SAUL EWING ARNSTEIN & LEHR LLP

ALERT

Cybersecurity and Privacy Practice

White Collar and Government Enforcement Practice

NOVEMBER 2021

# Revised FinCEN Advisory Warns Financial Institutions to Report Suspected Illegal Ransomware[1] Payments

Franklin Zemel | Joseph Valenti | Erik VanderWeyden

The U.S. Federal Government through its Financial Crimes Enforcement Network ("FinCEN") revised last year's Advisory on the Use of the Financial System to Facilitate Ransom Payments. In short, the U.S. Government is underscoring the importance of due-diligence and compliance obligations required by the U.S. Department of Treasury's Office of Foreign Assets Control ("OFAC").[2]

**What You Need to Know:**

- In response to increased frequency and severity of ransomware attacks, FinCEN has updated and replaced its October 1, 2020 Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments.
- The Revised Advisory provides financial institutions with a list of identified trends and typologies as well as a list of red flags that may indicate ransomware and associated payments.

The latest Advisory requires that financial institutions must comply with currency-transaction and suspicious-activity reporting requirements and continually update their compliance programs to establish procedures in advance for determining and assessing ransomware threats as well as prevent the laundering of ransomware proceeds to avoid criminal and civil penalties under the laws administered by DOJ, FinCEN, and OFAC.

***FinCEN Urges Financial Institutions to Revise Compliance Programs to Account for Recent Trends in Ransomware Attacks***

In response to increased frequency and severity of ransomware attacks, FinCEN has updated and replaced its October 1, 2020 Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments. As noted in the Advisory, all entities (including victims) involved in the chain of facilitating ransomware payments are at risk of criminal and civil penalties. Accordingly, appropriate due-diligence and compliance procedures are necessary to limit exposure to ransomware and sanctions-related violations. Failure to implement a risk-based compliance program—or a failure to ensure that it is up to date—may result in increased exposure to ransomware and harsher penalties.

The Revised Advisory provides financial institutions with a list of identified trends and typologies as well as a list of red flags that may indicate ransomware and associated payments, some of which include:

- A financial institution or its customer detects IT enterprise activity that is connected to ransomware cyber indicators or known cyber threat actors.
- A customer provides information that a payment is in response to a ransomware incident.

[1] As noted in the Revised Advisory, "[r]ansomware is a form of malicious software ('malware') designed to block access to a computer system or data, often by encrypting data or programs on information technology (IT) systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to systems or data. In some cases, in addition to the encrypting information, the perpetrators threaten to publish sensitive files belonging to the victims, which can be individuals or business entities (including financial institutions). See FIN-2021-A004

[2] *Id.*

- A customer's convertible virtual currency ("CVC") address, or an address with which a customer conducts transactions, is connected to ransomware variants, payments, or related activity.
- An irregular transaction occurs between a high-risk organization and a Digital Forensic/Incident Response or Cyber Insurance Company, especially one known to facilitate ransomware payments.
- A customer shows limited knowledge of CVC during onboarding or via other interactions with the financial institution, yet inquires about or purchases CVC.
- A customer that has no or limited history of CVC transactions sends a large CVC transaction, particularly when outside a company's normal business practices.

The Advisory notes that it is imperative that financial institutions review their current compliance programs to ensure they are up-to-date to reflect these red-flag indicators as well as the recent trends and typologies of ransomware and associated payments. The Advisory specifically warns of one notable trend - the growing proliferation of anonymity-enhanced cryptocurrencies ("AECs") and decentralized mixers utilized to obfuscate the trail of virtual currencies. It warns that one such AEC, Monero, is increasingly demanded by ransomware criminals.

***Reporting Requirements for Financial Institutions***

The Advisory reminds financial institutions of their regulatory obligations regarding suspicious activity reporting involving ransomware. If a financial institution detects a suspicious transaction, it is required "to file a Suspicious Activity Report ("SAR") if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at or through the financial institution involves or aggregates to $5,000 (or, with one exception, $2,000 for [money services businesses](MSB)." SAR obligations apply to both attempted and successful transactions, and FinCEN recommends filing a SAR even when there is no obligation to file.

Entities that facilitate ransomware payments to cybercriminals, such as some Digital Forensic/Incident Response companies and Cyber Insurance Companies, depending on the particular facts and circumstances, could constitute money transmission (which is considered MSB activity). Entities engaged in MSB activities are required to register as an MSB with FinCEN, and are subject to the Bank Secrecy Act obligations, including filing SARs. The Advisory also notes, "FinCEN will not hesitate to take action against entities and individuals engaged in money transmission or other MSB activities if they fail to register with FinCEN or comply with their other [anti-money laundering] obligations."

***Potential Sanctions Risks for Facilitating Ransomware Payments***

Several of the most destructive ransomware operators are presently sanctioned by OFAC. OFAC updates its sanctions frequently, particularly when new cyber threats emerge from China, Iran, North Korea, Russia, other countries, or organized non-state actors. Because the identity of perpetrators of ransomware attacks are usually not known or identifiable, OFAC is concerned that ransom payments are funneling into the coffers of entities and jurisdictions on their sanctions list, to be used against U.S. interests, and to fund further attacks.

Persons involved in ransomware payments must be aware of any OFAC-related obligations that may arise from that activity. "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 such person did not know or have reason to know that it was engaging in a transaction that was prohibited under sanctions laws and regulations administered by OFAC."[3] When an entity makes or facilitates a ransomware payment to a sanctioned entity, the violation is complete. Mental state, knowledge, duress, and other typical elements or affirmative defenses are not legally available.

OFAC will consider a company's self-initiated, timely, and complete report of a ransomware attack to law enforcement and its cooperation with law enforcement during and after a ransomware attack to be a "significant mitigating factor" in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus.

[3] See Department of the Treasury: Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments

Financial institutions can seek a license (in essence, pre-payment permission) to perform the requested financial transaction. Even taking the effort to verbally notify OFAC or complete its online form before making a time-sensitive payment demonstrates an effort to recognize the balance between national security and vital economic/operational interests (and, in some cases—like medical centers—lifesaving data restoration).

There are potential changes in reporting requirements on the horizon. On November 10, the Ransomware and Financial Stability Act was introduced in the U.S. House of Representatives, which would require financial institutions to receive special authorization from the Treasury prior to making ransomware payments greater than $100,000.[4]

***Conclusion***

The Revised Advisory stresses the importance of financial institutions not only having their own appropriate compliance program that, among other things, establishes a procedure in advance for determining and assessing the risks of ransomware attacks, but also puts the onus on the financial institution to continually evolve its compliance program to cover current red-flag indicators, trends, and typologies in ransomware and associated payments.

Consultation with well-trained lawyers and cybersecurity consultants ahead of any ransomware attacks are typically prudent measures that can dramatically reduce both the risks of attacks and the costs of responding to attacks. The Advisory also encourages early, full consultation with law enforcement, OFAC, and FinCEN.

Saul Ewing Arnstein & Lehr's lawyers are available to assist with any questions you may have regarding issues raised in this Alert. It is important to consult with a cyber lawyer before an attack and with white collar lawyer during or after. For further information, please contact the authors of this Alert, the Saul Ewing Arnstein & Lehr lawyer with whom you usually work, or the Co-Chairs of the Firm's Cybersecurity and Privacy Practice, Alexander (Sandy) R. Bilus or Evan J. Foster; or Co-Chairs of the Firm's White Collar and Government Enforcement Practice, Jennifer L. Beidel or Nancy DePodesta.

---

[4] See Press Release from House Republicans Financial Services

**This alert was written by Franklin Zemel and Erik VanderWeyden, both members in the Firm's Cybersecurity and Privacy Practice; and Joseph A. Valenti, a member of the Firm's White Collar and Government Enforcement Practice. Franklin can be reached at franklin.zemel@saul.com or (954) 713-7610. Erik can be reached at ej.vander@saul.com or (312) 876-7113. Joseph can be reached at joe.valenti@saul.com or (412) 209-2569. This alert has been prepared for information purposes only.**

**Did you find this information useful? Please provide your feedback here and also let us know if there are other legal topics of interest to you.**