Schulte Roth&Zabel

Alert

Treasury Issues Advisories Related to Ransomware Attacks

December 1, 2020

On Oct. 1, 2020, the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") and Office of Foreign Assets Control ("OFAC") each issued advisories on ransomware that, when taken together, make it more difficult for victims of such attacks to lawfully pay ransoms to regain access to hijacked systems and recover stolen data. The FinCEN advisory ("FinCEN Advisory") discusses predominant trends, typologies and potential red flag indicators of ransomware and associated money laundering activities, and the related suspicious activity reporting requirements applicable to financial institutions. Importantly, it clarifies that institutions functioning as intermediaries between victims and cyber actors in the payment of ransoms, including digital forensics, incident response and cyber insurance companies, may be required to register with FinCEN as money services businesses ("MSBs"). The OFAC advisory ("OFAC Advisory," and, together with the FinCEN Advisory, the "Advisories") highlights the sanctions risks associated with paying, or facilitating payment of, ransoms to certain designated cybercriminals, and in so doing, leaves no doubt that ransomware payments from victims to cyber actors can violate OFAC regulations.

Background

The Advisories raise the familiar debate over "negotiating with terrorists." On one hand, paying ransoms makes ransomware attacks more lucrative for cyber criminals and emboldens cyber criminals to perpetrate further attacks. On the other, paying ransoms may be the only way for victims to end the ransomware attack. On Oct. 13, 2020, the G-7 member nations warned that perpetrators of ransomware attacks might be state-sponsored or linked actors who might use the ransom funds for further illicit purposes, such as funding weapons of mass destruction.[1] Regulations that impose prohibitions, or at least cause delays, on paying ransoms inhibit what can be an economically efficient way for victims to respond to attacks and minimize the damage to their business continuity.

According to the Advisories, the frequency of ransomware attacks has surged, as has the amount cybercriminals demand. The average ransom payment in December 2019 was $190,946, with several organizations reporting seven-figure payments.[2] Navigating a ransomware attack has become increasingly challenging and complex, as attackers deploy ever more sophisticated technologies and victims are often asked to pay ransoms in digital currency. The Advisories reinforce the importance of having plans in place to prevent and respond to ransomware attacks, in particular due to the heightened burden placed on victims, who often choose to pay ransoms to regain access to hijacked systems or

[1] "Econ Chiefs Urge Ransomware Victims To Report Payoffs," *Law360*, Oct. 13, 2020, available here.

[2] "Ransomware Attacks Grow, Crippling Cities and Businesses," *New York Times*, Feb. 9, 2020, available here. ("The average payment to release files spiked to $84,116 in the last quarter of 2019, more than double what it was the previous quarter, according to data from Coveware, another security firm. In the last month of 2019, that jumped to $190,946, with several organizations facing ransom demands in the millions of dollars.").

recover stolen data.[3] Victims of ransomware schemes should review the Advisories closely and assess carefully whether paying ransom would violate the law.

FinCEN Advisory Alerts to Common Trends, Typologies and Indicators of Ransomware Attacks

Financial institutions are often involved in the processing of ransomware payments — a multi-step process that may include at least one depository institution and one or more MSBs — given that ransom demand payments are usually requested to be paid in convertible virtual currency ("CVC"), such as Bitcoin ("BTC"). The ransomware victim will often need to exchange fiat currency held at a bank for CVC through a MSB that operates as a CVC exchange by purchasing from the MSB the type and amount of CVC that the cybercriminal demands.

Further, certain institutions, including digital forensics and incident response companies ("DFIRs"), and cyber insurance companies ("CICs"), might function as an intermediary by facilitating the conversion of payments to CVC and paying the ransom demanded by a cybercriminal. Entities engaged in such transactions might be required to register as MSBs with FinCEN, subjecting them to certain Bank Secrecy Act obligations, including the obligation to file a suspicious activity report ("SAR").

Additionally, FinCEN warns the public and financial institutions of the increasingly complex and sophisticated schemes of ransomware attacks. Cybercriminals often use common tactics, including phishing schemes, to infiltrate a victim's systems. Employee training and institutional preparedness in the case of a cyber-attack is the best protection from a ransom scheme. FinCEN identifies the following types of schemes:

- *Big Game Hunting Schemes*. Selective targeting of larger enterprises to demand bigger payouts.
- *Ransomware Criminals Forming Partnerships and Sharing Resources*. Sharing resources to enhance the effectiveness of ransomware attacks, such as ransomware exploit kits that come with ready-made malicious codes and tools (which are offered for purchase or free) and forming partnerships to share advice, code, trends, techniques and illegally obtained information over shared platforms.
- "*Double Extortion" Schemes*. Removing sensitive data from the targeted networks, encrypting the system files and demanding ransom. The criminals then threaten to publish or sell the stolen data if the victim fails to pay the ransom.
- *Use of Anonymity-Enhanced Cryptocurrencies ("AECs")*. Requiring ransomware payments to be denominated in CVC such as BTC, or in AECs that reduce the transparency of CVC payment flows through anonymizing features, such as mixing and cryptographic enhancements. Some ransomware operators have even offered discounted rates to victims who pay their ransoms in AECs.[4]

[3] Our Aug. 17, 2020 *Alert* provides further information on the increasing risk of ransomware attacks, including steps that fund managers and financial institutions can take to increase preparedness for a cyber-attack.

[4] The Attorney General's Cyber Digital Task Force recently released a guide to cryptocurrency enforcement issues broadly. The guide warns that bad actors may exploit cryptocurrency to (1) engage in financial transactions associated with the commission of crimes, such as buying and selling drugs or weapons on the dark web, leasing servers to commit cybercrimes or soliciting funds to support terrorist activity; (2) engage in money laundering or shield otherwise legitimate activity from tax, reporting or other legal requirements; or (3) commit crimes directly implicating the cryptocurrency marketplace itself, such as stealing cryptocurrency from exchanges through hacking or using the promise of

- *Use of "Fileless" Ransomware*. Sophisticated tool that can be challenging to detect because the malicious code is written into the computer's memory rather than into a file on a hard drive, which allows attackers to circumvent off-the-shelf antivirus and malware defenses.[5]

Additionally, FinCEN warns that institutions should be alert for the following "red flags" which may indicate a ransomware-related scheme:

1. 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.
2. 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.
3. A customer's 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.
4. 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 DFIR or CIC, especially one known to facilitate ransomware payments.
5. A DFIR or CIC customer receives funds from a customer company and shortly after receipt of funds sends equivalent amounts to a CVC exchange.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.[6]

cryptocurrency to defraud unwitting investors. *See* U.S. Department of Justice, Cryptocurrency Enforcement Framework, Report of the Attorney General's Cyber Digital Task Force (October 2020), available here.

[5] Fin. Crimes Enf't Network, Dept. of Treasury, Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments (2020), available here.

[6] *Id.*

The FinCEN Advisory reminds each financial institution that it might be required to file a SAR "when dealing with an incident of ransomware conducted by, at, or through the financial institution"[7] and that such SAR must incorporate all relevant information, which might include "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."[8] FinCEN requests that financial institutions reference the Advisory on the SAR by including the key term "CYBER-FIN-2020-A006" in the SAR notes field and narrative section. In addition, financial institutions should select the suspicious activity type "cyber-event" in SAR field 42 and note the term "ransomware" in SAR field 42z.

The FinCEN Advisory also clarifies that information sharing among financial institutions pursuant to section 314(b) of the USA PATRIOT Act may be permissible for information related to ransomware, as the specified unlawful activities listed in 18 U.S.C. §§ 1956 and 1957 include an array of fraudulent and other criminal activities, including extortion and computer fraud and abuse.

OFAC Advisory Warns of Sanctions Violations for Direct Payments and Facilitation of Payments to Cybercriminals

OFAC has designated, and will continue to designate, malicious cyber actors under its cyber-related sanctions programs and other sanctions programs, and others "who materially assist, sponsor, or provide financial, material, or technological support for these activities."[9] The OFAC Advisory provides several notable examples of ransomware and ransomware variants, such as Cryptolocker, SamSam and WannaCry 2.0, and points out the designated individuals and entities involved in such ransomware. OFAC warns that payments to such malicious actors can be used to "fund activities adverse to national security and foreign policy objectives."

The OFAC Advisory makes clear that OFAC will impose sanctions on U.S. persons who engage in transactions with individuals and entities involved in ransomware that have been designated by OFAC and appear on OFAC's Specifically Designated Nationals and Blocked Persons List ("SDN"), and those covered by country or region sanctions. Additionally, OFAC cautions that a U.S. person need not know that the recipient of payment has been designated, stating that civil penalties may be imposed 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 administered by OFAC."[10] This poses a significant risk when paying a ransom, as cybercriminals often disguise their identities when demanding payment, making it nearly impossible to determine whether a recipient is prohibited.

The OFAC Advisory reminds us that under its Economic Sanctions Enforcement Guidelines, OFAC provides information regarding the factors it considers when determining responses to violations.[11]

---

[7] *Id.*

[8] *Id.*

[9] Office of Foreign Assets Control, Dept. of Treasury, Advisory on Potential Sanctions Risk for Facilitating Ransomware Payments (2020), available here.

[10] *Id.*

[11] Our July 12, 2019 *Alert* provides additional information on OFAC's guidance titled "A Framework for OFAC Compliance Commitments."

Financial institutions should implement a risk-based compliance program that contemplates the potential for a ransomware payment to an SDN, as OFAC will consider this in its enforcement analysis. Additionally, an entity's incident response and timely, self-initiated report of a ransomware attack to law enforcement might be considered when determining the appropriate sanctions.

Notably, OFAC deters any questions on obtaining specific licenses by stating that: "license applications involving ransomware payments demanded as a result of malicious cyber-enabled activities will be reviewed by OFAC on a case-by-case basis with a presumption of denial."[12]

The OFAC Advisory also encourages victims of ransomware attacks to contact OFAC, as well as certain government agencies, in the event of an attack, and provides contact information for those government authorities, including OFAC, the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection, the Federal Bureau of Investigation Cyber Task Force and the Cybersecurity and Infrastructure Security Agency. OFAC also recommends that victims of ransomware attacks consider whether they have additional regulatory obligations under FinCEN's regulation.

Conclusion

The Advisories make clear that victims of ransomware attacks must reconsider making payments to cybercriminals, as doing so may mean that in some cases cyber victims may become the subject of a SAR filed with FinCEN or could be fined or prosecuted for paying ransoms. With the increased enforcement of sanctions for ransom payments, victims of ransomware attacks can no longer determine that the cost of paying a cybercriminal outweighs the risk of disruption to business without determining first whether the cybercriminal constitutes a prohibited counterparty and whether there are downstream consequences for payment of such ransom. Therefore, companies in the financial services sector must be ever more vigilant in identifying cybercrime attempts and preparing for the event of a cyberattack.

Authored by Edward H. Sadtler, Betty Santangelo, Melissa G.R. Goldstein, Kelly Koscuiszka and Jaclyn N. Malmed.

If you have any questions concerning this *Alert*, please contact your attorney at Schulte Roth & Zabel or one of the authors.

Schulte Roth & Zabel
New York | Washington DC | London
www.srz.com

[12] *Id.*