



FinCEN ADVISORY

FIN-2021-A004

November 8, 2021

Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments

Detecting and reporting ransomware payments are vital to holding ransomware attackers accountable for their crimes and preventing the laundering of ransomware proceeds.

This Advisory should be shared with:

- Chief Executive Officers
- Chief Operating Officers
- Chief Compliance Officers
- Chief Risk Officers
- AML/BSA Departments
- Legal Departments
- Cyber and Security Departments
- Customer Service Agents
- Bank Tellers

SAR Filing Request

FinCEN requests financial institutions reference this advisory in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the following key term: **"CYBER FIN-2021-A004"** and select SAR field 42 (Cyber Event). Additional guidance for filing SARs appears near the end of this advisory.

Introduction

The Financial Crimes Enforcement Network (FinCEN) is updating and replacing its October 1, 2020 Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments.¹ This updated advisory is in response to the increase of ransomware attacks in recent months against critical U.S. infrastructure, such as the May 2021 ransomware attack that disrupted the operations of Colonial Pipeline, the largest pipeline system for refined oil products in the United States. This attack led to widespread gasoline shortages that affected tens of millions of Americans. Other recent targets include entities in the manufacturing, legal services, insurance, financial services, health care, energy, and food production sectors.

FinCEN issued the original advisory to alert financial institutions to predominant trends, typologies, and potential indicators of ransomware and associated money laundering activities. The advisory provided 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. This amended advisory reflects information released by FinCEN in its Financial

Trend Analysis Report issued on October 15, 2021, and is part of the Department of the Treasury's broader efforts to combat ransomware.² In particular, this updated advisory identifies new trends

1. FIN-2020-A006

2. See U.S. Department of the Treasury Press Release, "[Treasury Continues Campaign to Combat Ransomware As Part of Whole-of-Government Effort](#)," (Oct. 15, 2021); and FinCEN, [Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021](#) (FinCEN 2021 Ransomware Report), at 3 (Oct. 15, 2021); see also White House, [FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware](#) (Oct. 13, 2021).

and typologies of ransomware and associated payments, including the growing proliferation of anonymity-enhanced cryptocurrencies (AECs) and decentralized mixers.³

Additionally, in October 2020, the Department of Justice (DOJ) released “Cryptocurrency: An Enforcement Framework,” a publication produced by the Attorney General’s Cyber-Digital Task Force. The Framework provides a comprehensive overview of the emerging threats and enforcement challenges associated with the increasing prevalence and use of cryptocurrency; details the important relationships that the DOJ has built with regulatory and enforcement partners both within the U.S. government and around the world; and outlines the DOJ’s response strategies. Among other topics, the Framework discusses the use of cryptocurrency as a payment method by bad actors to facilitate ransom and blackmail.⁴

The information contained in this advisory is derived from FinCEN’s analysis of cyber and ransomware-related Bank Secrecy Act (BSA) data, open source reporting, and law enforcement partners.

Ransomware 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.⁵ 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). The consequences of a ransomware attack can be severe and far-reaching—with losses of sensitive, proprietary, and critical information and/or loss of business functionality.

The Role of Financial Intermediaries in Facilitating Ransomware Payments

Ransomware attacks are a growing concern for the financial sector because of the critical role financial institutions play in the collection of ransom payments. Processing ransomware payments is typically a multi-step process that involves at least one depository institution and one or more entities directly or indirectly facilitating victim payments, including money services businesses (MSB). Most ransomware schemes involve convertible virtual currency (CVC), the preferred payment method of ransomware perpetrators. Following the delivery of the ransom demand, a ransomware victim will typically transmit funds via wire transfer, automated clearinghouse, or credit card payment to a CVC exchange to purchase the type and amount of CVC specified by the ransomware perpetrator. Next, the victim or an entity working on the victim’s behalf sends the CVC, often from a wallet hosted⁶ at the exchange, to the perpetrator’s designated account or CVC

3. See [FinCEN 2021 Ransomware Report](#), at 2, 3, 9, 12-13 (Oct. 15, 2021).

4. See DOJ Report of the Attorney General’s Cyber Criminal Task Force, [Cryptocurrency: An Enforcement Framework](#) (Oct. 2020) (hereinafter, DOJ Cryptocurrency Enforcement Framework); see also DOJ Press Release, [“Attorney General William P. Barr Announces Publication of Cryptocurrency Enforcement Framework,”](#) (Oct. 8, 2020).

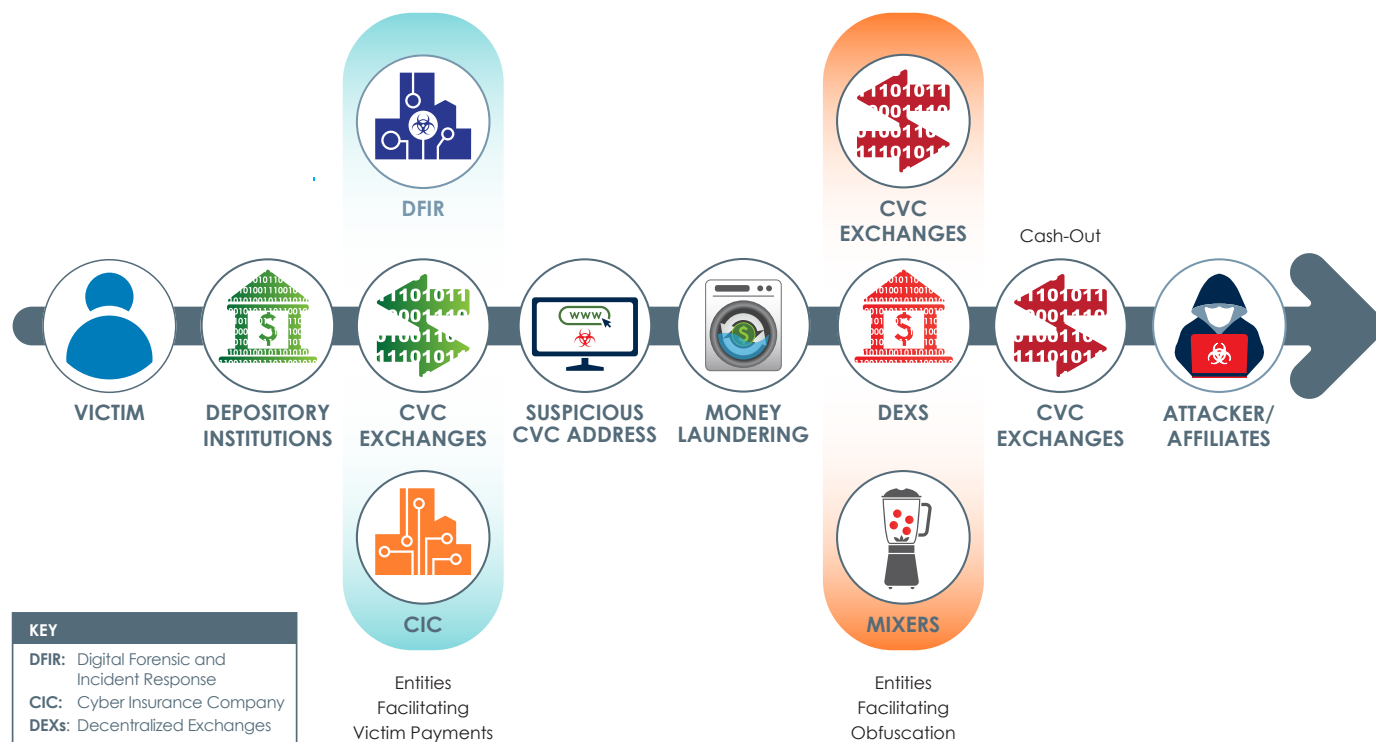
5. Both extortion and computer fraud and abuse are specified unlawful activities and predicate offenses to money laundering. See 18 U.S.C § 1956(c)(7).

6. “Hosted wallets” are CVC wallets where the CVC exchange receives, stores, and transmits the CVCs on behalf of their accountholders. See FinCEN Guidance, FIN-2019-G001, [“Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies,”](#) (May 9, 2019).

address. The perpetrator then launders the funds through various means — including mixers, tumblers,⁷ and chain hopping⁸ — to convert funds into other CVCs. These transactions may be structured into smaller “smurfing”⁹ transactions involving multiple people, and across many different CVC addresses, accounts, and exchanges, including peer-to-peer (P2P)¹⁰ and nested exchanges. Criminals prefer to launder their ransomware proceeds in jurisdictions with weak anti-money laundering and countering financing of terrorism (AML/CFT) controls.

Cyber insurance companies (CICs) and digital forensic and incident response (DFIR) companies can also play a role in ransomware transactions. CICs issue policies designed to mitigate an entity’s losses from a variety of cyber incidents, such as data breaches, business interruption, and network damage. CICs may reimburse policyholders for particular remediation services including the use of DFIRs if needed. As part of incident remediation, affected entities may hire a DFIR company to negotiate with the cybercriminal, facilitate payment to the cybercriminal, and investigate the source of the cybersecurity breach.

Figure 1. Movement of CVC in Ransomware Incidents



- Mixing or tumbling involves the use of mechanisms to break the connection between an address sending CVC and the addresses receiving CVC. For more information, see [FinCEN 2021 Ransomware Report](#), at 13 (Oct. 15, 2021).
- Chain hopping is a cross-virtual-asset layering technique for users attempting to conceal criminal behavior. Criminals obfuscate the trail of virtual currency by shifting the trail of transactions from the blockchain of one virtual currency to the blockchain of another virtual currency, often in rapid succession. See DOJ [Cryptocurrency Enforcement Framework](#), at 41-44.
- Smurfing refers to a layering technique in money laundering that involves breaking total amounts of funds into smaller amounts to move through multiple accounts before arriving at the ultimate beneficiary.
- P2P exchangers are individuals or entities offering to exchange fiat currencies for virtual currencies or one virtual currency for another virtual currency. P2P exchangers usually operate informally, typically advertising and marketing their services through online classified advertisements or fora, social media, and by word of mouth. See FinCEN Advisory, FIN-2019-A003, [“Advisory on Illicit Activity Involving Convertible Virtual Currency,”](#) (May 9, 2019).

Some DFIR companies and CICs, as well as some MSBs that offer CVCs, facilitate ransomware payments to cybercriminals, often by directly receiving customers' fiat funds, exchanging them for CVC, and then transferring the CVC to criminal-controlled accounts. Depending on the particular facts and circumstances, this activity could constitute money transmission. 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.¹¹ 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.

Persons involved in ransomware payments must also be aware of any Office of Foreign Assets Control (OFAC)-related obligations that may arise from that activity.¹² On September 21, 2021, OFAC issued an updated advisory highlighting the sanctions risks associated with facilitating ransomware payments on behalf of victims targeted by malicious cyber-enabled activities.¹³ Additionally, in October 2021, OFAC issued sanctions compliance guidance for the virtual currency industry, which provides an overview of key items such as reporting instructions, consequences of non-compliance, and compliance best practices.¹⁴

Trends and Typologies of Ransomware and Associated Payments

The severity and sophistication of ransomware attacks continue to rise¹⁵ across various sectors, particularly across governmental entities, and financial, educational, and healthcare institutions.¹⁶ Ransomware attacks on small municipalities and healthcare organizations have increased, likely due to the victims' weaker cybersecurity controls, such as inadequate system backups and ineffective incident response capabilities.¹⁷

Cybercriminals using ransomware often resort to common tactics, such as wide-scale phishing and targeted spear-phishing campaigns that induce victims to download a malicious file or go to a malicious site, exploit remote desktop protocol endpoints and software vulnerabilities, or deploy "drive-by" malware attacks that host malicious code on legitimate websites. Proactive prevention through effective cyber hygiene, cybersecurity controls, and business continuity resiliency is often the best defense against ransomware.¹⁸ On July 15, 2021, the U.S. government announced

11. See generally 31 CFR Part 1022; and 31 CFR § 1010.100(ff).
12. See OFAC, "[Sanctions Compliance Guidance for the Virtual Currency Industry](#)," (Oct. 15, 2021); [FinCEN Ransomware Report 2021](#), at 13 (Oct. 15, 2021); and White House, [FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware](#), (Oct. 13, 2021).
13. See OFAC, "[Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments](#)," (Sept. 21, 2021).
14. See OFAC, "[Sanctions Compliance Guidance for the Virtual Currency Industry](#)," (Oct. 15, 2021).
15. The Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) received 20% more reports of ransomware incidents in 2020 than in 2019, with a 225% increase in ransom demands, totaling \$29 million in 2020 up from \$9 million in 2019. See FBI IC3, [2020 Internet Crime Report](#), (2020). In the first six months of 2021, FinCEN identified \$590 million in ransomware-related SARs, a 42 percent increase, compared to 2020's total of \$416 million. See [FinCEN 2021 Ransomware Report](#), at 3 (Oct. 15, 2021).
16. See FinCEN Advisory, FIN-2019-A005, "[Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 \(COVID-19\) Pandemic](#)," (July 30, 2020).
17. See [FinCEN 2021 Ransomware Report](#), at 3 (Oct. 15, 2021). Also see generally DHS Cybersecurity & Infrastructure Security Agency (CISA), [Ransomware Guide](#), (Sept. 2020).
18. See FBI and DHS CISA, "[Joint Cybersecurity Advisory: Ransomware Awareness for Holidays and Weekends](#)," (Aug. 31, 2021).

new resources and initiatives to protect American businesses and communities from ransomware attacks. The DOJ and the Department of Homeland Security (DHS), together with federal partners, launched a new website to combat the threat of ransomware.¹⁹ StopRansomware.gov establishes a one-stop hub for ransomware resources for individuals, businesses, and other organizations. This new hub is a collaborative effort across the federal government and is the first joint website created to help private and public organizations mitigate their ransomware risk.²⁰

Extortion Schemes: Cybercriminals are increasingly engaging in “double extortion schemes,” which involve removing sensitive data from the targeted networks and encrypting the system files and demanding ransom.²¹ The cybercriminals then threaten to publish or sell the stolen data if the victim does not pay the ransom. Other extortion schemes have also emerged whereby the cybercriminals use the system breach to target additional parties related to the initial victim, such as the victim’s business partners and customers, in an attempt to identify follow-on targets.²² These third parties may provide new leverage for the attacker to use against the victim.

Use of Anonymity-Enhanced Cryptocurrencies (AECs): Cybercriminals usually require ransomware payments to be denominated in CVCs, most commonly in Bitcoin. However, they are also increasingly requiring or incentivizing victims to pay in AECs that reduce the transparency of CVC financial flows, through anonymizing features, such as mixing and cryptographic enhancements.²³ Cybercriminals have even offered discounted rates to victims who pay their ransoms in AECs. One such AEC increasingly demanded by ransomware criminals is Monero.

Unregistered CVC Mixing Services: In order to protect their illicit gains, cybercriminals often use mixers to obfuscate their illicit activities.²⁴ Mixers aim to “break” the connection between the sender and the receiver of the CVC transaction by commingling CVC belonging to other mixer users and splitting the value into many small pieces that pass through a number of different intermediary accounts. The result is that cybercriminals trade CVC directly associated with any one particular crime for other CVC of equal value originating from alternative sources. Mixers include both anonymizing service providers, and anonymizing software providers.

Cashing Out Through Foreign CVC Exchanges: In order to launder and cash out their illicit proceeds, cybercriminals often use CVC exchanges that have lax compliance controls or that operate in jurisdictions with little regulatory oversight. These exchanges often operate in high-risk jurisdictions or in jurisdictions that do not maintain effective information sharing agreements with other countries. Cybercriminals and their affiliates may use these exchanges to facilitate conversion of the “dirty” CVC to their preferred legal tender or fiat currency to integrate back into the financial system.

19. See DOJ Press Release, “[U.S. Government Launches First One-Stop Ransomware Resource at StopRansomware.gov](#),” (July 15, 2021).

20. See CISA, <https://www.cisa.gov/stopransomware> - StopRansomware.gov is the U.S. Government’s official one-stop location for resources to tackle ransomware more effectively.

21. See [FinCEN 2021 Ransomware Report](#), at 3 (Oct. 15, 2021).

22. See FBI and DHS CISA, “[Joint Cybersecurity Advisory: Ransomware Awareness for Holidays and Weekends](#),” (Aug. 31, 2021).

23. See FinCEN Advisory, FIN-2019-A003, “[Advisory on Illicit Activity Involving Convertible Virtual Currency](#),” (May 9, 2019).

24. See [FinCEN 2021 Ransomware Report](#), at 13 (Oct. 15, 2021).

Ransomware Criminals Forming Partnerships and Sharing Resources: Many cybercriminals engage in profit sharing through ransomware-as-a-service (RaaS), a business model in which ransomware developers sell or otherwise deliver ransomware software to individuals or groups that have separately gained illicit access to the victim network. RaaS allows cybercriminals of varying skill levels to monetize their illicit access by infecting computer networks with ransomware. As part of the profit sharing arrangement, the RaaS developer often receives a percentage of any ransom paid by the victim. A recent example of this model is the DarkSide ransomware, which cybercriminals deployed against Colonial Pipeline in early 2021.²⁵

Use of “Fileless” Ransomware: Fileless ransomware is a sophisticated tool that can be challenging to detect because the malicious code is written to a computer’s memory rather than into a file on a hard drive, which allows cybercriminals to circumvent off-the-shelf antivirus and malware defenses.²⁶

“Big Game Hunting” Schemes: Cybercriminals are increasingly engaging in selective targeting of larger enterprises to demand bigger payouts – commonly referred to as “big game hunting.”²⁷ Cybercriminals may target organizations with weaker security controls and a higher propensity to pay the ransom due to the criticality of their services.

Recent Examples of Ransomware Attacks

In 2021, there have been some noteworthy ransomware attacks against critical U.S. infrastructure conducted by cybercriminal groups:

- As noted above, in May 2021, a cybercriminal group perpetrated an attack that disrupted Colonial Pipeline causing widespread U.S. gasoline shortages. The FBI subsequently attributed the attack to a Russian-speaking group known as DarkSide.²⁸ DarkSide developed ransomware for a criminal organization that then perpetrated the attack. This other criminal organization transferred a portion of the ransom proceeds to DarkSide as payment for the development of the ransomware. (As discussed earlier in this advisory, the development of ransomware as a service is known as RaaS.) The FBI successfully seized criminal proceeds from a bitcoin wallet that DarkSide ransomware actors used to collect a ransom payment from a victim.²⁹
- Also in May 2021, a cybercriminal group conducted a ransomware attack of JBS Meat Packing Corporation, causing a shutdown to their entire production process. The FBI attributed this attack to Sodinokibi/REvil.³⁰

25. See DOJ Press Release, [“DAG Monaco Delivers Remarks at Press Conference on Darkside Attack on Colonial Pipeline,”](#) (June 7, 2021).

26. The Multi-State Information Sharing and Analysis Center (MS-ISAC) observed a 153% increase of reported instances of ransomware targeting state, local, tribal, and territorial governments from 2018 to 2019. See MS-ISAC, [Security Primer – Ransomware](#), (May 2020).

27. See FBI Public Service Announcement, Alert No. I-100219-PSA, [“High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations,”](#) (Oct. 2, 2019).

28. See FBI, [Press Conference Regarding the Ransomware Attack on Colonial Pipeline](#), (June 7, 2021).

29. See *id.*

30. See FBI, [FBI Statement on JBS Cyberattack](#), (June 2, 2021).

- In July 2021, Sodinokibi/REvil attacked Kaseya, a U.S.-based critical infrastructure entity in the IT Sector and implementations of their remote monitoring and management tool, affecting hundreds of organizations—including multiple managed service providers and their customers.³¹

FinCEN’s review of BSA data has identified DarkSide and Sodinokibi/REvil as among the most costly ransomware variants in the first six months of 2021. During this timeframe, 458 ransomware related transactions were reported with a total value of \$590 million.³²

Financial Red Flag Indicators of Ransomware and Associated Payments

FinCEN has identified the following financial red flag indicators of ransomware-related illicit activity to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with ransomware attacks. As no single financial red flag indicator is indicative of illicit or suspicious activity, financial institutions should consider the relevant facts and circumstances of each transaction, in keeping with their risk-based approach to compliance.³³

-  1 A financial institution or its customer detects IT enterprise activity that is connected to ransomware cyber indicators or known cyber threat actors. Malicious cyber activity may be evident in system log files, network traffic, or file information.³⁴
-  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 is connected to ransomware variants,³⁵ payments, or related activity. These connections may appear in open sources or commercial or government analyses.
-  4 An irregular 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.

31. See FBI and CISA, “[Joint Cybersecurity Advisory: Ransomware Awareness for Holidays and Weekends](#),” (August 31, 2021).

32. See FinCEN, [FinCEN 2021 Report](#), at 3 (Oct. 15, 2021).

33. For more information about red flags of illicit CVC use, see FinCEN Advisory, FIN-2019-A003, “[Advisory on Illicit Activity Involving Convertible Virtual Currency](#),” (May 9, 2019).

34. For example cyber indicators of compromise on specific ransomware threats, see DHS CISA Technical Alerts, [Ransomware Alerts](#). For other cyber indicator resources, see also FinCEN’s Cyber Indicator Lists (CILs), shared through the FinCEN Secure Information Sharing System; the U.S. Department of the Treasury’s Office of Cybersecurity and Critical Infrastructure Protection’s CILs and circulars, available upon request; and DHS CISA’s [cyber analytic products and services](#), including a comprehensive list of COVID-19-related indicators of compromise in [CSV](#) or [STIX-formatted XML](#) formats, the [Cyber Information Sharing and Collaboration Program \(CISCP\)](#), and the [Automated Indicator Sharing \(AIS\) program](#). Public-private and industry partnerships, such as the [Financial Services Information Sharing and Analysis Center](#), and open source and commercial cyber threat feeds can also be useful resources.

35. Ransomware actors develop their own versions of ransomware, known as “variants.” For more information, see FinCEN, [FinCEN 2021 Ransomware Report](#), at 3 (Oct. 15, 2021).

-  A DFIR or CIC customer receives funds from a counterparty and shortly after receipt of funds sends equivalent amounts to a CVC exchange.
-  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.
-  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.
-  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.
-  A customer uses a foreign-located CVC exchanger in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for CVC entities.
-  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. This may be indicative of attempts to break the chain of custody on the respective blockchains or further obfuscate the transaction.
-  A customer initiates a transfer of funds involving a mixing service.
-  A customer uses an encrypted network (e.g., the onion router) or an unidentified web portal to communicate with the recipient of the CVC transaction.

Reminder of Regulatory Obligations for U.S. Financial Institutions Regarding Suspicious Activity Reporting Involving Ransomware and USA PATRIOT ACT Section 314(b) Information Sharing Authority

Suspicious Activity Reporting

Financial institutions play an important role in protecting the U.S. financial system from ransomware threats through compliance with their BSA obligations. Financial institutions should determine if filing a SAR is required or appropriate when dealing with an incident of ransomware conducted *by, at, or through* the financial institution, including ransom payments made by financial institutions that are victims of ransomware. As a reminder, a financial institution is required to file a 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 MSBs)³⁶ or more in funds or other assets and involves funds derived from illegal activity, or attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity. Reportable activity can involve transactions, including payments made by financial institutions, related to criminal activity like extortion and unauthorized electronic intrusions that damage, disable, or otherwise affect critical systems. SAR obligations apply to both *attempted and successful* transactions, including both attempted and successful initiated extortion transactions.³⁷

Financial institutions are required to file complete and accurate reports that incorporate *all relevant information available*, including cyber-related information. When filing a SAR regarding suspicious transactions that involve cyber events (including ransomware), financial institutions should provide all pertinent available information on the event and associated with the suspicious activity, including cyber-related information and technical indicators, in the SAR form and narrative. When filing is not required, institutions may file a SAR voluntarily to aid law enforcement in protecting the financial sector. Valuable cyber indicators for law enforcement investigations for ransomware can include relevant email addresses, Internet Protocol (IP) addresses with their respective timestamps, login information with location and timestamps, CVC 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.

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.³⁸ Financial institutions must provide any requested SAR and all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.³⁹ When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or anti-money laundering program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.⁴⁰

36. See 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.20. The monetary threshold for filing money services businesses SARs is, with one exception, set at or above \$2,000. See also 31 CFR § 1022.320(a)(2).

37. FinCEN assesses that ransomware-related activity is under-reported.

38. See 31 CFR §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), and 1026.320(d).

39. *Id.* See also FinCEN Guidance, FIN-2007-G003, "[Suspicious Activity Report Supporting Documentation](#)," (June 13, 2007).

40. See FinCEN Guidance, FIN-2007-G003, "[Suspicious Activity Report Supporting Documentation](#)," (June 13, 2007).

Ransomware Payments Require Immediate Attention

It is critical that financial institutions (including CVC exchanges) identify and immediately report any suspicious transactions associated with ransomware attacks. For purposes of meeting a financial institution's SAR obligations, FinCEN and law enforcement consider suspicious transactions involving ransomware attacks to constitute "situations involving violations that require immediate attention."⁴¹ Financial institutions wanting to report suspicious transactions related to recent or ongoing ransomware attacks should contact FinCEN's Financial Institution Hotline at 1-866-556-3974. Financial institutions must subsequently file a SAR using FinCEN's BSA E-filing System, providing as much of the relevant details around the activity as available at that time. Amended SARs should be filed to include additional information related to the same activity that is learned later; completely new activity should be filed in a new "initial" SAR filing.

SAR Filing Instructions

FinCEN requests that financial institutions reference this advisory by including the key term:

"CYBER-FIN-2021-A004"

In SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and ransomware-related activity.

Financial institutions should also select SAR field 42 (Cyber event) as the associated suspicious activity type, as well as select SAR field 42z (Cyber event - Other) while including "ransomware" as keywords in SAR field 42z, to indicate a connection between the suspicious activity being reported and possible ransomware activity. Additionally, financial institutions should include any relevant technical cyber indicators related to the ransomware activity and associated transactions within the available structured cyber event indicator SAR fields 44(a)-(j), (z).

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing evolving ransomware schemes. Financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information relating to transactions that the institution suspects may involve the proceeds of one or more specified unlawful activities ("SUAs") and such an institution will still remain protected from civil liability under the section 314(b) safe harbor. The SUAs 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. FinCEN strongly encourages information sharing via section 314(b) where financial institutions suspect that a transaction may involve terrorist financing or money laundering, including one or more SUAs.⁴²

41. See e.g., 31 CFR § 1020.320(b)(3) (Banks), 31 CFR § 1022.320(b)(3) (Money Services Businesses), and 31 CFR § 1025.320(b)(3) (Insurance Companies).

42. For further guidance related to the 314(b) Program, see FinCEN, "[Section 314\(b\) Fact Sheet](#)" (Dec. 2020).

For Further Information

Questions or comments regarding the contents of this advisory to the FinCEN Regulatory Support Section at frc@fincen.gov.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.