Davis Polk

FinCEN updates its ransomware advisory for financial institutions

November 12, 2021 | Client Update | 7-minute read

Updated in response to an increase in ransomware attacks against critical infrastructure, the revised advisory identifies new trends, typologies and indicators of ransomware payments and associated money laundering activities and highlights reporting and notification requirements for ransom payments.

The Financial Crimes Enforcement Network (FinCEN) updated and replaced its Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments (the Advisory) on November 8, 2021.[1] The Advisory, which expands on a previous version issued last year, provides information on: (1) the role of financial intermediaries in the processing of ransomware payments; (2) trends and typologies of ransomware and associated payments; (3) ransomware-related financial red-flag indicators; and (4) reporting and sharing information related to ransomware attacks. Because ransom payments are often processed and laundered through the financial system, FinCEN expects financial institutions, including entities dealing in convertible virtual currency (CVC), to detect and report ransomware activities. The Advisory notes that FinCEN has now designated ransomware attacks as "situations involving violations that require immediate attention," which imposes heightened reporting requirements on financial institutions. Accordingly, financial institutions that suspect a ransomware transaction has taken or is taking place must *immediately* contact FinCEN's Financial Institution Hotline or otherwise notify an appropriate law enforcement authority, in addition to the requirement that they subsequently file a suspicious activity report (SAR).

FinCEN updated the Advisory in response to a number of ransomware attacks on U.S. companies and critical infrastructure throughout 2021, including a ransomware attack on the operator of the largest fuel pipeline in the United States that led to widespread fuel shortages across the nation. The updated Advisory reflects FinCEN's most recent Financial Trend Analysis Report on ransomware, which found that "most ransomware attacks" involved demands for payment in CVC. Accordingly, much of this update addresses red-flag indicators and regulatory expectations concerning CVC.

Role of financial intermediaries in processing ransomware payments

The Advisory clarifies that entities that facilitate ransomware payments to cybercriminals may be required to register with FinCEN because, depending on the facts and circumstances, those activities could qualify as money transmission.[2] This interpretation could bring a variety of actors in the virtual asset sector within the scope of the Bank Secrecy Act's anti-money laundering and reporting requirements. The Advisory notes that most ransomware schemes involve CVC, which, according to FinCEN, is "the preferred payment method of ransomware perpetrators." As a result, entities such as CVC exchanges, cyber insurance companies (CICs) and digital forensic and incident response (DFIR) companies often play a role in handling ransomware payments. For example, after receiving a ransom demand, a ransomware victim usually transmits funds to a CVC exchange to purchase and send the type and amount of CVC specified by the ransomware attacker. CICs, meanwhile, issue policies designed to mitigate losses resulting from ransomware payments, data breaches, and network damage. Finally, DFIR companies often negotiate with cybercriminals, facilitate payments and investigate the source of cybersecurity breaches. Accordingly, financial institutions and entities providing these services should ensure that their operations comply with the Bank Secrecy Act and its implementing regulations. The Advisory

states that FinCEN will "not hesitate to take action" against entities engaged in money transmission and similar activities if they fail to register with FinCEN or comply with their respective anti-money laundering obligations.

Trends and typologies of ransomware and associated payments

The Advisory provides useful insight into recent trends and typologies of ransomware:

1. Extortion schemes: Ransomware attackers are increasingly engaging in "double extortion schemes" that involve removing and encrypting data from the victim's targeted networks and demanding a ransom for the data.
2. Anonymity-enhanced cryptocurrencies (AECs) and mixing services: Recently, ransomware attackers have started requiring or incentivizing their victims to pay ransoms in AECs such as Monero and subsequently reducing the transparency of the ransom transactions through anonymizing services such as "mixing" and "tumbling."[3]
3. Foreign CVC exchanges: Cybercriminals are increasingly cashing out ransoms using the services of foreign CVC exchanges located in jurisdictions that have limited regulatory oversight. According to the Advisory, "[t]hese exchanges often operate in high-risk jurisdictions or in jurisdictions that do not maintain effective information sharing agreements with other countries."
4. Ransomware partnerships and shared resources: Cybercriminals are continuing to engage in profit sharing via "ransomware-as-a-service" platforms, through which ransomware developers sell and support malware to allow a broader network of cybercriminals to monetize access to infected networks. The Advisory notes that the result has been higher ransom payments and more frequent, coordinated attacks on computer networks.
5. "Fileless" ransomware: Cybercriminals are expanding their use of fileless ransomware, which embed malicious code directly in a computer's memory instead of a specific file on a hard drive. This approach is challenging to detect and allows cybercriminals to circumvent widely used commercial antivirus and malware defenses.
6. Targeting large enterprises: Ransomware attackers are increasingly targeting large entities, particularly those with weaker security controls and a higher propensity to pay ransoms, to demand larger ransom payments.

Indicators of ransomware and associated payments

FinCEN identified a number of red-flag indicators of ransomware-related activity to help financial institutions detect, prevent and report suspicious transactions associated with ransomware attacks. Because there is no single red flag that definitively identifies suspicious activity, the Advisory recommends that financial institutions consider the relevant facts and circumstances of each transaction in accordance with their respective risk-based approaches to compliance. The red-flag indicators include:

1. When opening a new account, a customer provides information that a payment is in response to a ransomware attack.
2. A customer's CVC wallet address is connected to ransomware variants, payments or related activity.[4]
3. An irregular transaction occurs between an organization, particularly an organization in a high-risk sector for ransomware attacks, and a DFIR or CIC.
4. A DFIR or CIC customer receives funds from a counterparty and shortly thereafter sends equivalent amounts to a CVC exchange.
5. A customer has limited knowledge of CVC during onboarding but inquires about or purchases large amounts of CVC.
6. A customer that has no or limited history of CVC transactions sends a large CVC transaction that can be characterized as outside the customer's normal business practices.
7. A customer initiates a transfer of funds using a mixing service.
8. A customer uses a foreign CVC exchanger in a high-risk jurisdiction.
9. A customer uses an encrypted network or an unidentified web portal to communicate with the recipient of the CVC transaction.
10. A customer receives CVC from an external wallet and immediately initiates multiple, rapid trades among multiple CVCs, especially AECs, with no apparent related purpose, followed by a transaction off the platform.

Guidance for reporting suspected ransomware transactions

When a financial institution suspects that a ransomware-related transaction is conducted by, at, or through the institution, it should determine whether a SAR filing is mandatory or appropriate.[5] Because ransomware attacks are classified as "situations involving violations that require immediate attention," financial institutions must immediately report suspected ransomware transactions to FinCEN's Financial Institutions Hotline and file a SAR as soon as reasonably practicable thereafter. When a financial institution files a SAR connected to cyber incidents such as ransomware, FinCEN advises the financial institution to provide information such as the relevant email and Internet Protocol addresses (including timestamps and location information); identifying information relating to mobile devices; login information with location and timestamps; CVC wallet addresses; malware hashes; malicious domains; and descriptions and timing of suspicious electronic communication. The SAR should indicate that the suspicious activity being reported is connected to ransomware-related activity. Like the recent advisory on Sanctions Compliance for the Virtual Currency Industry from the Office of Foreign Assets Control (OFAC), FinCEN's update signals that the agency expects the virtual assets industry, including any financial intermediaries, to play a significant role in detecting and reporting financial crime.[6]

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Robert A. Cohen
+1 202 962 7047
robert.cohen@davispolk.com

Kendall Howell
+1 202 962 7068
kendall.howell@davispolk.com

Paul Marquardt
+1 202 962 7156
paul.marquardt@davispolk.com

John B. Reynolds III
+1 202 962 7143
john.reynolds@davispolk.com

Will Schisa
+1 202 962 7129
will.schisa@davispolk.com

Daniel P. Stipano
+1 202 962 7012
dan.stipano@davispolk.com

Zachary J. Zweihorn
+1 202 962 7136
zachary.zweihorn@davispolk.com

1 FinCEN released its original advisory in October 2020.

2 Under the Bank Secrecy Act and its implementing regulations, entities that engage in "money transmission" qualify as money services businesses (MSBs) and are required to register with FinCEN and implement an anti-money laundering program. *See* 31 C.F.R. 1010.100(ff) and 31 C.F.R. 1022.380.

3 Mixers and tumblers obfuscate the connection between the sender and the receiver of CVC transactions by commingling CVC belonging to other mixer users and splitting the value into smaller pieces that pass through an intermediary account.

4 Ransomware attackers use different versions of ransomware, which are commonly referred to as "variants." FinCEN identified 68 ransomware variants reported in SAR data for transactions reviewed for the October 2021 Financial Trend Analysis.

5 SAR filing is mandatory when, among other things, a financial institution knows, suspects, or has reason to suspect that a transaction aggregating to $5,000 or more (or $2,000 for MSBs) may involve potential money laundering or illegal activity, is designed to evade regulations promulgated under the Bank Secrecy Act, or has no apparent lawful purpose and is not the type of activity in which the customer would typically be expected to engage.

6 Please see our recent Client Update on OFAC's advisory on Sanctions Compliance for the Virtual Currency Industry.