November 11, 2021

FinCEN Updates Ransomware Advisory

Updated Guidance Emphasizes Timely Reporting, Virtual Currencies, and Whole-of-Government Approach to Enforcement

SUMMARY

On November 8, 2021, the United States Department of the Treasury Financial Crimes Enforcement Network ("FinCEN") issued an updated version of its *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments,* originally issued in the fall of 2020. Coming as part of a strengthened and more unified federal government focus on the ransomware threat, the Updated Advisory provides additional guidance to regulated institutions on how to detect potential ransomware payments and augments FinCEN's call for institutions to report suspected ransomware transactions promptly. FinCEN released the Updated Advisory contemporaneously with a joint enforcement action against a ransomware group and shortly after the United States Department of Treasury's Office of Foreign Assets Control ("OFAC") released new guidance concerning convertible virtual currencies ("CVCs") and sanctions.

BACKGROUND

On October 1, 2020, FinCEN and OFAC published advisories regarding ransomware and the implications of payments made or facilitated by financial institutions and other entities in response to ransomware attacks (the "October 2020 Advisories"). On September 23, 2021, OFAC updated its own ransomware advisory (the "September 2021 OFAC Update"). The advisories addressed red flags, reporting requirements, and potential sanctions risks involved in making payments in response to ransomware attacks. Among other things, FinCEN and OFAC highlighted ongoing ransomware trends and typologies and the risk that a victim might only discover after the fact that a ransomware payment involved a sanctioned actor or jurisdiction and thus constituted a potential violation of U.S. sanctions.

FINCEN ADVISORY

FinCEN's Updated Advisory emphasizes the recent "increase of ransomware attacks . . . against critical U.S. infrastructure," and identifies new trends in ransomware attacks and associated payments, including the increased use of anonymity-enhanced cryptocurrencies,[1] which were first mentioned in the October 2020 Advisories.[2] The Updated Advisory also makes explicit reference to the Department of Justice and its work to counter ransomware attacks through the Attorney General's Cyber-Digital Task Force.[3]

The Updated Advisory largely builds on the October 2020 Advisories, including warning Digital Forensics and Incident Response ("DFIR") companies and cyber insurance companies ("CICs") as to the risk that they will facilitate ransomware payments in violation of their obligations under the Bank Secrecy Act ("BSA"). The advisory adds that "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 AML obligations."[4] As detailed below, it also adds two new red flags concerning ransomware and associated payments, and a new warning that transactions that are suspected of being associated with ransomware attacks must be reported to law enforcement promptly along with the filing of a Suspicious Activity Report using the BSA E-filing System.[5]

A. CONVERTIBLE VIRTUAL CURRENCIES AND MONEY LAUNDERING

1. Unregistered CVC Mixing Services

According to the advisory, "cybercriminals often use mixers to obfuscate their illicit activities," in particular in connection with receiving payment of a ransom during a ransomware attack.[6] Mixers, or "Unregistered CVC Mixing Services," are described as services that commingle CVCs from multiple users and pass the value of the CVCs out of the service through smaller pieces and multiple intermediary accounts.[7] The mixing services, which include both "anonymizing service providers" and "anonymizing software providers," allow cybercriminals to exchange CVCs associated with a particular ransom payment for other CVCs of equal value from other sources, in order to disguise the origin of the virtual currency.[8]

2. CVC Exchanges

In addition, cybercriminals often use CVC exchanges with "lax compliance controls or that operate in jurisdictions with little regulatory oversight" to "facilitate conversion of the 'dirty' CVC to their preferred legal tender" and then re-enter the traditional financial system to spend their ransom proceeds.[9] FinCEN's Updated Advisory repeats the statement in its October 2020 Advisory that "entities engaged in MSB activities (such as money transmission) are required to register as an MSB with FinCEN, and are subject to BSA obligations, including filing SARs."[10]

B. ADDITIONAL RED FLAGS

FinCEN's October 2020 Advisory included a list of 10 red flags that may indicate to financial institutions that a transaction could relate to ransomware attacks and therefore constitute an illicit payment. The Updated Advisory adds the following two red flags:

1. Mixing Services

Red flag number 11 exists when "[a] customer initiates a transfer of funds involving a mixing service," which implies an attempt by ransomware cybercriminals to obfuscate the source of a payment and launder CVCs received as part of a ransom.[11]

2. Use of Encrypted Network and Other Anonymizing Software

Red flag number 12 exists when "[a] customer uses an encrypted network (e.g., the onion router[12]) or an unidentified web portal to communicate with the recipient of the CVC transaction.[13] Cybercriminals commonly use anonymizing software and network services to disguise their identities while negotiating for payment of ransoms and when sending payment instructions.

C. IMMEDIATE REPORTING

FinCEN's new warning emphasizes that financial institutions, including CVC exchanges specifically, must identify and *immediately* report any suspicious transactions associated with ransomware attacks.[14] The advisory states that transactions associated with ransomware are serious enough that they will constitute "situations involving violations that require immediate attention," pursuant to the BSA regulations pertaining to Banks, Money Services Businesses, and Insurance Companies.[15] FinCEN reiterates that the sharing of information regarding suspicious transactions concerning specified unlawful activities is protected from liability by a statutory safe harbor.[16]

IMPLICATIONS

The November Advisory is the latest in a series of actions by federal agencies that are designed to encourage better reporting of ransomware attacks. Most recently, for example, OFAC issued new guidance in September stating that OFAC will consider "the reporting of ransomware attacks to appropriate U.S. government agencies . . . including whether an apparent violation of U.S. sanctions is voluntarily self-disclosed" as "a significant mitigating factor in determining an appropriate enforcement response."[17] Relatedly, in announcing the arrest this week of a Ukrainian national for perpetrating the ransomware attack on IT software provider Kaseya, which affected companies across the country, Attorney General Merrick Garland and Deputy Attorney General Lisa Monaco highlighted the importance of companies promptly reporting ransomware attacks to law enforcement, stating that Kaseya's prompt notification enabled law enforcement to respond to the incident.[18]

Financial institutions should update their processes to include the new potential "financial red flags" for payments that may be associated with ransomware, and to enable rapid filing of SARs and reporting in order to take advantage of the safe harbors discussed in the Advisory.

* * *

ENDNOTES

[1] FinCEN Advisory, FIN-2021-A004, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments" at 1–2 (Nov. 8, 2021), https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf.

[2] FinCEN Advisory, FIN-2020-A006, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments" at 5 (Oct. 1, 2020), https://www.fincen.gov/sites/default/files/advisory/2021-11-08/Advisory%20Ransomware%20FINAL%20508_2020%20rescinded.pdf.

[3] FinCEN Advisory, FIN-2021-A004 at 2.

[4] *Id.* at 4. MSB is an acronym for "Money Services Business."

[5] *Id.* at 7–8, 10.

[6] *Id.* at 5.

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] *Id.* at 4.

[11] *Id.* at 8.

[12] The onion router, or "Tor," is an online service that allows users to obscure their internet protocol address to engage in activity on the Internet anonymously.

[13] FinCEN Advisory, FIN-2021-A004 at 8.

[14] *Id.* at 10 (emphasis added).

[15] *Id.* at 10 & n.41.

[16] *Id.* at 10. Sharing information regarding SUAs with other financial institutions is protected by § 314(b) of the USA PATRIOT Act. *See FinCEN 314(b) Fact Sheet* (December 2020), https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf. In addition, a financial institution's filing of a SAR is protected from liability by the Bank Secrecy Act's safe harbor provision at 31 U.S.C. § 5318(g)(3). *See Interagency Advisory: Federal Court Reaffirms Protections for Financial Institutions Filing Suspicious Activity Reports* (May 24, 2004), https://www.fincen.gov/sites/default/files/guidance/advis35.pdf.

[17] OFAC Advisory, "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," at 5 (Sept. 21, 2021), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.

[18] Dep't of Just., "Ukrainian Arrested and Charged with Ransomware Attack on Kaseya," Press Release (Nov. 8, 2021), https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya; Dep't of Just., "Attorney General Merrick B. Garland, Deputy Attorney General Lisa O. Monaco and FBI Director Christopher Wray Deliver Remarks on Sodinokibi/REvil Ransomware Arrest" (Nov. 8, 2021), https://www.justice.gov/opa/speech/attorney-general-merrick-b-garland-deputy-attorney-general-lisa-o-monaco-and-fbi-director.

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 or to any 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.