SULLIVAN & CROMWELL LLP

October 2, 2020

Treasury Department Issues Advisories on Ransomware Attacks

FinCEN and OFAC Advisories Highlight Risks Associated With Ransomware Payments as Well as "Red Flags" and Reporting Requirements for Ransomware Attacks

SUMMARY

On October 1, 2020, the United States Department of the Treasury's Office of Terrorism and Financial Intelligence issued, through Treasury's Financial Crimes Enforcement Network ("FinCEN") and Treasury's Office of Foreign Assets Control ("OFAC"), two advisories focused on the implications of payments made or facilitated by financial institutions and other entities in response to ransomware attacks. The advisory issued by FinCEN, entitled *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*, discusses the role played by financial intermediaries in ransomware payments, discusses trends and typologies of ransomware and associated payments, identifies ransomware-related "financial red flags," and provides instructions on the reporting and sharing of information related to ransomware attacks. The advisory issued by OFAC, entitled *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, outlines the sanctions risks of facilitating ransomware payments, and highlights the threat that ransomware poses to U.S. national security interests. Both the FinCEN and OFAC advisories warn that payment of ransomware demands may promote future attacks, and encourage financial institutions and other companies that facilitate ransomware payments to share information and to cooperate fully with law enforcement during and after ransomware attacks.

BACKGROUND

Ransomware is a form of malicious software, known as "malware," designed to block access to, and often encrypt, computer systems or data belonging to third parties. Once the victim's computer system or data is locked down and encrypted, rendering it essentially useless, the malicious cyber actor then extorts the

victim by demanding a ransom payment in exchange for providing a method to decrypt it. The attacker may also copy the victim's data in the course of the attack and threaten to sell or publish the data if the ransom is not paid. Ransomware attacks can result in a loss of business functionality and of sensitive data.

The financial sector plays a crucial role in the collection and payment of ransomware demands by malicious cyber actors. Malicious cyber actors often demand payment in convertible virtual currency, or "CVC." Bitcoin is the most common CVC, but ransom demands in other CVCs with anonymizing features, such as anonymity-enhanced cryptocurrencies ("AECs"), have grown in frequency. To meet the ransom demand, victims need to obtain CVC in the type and amount demanded, typically by transmitting funds via wire transfer, automated clearing house, credit card payment, or other means involving the financial sector. After the victim makes the demanded CVC payment, the malicious cyber actor often seeks to launder the funds to obscure their source and the actor's identity.

The complexity and prevalence of ransomware attacks have led to the development of specialized companies that provide services for ransomware victims, such as obtaining and paying CVC. These include digital forensic and incident response companies ("DFIRs") and cyber insurance companies ("CICs"). These companies may conduct activity constituting money transmission, which requires registration with FinCEN as a money service business ("MSB") subject to Bank Secrecy Act obligations, including the filing of suspicious activity reports ("SARs"). Ransomware payments may also implicate OFAC-administered sanctions.

FINCEN ADVISORY

The October 1 FinCEN advisory is intended to assist financial institutions in detecting, preventing, and reporting ransomware-related illicit activity.[1] The FinCEN advisory emphasizes that the detection and reporting of ransomware payments assists in prevention and deterrence of cyber actors from deploying malicious software, and helps hold ransomware attackers accountable.

To assist with detection, the FinCEN advisory identifies trends and typologies of ransomware and associated payments and provides 10 financial red flags that evidence potential ransomware-related payments.[2] While no single red flag is determinative of ransomware activity, each should be considered in the context of the facts and circumstances of a transaction. These financial red flags are:

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, [anti-money laundering and countering financing of terrorism] 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.

To assist in reporting ransomware attacks, FinCEN "strongly encourages" information sharing among financial institutions pursuant to section 314(b) of the USA PATRIOT Act where a transaction is suspected of involving terrorist financing or money laundering, and urges financial institutions to file SARs as a means of protecting the U.S. financial system from ransomware threats. The FinCEN advisory includes a reminder that SARs may be required or appropriate when ransomware payments, whether attempted or successful, are conducted "*by, at, or through*" a financial institution, with specific instructions to indicate a connection with ransomware-related activity.[3] The advisory includes a footnote that FinCEN "assesses that ransomware-related activity is under-reported." It reminds financial institutions that they are required to incorporate "all relevant information available" in a SAR, including cyber-related information and technical indicators which can be valuable for law enforcement investigations for ransomware. These indicators 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."[4]

OFAC ADVISORY

The October 1 OFAC advisory highlights the sanctions risks posed by ransomware payments and the associated risks to U.S. national security interests.[5] The International Emergency Economic Powers Act ("IEEPA") and the Trading with the Enemy Act ("TWEA")[6] generally prohibit U.S. persons from engaging in transactions with persons on OFAC's Specially Designated Nationals and Blocked Persons List ("SDN List"), other blocked persons, and persons covered by comprehensive country or region embargoes.

OFAC's cyber-related sanctions program and other sanctions programs have been used to designate numerous malicious cyber actors, including perpetrators of ransomware attacks. These include nation-state actors that have a nexus to U.S. sanctions, such as Russia, Iran, and North Korea. U.S. persons, including financial institutions, that facilitate payment of ransomware demands to these sanctioned cyber actors are in violation of U.S. sanctions and may be subject to OFAC enforcement action.

Non-U.S. persons facilitating such payments through the U.S. financial system may also be exposed to OFAC enforcement action, as U.S. sanctions laws further prohibit transactions by a non-U.S. person that cause a U.S. person to violate IEEPA-based sanctions. The OFAC advisory also makes clear that it is not only financial institutions that should exercise caution, as the sanctions laws extend to "companies that engage with victims of ransomware attacks, such as those involved in providing cyber insurance, digital forensics and incident response, and financial services that may involve processing ransom payments (including depository institutions and money services businesses)."[7] Such companies should be mindful of the risks that a ransomware payment may involve an SDN or blocked person, or a comprehensively embargoed jurisdiction.[8]

Given the threats that ransomware may inflict on U.S. national security interests, the OFAC advisory encourages financial institutions and companies that engage with victims of ransomware attacks to adopt risk-based sanctions compliance programs that account for the risk that a ransomware payment may involve an SDN or blocked person, or a comprehensively embargoed jurisdiction. In addition, the OFAC advisory encourages victims and those involved with addressing ransomware attacks to contact OFAC immediately if a ransomware payment is believed to involve a sanctions nexus. Though the advisory states that license applications seeking authorization to pay ransomware demands will be subject to a presumption of denial, it also indicates that, in evaluating a potential enforcement response in a case involving ransomware, OFAC will treat notification to, and cooperation with, law enforcement as "significant mitigating factors" under its Enforcement Guidelines. As such, the advisory encourages companies to provide law enforcement with a "self-initiated, timely, and complete report of a ransomware attack" and to cooperate fully and timely with law enforcement during and after a ransomware attack.[9]

IMPLICATIONS

By outlining risks to financial institutions when processing ransomware payment requests, the FinCEN and OFAC advisories offer guidance to financial institutions formulating policies and procedures for deciding whether to process or report payment requests that may be related to ransomware. The advisories suggest that additional scrutiny will be applied to ransomware-related payments given the growing national security concerns associated with ransomware attacks, which include potential sanctions violations. The advisories add complexity to the analysis for victims of ransomware and those facilitating ransomware payments regarding whether to pay a ransom. Financial institutions and other payment intermediaries should formulate policies and procedures for processing ransomware payments based on their own individual

assessment of the potential legal and reputational risks involved. In addition, they should evaluate carefully the facts and circumstances, including a review for potential "financial red flags," in connection with payment requests that may be connected with ransomware attacks. Finally, financial institutions and MSBs should ensure they have appropriate reporting mechanisms in place to ensure that ransomware attacks and payments are the subject of timely filed SARs, as appropriate.

* * *

ENDNOTES

1 FinCEN Advisory, FIN-2020-A006, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments" (Oct. 1, 2020), *available at* https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2020-a006.

2 *Id.* at 5–6.

3 *Id.* at 6; *id.* at 8 (requesting that financial institutions indicate a connection between the reported suspicious activity and ransomware-related activity by including the term "CYBER FIN-2020-A006" in SAR field 2, selecting SAR field 42 (Cyber Event), and selecting and including as a keyword "ransomware" in SAR field 42z (Cyber Event - Other)).

4 *Id.* at 7.

5 OFAC Advisory, "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" (Oct. 1, 2020), *available at* https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201001.

6 50 U.S.C. §§ 4301–41; 50 U.S.C. §§ 1701–06.

7 OFAC Advisory at 3–4.

8 *Id.* at 4.

9 *Id.*

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.

CONTACTS

New York		
H. Rodgin Cohen	+1-212-558-3534	cohenhr@sullcrom.com
Elizabeth T. Davy	+1-212-558-7257	davye@sullcrom.com
Mitchell S. Eitel	+1-212-558-4960	eitelm@sullcrom.com
John Evangelakos	+1-212-558-4260	evangelakosj@sullcrom.com
Nicole Friedlander	+1-212-558-4332	friedlandern@sullcrom.com
Shari D. Leventhal	+1-212-558-4354	leventhals@sullcrom.com
Sharon Cohen Levin	+1-212-558-4334	levinsc@sullcrom.com
Nader A. Mousavi	+1-212-558-1624	mousavin@sullcrom.com
Sharon L. Nelles	+1-212-558-4976	nelless@sullcrom.com
Washington, D.C.		
James A. Earl	+1-202-956-7566	earlja@sullcrom.com
Eric J. Kadel, Jr.	+1-202-956-7640	kadelej@sullcrom.com
Stephen H. Meyer	+1-202-956-7605	meyerst@sullcrom.com
Kamil R. Shields	+1-202-956-7040	shieldska@sullcrom.com
Jennifer L. Sutton	+1-202-956-7060	suttonj@sullcrom.com
Adam J. Szubin	+1-202-956-7528	szubina@sullcrom.com
Andrea R. Tokheim	+1-202-956-7015	tokheima@sullcrom.com
Los Angeles		
Anthony J. Lewis	+1-310-712-6615	lewisan@sullcrom.com
Palo Alto		
Nader A. Mousavi	+1-650-461-5660	mousavin@sullcrom.com