition on making ransom payments, directly or indirectly, to malicious cyber actors on OFAC's Specially Designated Nationals List (the "SDN List"). As described below, FinCEN states that reports to, and cooperation with, law enforcement may reduce potential fines for non-compliance. This may be cold comfort to victims of ransomware faced with the choice between the operations of networks and systems critical to their businesses, and non-compliance with federal law, but it does reaffirm the critical role of planning and taking preventative steps that seek to minimize both the likelihood of a successful attack and the potential scope of damage a successful attack might cause.

In addition to highlighting the compliance risks, the advisories encourage victims of ransomware attacks to contact the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection if an attack involves a U.S. financial institution or may cause significant disruption to a firm's ability to perform critical financial services.

1. Filing Suspicious Activity Reports

FinCEN's advisory notes that ransomware payments are typically multistep processes involving at least one depository institution and one or more money service businesses ("MSB").[1] Under the Bank Secrecy Act, MSBs and other regulated financial institutions are required to file suspicious activity reports for any transactions relevant to a possible violation of U.S. laws or regulations, including U.S. sanctions laws and regulations.[2] In order to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with ransomware attacks, FinCEN identified the following red flags:

- IT enterprise activity is connected to cyber indicators that have been associated with possible ransomware activity or cyber threat actors known to perpetrate ransomware schemes. Malicious cyber activity may be evident in system log files, network traffic, or file information.
- When opening a new account or during other interactions with the financial institution, a customer provides information that a payment is in response to a ransomware incident.
- A customer's convertible virtual currency ("CVC") address, or an address with which a customer conducts transactions, appears on open sources, or commercial or government analyses have linked those addresses to ransomware strains, payments, or related activity.
- A transaction occurs between an organization, especially an organization from a sector at high risk for targeting by ransomware (e.g., government, financial, educational, healthcare), and a digital forensics and incident response ("DFIR") or cyber insurance company ("CIC"), especially one known to facilitate ransomware payments.
- A DFIR or CIC customer receives funds from a customer company and shortly after receipt of funds sends equivalent amounts to a CVC exchange.

---

1 Money Service Business is defined as any person or entity operating in one or more of the following capacities: currency dealer or exchanger; check casher; issuer of traveler's checks, money orders or stored value; seller or redeemer of traveler's checks, money orders or stored value; money transmitter; U.S. Postal Service. This definition does not include a bank or person registered with and regulated or examined by, the U.S. Securities and Exchange Commission or the U.S. Commodity Futures Trading Commission. *See* 31 CFR § 1010.100(ff).

2 *See* 31 CFR § 1020.320.

- A customer shows limited knowledge of CVC during onboarding or via other interactions with the financial institution, yet inquires about or purchases CVC (particularly if in a large amount or rush requests), which may indicate the customer is a victim of ransomware.
- A DFIR, CIC, or other company that has no or limited history of CVC transactions sends a large CVC transaction, particularly if outside a company's normal business practices.
- A customer that has not identified itself to the CVC exchanger, or registered with FinCEN as a money transmitter, appears to be using the liquidity provided by the exchange to execute large numbers of offsetting transactions between various CVCs, which may indicate that the customer is acting as an unregistered MSB.
- A customer uses a CVC exchanger or foreign-located MSB in a high-risk jurisdiction lacking, or known to have inadequate, anti-money laundering or countering financing of terrorism regulations for CVC entities.
- A customer initiates multiple rapid trades between multiple CVCs, especially anonymity-enhanced cryptocurrencies, with no apparent related purpose, which may be indicative of attempts to break the chain of custody on the respective blockchains or further obfuscate the transaction.

Financial institutions should remain vigilant for signs of transactions related to illicit ransomware activity and be prepared to report their findings.

2. Sanctions-Related Compliance Risks

OFAC has designated, and indicated that it will continue to designate, malicious cyber actors to the SDN List under its Cyber-related Sanctions Program. U.S. persons are generally prohibited from entering into or facilitating direct or indirect transactions involving a person or entity on the SDN List. Non-U.S. persons can also be subject to OFAC enforcement actions by causing a U.S. person to violate U.S. sanctions laws. OFAC also highlighted the fact that ransomware attacks are increasingly originating from countries subject to comprehensive sanctions, such as Cuba, Iran, Syria, and North Korea. U.S. and non-U.S. persons face restrictions similar to those described above when entering into transactions involving individuals or entities in embargoed countries.

The advisory encourages financial institutions and companies, including those that engage with victims of ransomware attacks, to implement a risk-based compliance program that adheres to OFAC's Framework for Compliance Commitments.[3] OFAC specifically notes that their compliance programs should account for the risk that a ransomware payment may involve a person or entity on OFAC's SDN List or embargoed jurisdiction. OFAC generally considers a

[3] OFAC's Framework encourages a risk-based approach to compliance while maintaining a compliance program that incorporates the five essential components of compliance: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training.

strong compliance program as a mitigating factor when determining whether to bring an enforcement action and, if so, in calculating any penalty. Additionally, OFAC stated that it will also consider a self-initiated, timely, and complete report of a ransomware attack to law enforcement as well as full cooperation with law enforcement during and after the attack as a significant mitigating factor.

Victims of ransomware attacks, and their advisors and service providers, are encouraged to reach out to OFAC immediately if they believe a request for a ransomware payment may violate U.S. sanctions.

Recommendations

The Department of Treasury has clearly indicated its concern with the rising rates of and damage associated with cyber crime and ransomware attacks. In light of these advisories, we recommend that victims of ransomware, consultants representing victims in negotiations with attackers, financial institutions, including cyber insurance companies and other entities that may be involved in transactions for the payments of ransomware, review their compliance programs to ensure that they are in line with OFAC's Framework for Compliance Commitments. These companies also should provide appropriate training and internal guidance documents to help employees recognize transactions related to ransomware attacks that may require the filing of a suspicious activity report or violate U.S. sanctions.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

David Mortlock
202 303 1136
dmortlock@willkie.com

Elizabeth Bower
202 303 1252
ebower@willkie.com

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Richard M. Borden
212 728 3872
rborden@willkie.com

William J. Stellmach
202 303 1130
wstellmach@willkie.com

Michael J. Gottlieb
202 303 1442
mgottlieb@willkie.com

Ahmad El-Gamal
202 303 1142
ael-gamal@willkie.com