Crowell

CLIENT ALERT

OFAC and FinCEN Release Advisories on Risks of Ransomware Payments

October 8, 2020

On October 1, 2020, the Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN) each released advisories (the OFAC Advisory and the FinCEN Advisory) addressing financial crime-related risks associated with ransomware and ransomware payments. The OFAC Advisory focuses on the risk that ransomware attacks or payments may involve sanctioned persons or jurisdictions, the risk that paying ransoms, or otherwise dealing with ransomware attackers may result in liability under OFAC sanctions authorities, and the possibility for victims of such attacks to earn credit against potential sanctions penalties by voluntarily disclosing such attacks to law enforcement. The FinCEN Advisory draws attention to the potential for financial institutions to be used in the processing of ransomware payments, the risk that intermediaries that facilitate such payments may be deemed money transmitters, red flags of potential ransomware-related activity, and the need to report technical details related to such attacks in suspicious activity reporting.

Ransomware

The advisories both discuss ransomware issues and trends in general terms before turning to sanctions- and AML-specific aspects of these crimes. The OFAC Advisory defines ransomware as "a form of malicious software … designed to block access to a computer system or data, often by encrypting data or programs on information technology systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data." The perpetrators may also "threaten to publicly disclose victims' sensitive files," a tactic increasingly seen in ransomware attacks. The FinCEN Advisory defines ransomware in substantially similar terms, and also explains that perpetrators of ransomware attacks typically demand payment in convertible virtual currency (CVC), such as Bitcoin.

According to the OFAC Advisory, citing statistics from the Federal Bureau of Investigation, "there was a 37 percent annual increase in reported ransomware cases and a 147 percent annual increase in associated losses from 2018 to 2019." The FinCEN Advisory highlights a number of trends related to the increasing sophistication and scope of ransomware attacks, including:

- Big Game Hunting Schemes: Targeting of larger enterprises and significantly larger ransom demands.
- Ransomware Criminals Sharing Resources: Increased sharing of ready-made ransomware kits as well as "advice, code, trends, techniques and illegally-obtained information over shared platforms."
- "Double Extortion" Schemes: Threatening both to withhold access to the victim's systems and data along with threats to publish or sell the data to provide a "double" incentive to pay.
- Use of Anonymity-Enhanced Cryptocurrencies ("AECs"): Requiring or incentivizing victims to pay in AECs that include anonymizing features, such as mixing and cryptographic enhancements.
- Use of "Fileless" Ransomware: Fileless ransomware writes malicious code into the computer's memory rather than into a file on a hard drive, which is more difficult to detect and can circumvent off-the-shelf antivirus and malware defenses.

Finally, the FinCEN Advisory illustrates the complex transactions that are involved in making ransomware payments with CVC, in part to highlight for financial institutions the different sorts of actors that may be involved in these payments. A ransomware payment involving CVC typically begins with the victim transmitting funds via wire transfer, ACH or credit card payment to a CVC exchange in order to obtain the demanded form of CVC. Next, the victim sends the CVC to the perpetrator's designated account or CVC address. The perpetrator then launders the CVC using a variety of methods, including mixers and tumblers (mechanisms that obscure the link between sender and receiver), converting CVC into different CVCs, smurfing (breaking the funds into smaller amounts that move separately), and using many different accounts, exchanges, and peer-to-peer exchangers located in different jurisdictions.

Sanctions Risks and Issues in Ransomware Payments

The major sanctions-related risk in a ransomware attack is that a ransom payment will go to a sanctioned person or sanctioned jurisdiction. The OFAC Advisory emphasizes that OFAC "may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations." In this manner, OFAC suggests that it may be willing to penalize dealings with sanctioned parties even in situations where, as with ransomware, it is often difficult or impossible to know who is responsible for the attack or where any payment may be sent (and indeed where the goal of the attacker receiving payment is to maintain anonymity).

OFAC does not comment on the difficulty of determining who is responsible for a ransomware attack but does identify factors that may mitigate any enforcement action in the event a payment goes to a sanctioned actor.

First, OFAC encourages companies to maintain a *risk-based compliance program* to mitigate exposure to sanctions-related violations, and notes its previous guidance that OFAC will consider the "existence, nature, and adequacy of a sanctions compliance program" when determining an appropriate enforcement response. Adopting a risk-based approach to compliance generally also may benefit companies in other regulatory settings and allow companies to have a more focused approach to security.

Second, for "companies that engage with victims of ransomware attacks, such as those involved in providing cyber insurance, digital forensics and incident response," as well as "financial services" providers such as depository institutions and money services businesses, that may be involved in processing ransom payments, OFAC encourages such companies to maintain risk-based sanctions compliance programs that specifically "account for the risk that a ransomware payment may involve an SDN or blocked person, or a comprehensively embargoed jurisdiction." At the same time, OFAC does not address the key problem of determining sanctions risks in such situations – the difficulty in identifying the involvement of a sanctioned person or jurisdiction in what typically are designed to be anonymous attacks.

Third, OFAC will consider a "self-initiated, timely, and complete report of a ransomware attack to law enforcement" as well as "full and timely cooperation with law enforcement both during and after a ransomware attack" to be "significant mitigating factor[s]" in determining the appropriate enforcement outcome. OFAC does not define "law enforcement" or prescribe any particular agency to whom such a report should be made.

By contrast, although OFAC says that it will consider license applications to pay a ransomware attacker despite the potential involvement of sanctioned parties "on a case-by-case basis," it emphasizes that it approaches such applications with a

"presumption of denial," noting that such payments "benefit illicit actors and can undermine the national security and foreign policy of the United States," may "embolden cyber actors to engage in future attacks," and "do[] not guarantee that the victim will regain access to its stolen data."

In addition to its general admonition to companies to alert "law enforcement" to ransomware demands, OFAC encourages them to notify OFAC in particular in situations where they believe that a demand for a ransomware payment may involve a sanctions nexus, and also separately to notify the U.S. Department of the Treasury's Office of 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."

AML Risks and Issues in Ransomware Payments

The FinCEN Advisory focuses on the role of financial institutions, including banks and money services businesses (MSBs), in making ransomware payments, observing that "[p]rocessing ransomware payments is typically a multi-step process that involves at least one depository institution and one or more [MSBs]."

The FinCEN Advisory also discusses the role of "companies that provide protection and mitigation services to victims of ransomware attacks," including digital forensics and incident response companies (DFIRs) and cyber insurance companies (CICs). FinCEN warns that that activities by these companies to facilitate payments to perpetrators on behalf of victims, "[d]epending on the particular facts and circumstances," could "constitute money transmission," and thus subject such companies to regulation under the Bank Secrecy Act (BSA).

The FinCEN Advisory continues to identify "red flags" associated with ransomware activity. Financial institutions generally are expected to investigate such red flags in order to determine if there is a reasonable, non-suspicious explanation for the activity or whether, if not, the financial institution should report the activity to FinCEN in a suspicious activity report (SAR). With respect to ransomware payments, the FinCEN Advisory lists a number of red flags, including: (1) activity bearing certain technical indicators of a potential ransomware attack, which may be evident in system log files, network traffic, or file information; (2) any instance in which a customer indicates a payment is in response to a ransomware incident; (3) a customer transacts with CVC addresses that are linked in public or other reporting to ransomware activity; (4) any transaction between an organization and a DFIR or CIC – especially if the organization is in a sector at high-risk for ransomware attack (e.g., governmental, education, healthcare, financial); (5) the customer appears to be using the financial institution's liquidity to execute "large numbers of offsetting transactions between various CVCs, which may indicate that the customer is acting as an unregistered MSB"; (6) a customer "uses a CVC exchanger or foreign-located MSB in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for CVC entities"; and (7) a "customer initiates multiple rapid trades between multiple CVCs, especially AECs, 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."

Essentially, FinCEN's guidance suggests that any potential indication that a transaction is related to a ransomware payment or ransomware attack be treated as a red flag that a financial institution should investigate and determine whether a SAR is appropriate. FinCEN does not say that payments by victims automatically trigger an obligation to report, but strongly suggests that is the case, emphasizing that a financial institutions must file a SAR when it "knows, suspects, or has reason to suspect" that a transaction "involves the use of the financial institution to facilitate criminal activity," and that "[r]eportable activity can

involve transactions, including payments made by financial institutions, related to criminal activity like extortion and unauthorized electronic intrusions that damage, disable, or otherwise affect critical systems."

Finally, FinCEN provides specific instructions for filing SARs regarding ransomware activity. The advisory notes that "financial institutions should provide all pertinent available information on the event and associated with the suspicious activity, including cyber-related information [a term of art FinCEN has defined in past guidance on filing SARs] and technical indicators, in the SAR form and narrative." The advisory also identifies valuable information and indicators including: "relevant email addresses, Internet Protocol (IP) addresses with their respective timestamps, login information with location and timestamps, virtual currency wallet addresses, mobile device information (such as device International Mobile Equipment Identity (IMEI) numbers), malware hashes, malicious domains, and descriptions and timing of suspicious electronic communications."

FinCEN requests that financial institutions filing SARs related to potential ransomware activity reference the advisory by including "CYBER-FIN-2020-A006" in SAR field 2 and the narrative, select SAR field 42 (Cyber event) as the associated suspicious activity type, and select SAR field 42z (Cyber event - Other) and include the keyword "ransomware" in SAR field 42z, to indicate a connection between the suspicious activity being reported and possible ransomware activity. Financial institutions "should include any relevant technical cyber indicators related to the ransomware activity and associated transactions within the available structured cyber event indicator SAR fields 44(a)- (j), (z)."

Practical Considerations

Although OFAC says that timely reporting of a ransomware attack to law enforcement will be a substantial mitigating factor for enforcement "if the situation later is found to have a sanctions nexus," OFAC also confirms that there is a significant enforcement risk for anyone involved in a ransomware payment that goes to a sanctioned person or jurisdiction. Furthermore, OFAC suggests that it is not inclined to grant licenses that would allow ransom payments that involve sanctioned persons or jurisdictions. Accordingly, some companies may face difficult choices about whether to alert OFAC in situations where there is significant evidence that a sanctioned party is involved. Because OFAC has suggested that it will not license payments to such persons, alerting law enforcement or OFAC to a ransomware demand may give rise to situations where these agencies expect a victim company to refuse to pay the ransom, and the company will need to comply to avoid a sanctions violation while figuring out how to restore systems and manage potential data loss without making a payment. In the alternative, if it decides it must pay – despite the fact that paying ransomware demands does not necessarily result in system restoration and can leave lingering issues related to third-party access to the data and data loss – the company will have alerted OFAC to a potential violation, and must hope that its timely involvement of law enforcement will mitigate against any penalty.

Companies therefore may wish to develop a risk-based compliance plan or playbook that analyzes key decisions and factors that a company may face during a ransom attack. The same is true for financial institutions, DFIRs, and CICs that may find themselves in the position of facilitating ransomware payments or other related dealings. Such policies might address a company's approach to attribution, and in particular attribution of attacks to sanctioned persons or jurisdictions, and the different ways that sanctioned persons or jurisdictions might arise in ransomware situations, including internal analysis and the use of third-party vendors in this process. This includes potentially not only the attackers themselves, but also negotiators, virtual currency exchangers and other financial institutions, and other third-party intermediaries or facilitators.

Separately, financial institutions should consider incorporating the red flags FinCEN has identified for potential ransomware activity into their AML programs, and more broadly addressing how they will detect and deal with ransomware-related transactions. The obligation of Bank Secrecy Act-regulated financial institutions to detect and report suspicious activity extends beyond dealings with sanctioned parties to include all transactions over the relevant reporting threshold where there is reason to suspect that the transaction lacks a legitimate business purpose or is not the kind in which the customer normally would engage. FinCEN's advisory makes clear that financial institutions should ensure their transaction and suspicious activity monitoring is able to detect red flags associated with ransomware activity, as well as to investigate such red flags and make robust determinations on whether to file a SAR. The guidance suggests that any indication of ransomware activity should be treated as a red flag and any suspected ransomware activity that exceeds the relevant reporting threshold should be reported in a SAR. Financial institutions also should take steps to ensure that their AML compliance teams have access to any cyber-related information known to the financial institution that is associated with such incidents, and that they include such information in any SARs.

The FinCEN Advisory also provides a warning to entities such as DFIRs and CICs that FinCEN may treat them as money transmitters (a form of MSB and thus subject to regulation under the BSA) if they arrange or make ransomware-related payments on behalf of clients, and that the fact that these transactions are done as part of a broader client service may not exempt them from regulation.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Caroline E. Brown
Partner – Washington, D.C.
Phone: +1.202.624.2509
Email: cbrown@crowell.com

Carlton Greene
Partner – Washington, D.C.
Phone: +1.202.624.2818
Email: cgreene@crowell.com

David (Dj) Wolff
Partner; Attorney at Law – London, Washington, D.C.
Phone: +44.20.7413.1368, +1.202.624.2548
Email: djwolff@crowell.com

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1.202.624.2615
Email: ewolff@crowell.com