



FinCEN ADVISORY

FIN-2020-A006

October 1, 2020

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

Detecting and reporting ransomware payments are vital to prevent and deter cybercriminals from deploying malicious software to extort individuals and businesses and hold ransomware attackers accountable for their crimes.

This Advisory should be shared with:

- Chief Executive Officers
- Chief Operating Officers
- Chief Compliance Officers
- Chief Risk Officers
- Chief Information 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-2020-A006” and select SAR field 42 (Cyber Event). Additional guidance on filing SARs appears near the end of this advisory.

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to predominant trends, typologies, and potential indicators of ransomware and associated money laundering activities. This advisory 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.

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 their systems or data.¹ In some cases, in addition to the attack, the perpetrators threaten to publish sensitive files belonging to the victims, which can be individuals or business entities

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

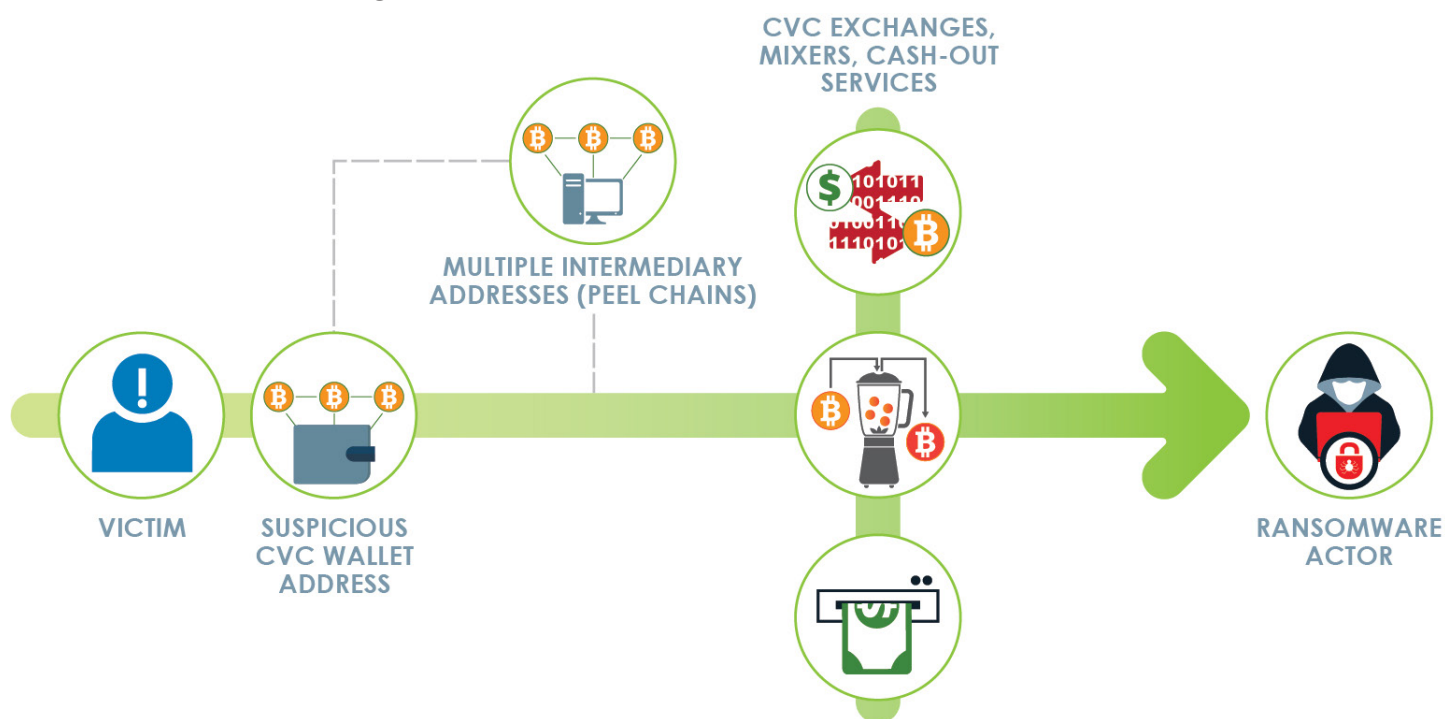
(including financial institutions). The consequences of a ransomware attack can be severe and far-reaching—with losses of sensitive, proprietary, and critical information and/or loss of business functionality.

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 money services business (MSB). Many 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 will send the CVC, often from a wallet hosted² at the exchange, to the perpetrator's designated account or CVC address. The perpetrator then launders the funds through various means, including mixers and tumblers³ to convert funds into other CVCs, smurfing⁴ transactions across many accounts and exchanges, and/or moving the CVC to foreign-located exchanges and peer-to-peer (P2P) exchangers⁵ in jurisdictions with weak anti-money laundering and countering financing of terrorism (AML/CFT) controls.

-
2. "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).
 3. Mixing or tumbling involves the use of mechanisms to break the connection between an address sending CVC and the addresses receiving CVC.
 4. 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.
 5. 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).

Figure 1. Movement of CVC in Ransomware Attacks



Involvement of Digital Forensics and Incident Response and Cyber Insurance Companies in Ransomware Payments

The prevalence of ransomware attacks has led to the creation of companies that provide protection and mitigation services to victims of ransomware attacks. Among these entities are digital forensics and incident response (DFIR) companies and cyber insurance companies (CICs). 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 money services business activities (such as money transmission) are required to register as an MSB with FinCEN, and are subject to BSA obligations, including filing suspicious activity reports (SARs).⁶ 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. Today, OFAC issued an [advisory](#) highlighting the sanctions risks associated with facilitating ransomware payments on behalf of victims targeted by malicious cyber-enabled activities.

6. See generally 31 C.F.R. Part 1022 and 31 CFR § 1010.100(ff).

Trends and Typologies of Ransomware and Associated Payments

The severity and sophistication of ransomware attacks continue to rise⁷ across various sectors, particularly across governmental entities, and financial, educational, and healthcare institutions.⁸ 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.⁹

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.¹⁰

Increasing Sophistication of Ransomware Operations

Big Game Hunting Schemes: Ransomware actors are increasingly engaging in selective targeting of larger enterprises to demand bigger payouts – commonly referred to as "big game hunting."¹¹

Ransomware Criminals Forming Partnerships and Sharing Resources: Many cybercriminals are sharing resources to enhance the effectiveness of ransomware attacks, such as ransomware exploit kits that come with ready-made malicious codes and tools. These kits can be purchased, although they are also offered free of charge. Some ransomware groups are also forming partnerships to share advice, code, trends, techniques, and illegally-obtained information over shared platforms.

"Double Extortion" Schemes: Ransomware criminals are increasingly engaging in "double extortion schemes," which involve removing sensitive data from the targeted networks and encrypting the system files and demanding ransom. The criminals then threaten to publish or sell the stolen data if the victim fails to pay the ransom.




-
7. The Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) received 37% more reports of ransomware incidents in 2019 than in 2018, with a 46% increase in associated financial losses. BSA reporting shows a stark increase in financial losses per ransomware incident, with the average dollar amount in financial institution SARs on ransomware increasing approximately \$87,000 from 2018 to 2019 (\$417,000 to \$504,000) and \$280,000 from 2019 to thus far in 2020 (\$504,000 to \$783,000). See FBI IC3, "[2019 Internet Crime Report](#)," (2019); and FBI IC3, "[2018 Internet Crime Report](#)," (2018).
 8. See FinCEN Advisory, [FIN-2020-A005](#), "Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic," (July 30, 2020).
 9. Multi-State Information Sharing and Analysis Center (MS-ISAC), "[Security Primer – Ransomware](#)," (May 2020).
 10. For more information about ransomware risk, see Federal Financial Institutions Examination Council (FFIEC), Press Release, "[FFIEC Releases Statement on Cyber Attacks Involving Extortion](#)," (November 3, 2015); Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), "[Security Tip \(ST19-001\): Protecting against Ransomware](#)," (April 11, 2019); and DHS CISA, MS-ISAC, National Governors Association (NGA), and National Association of State Chief Information Officers (NASCIO), Joint Alert, "[CISA, MS-ISAC, NGA & NASCIO Recommend Immediate Action to Safeguard against Ransomware](#)," (July 29, 2019).
 11. See FBI Public Service Announcement, [Alert No. I-100219-PSA](#), "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations," (October 2, 2019).

Use of Anonymity-Enhanced Cryptocurrencies (AECs): Cybercriminals usually require ransomware payments to be denominated in CVCs, most commonly in bitcoin (see Figure 1). However, they are also increasingly requiring or incentivizing victims to pay in AECs that reduce the transparency of CVC financial flows, including ransomware payments, through anonymizing features, such as mixing and cryptographic enhancements.¹² Some ransomware operators have even offered discounted rates to victims who pay their ransoms in AECs.

Use of “Fileless” Ransomware: Fileless ransomware is a more sophisticated tool that can be challenging to detect because the malicious code is written into the computer’s memory rather than into a file on a hard drive, which allows attackers to circumvent off-the-shelf antivirus and malware defenses.¹³

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.¹⁴








-  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.¹⁵
-  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.
-  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.

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

13. The 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).

14. 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).

15. 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.

-  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.
-  A DFIR or CIC customer receives funds from a customer company 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 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.
-  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 CVC exchanger or foreign-located MSB in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for CVC entities.
-  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.

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 can 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)¹⁶ or more in funds or other assets and involves

16. See 31 C.F.R. §§ 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 C.F.R. § 1022.320(a)(2).

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.¹⁷

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, 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.

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.¹⁸ 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.¹⁹ 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.²⁰

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

18. See 31 C.F.R. §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), and 1026.320(d).

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

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

SAR Filing Instructions

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

“CYBER-FIN-2020-A006”

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.²¹

For Further Information

Questions or comments regarding the contents of this advisory should be addressed 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.

21. For further guidance related to the 314(b) Program, see FinCEN [Fact Sheet](#), “Section 314(b)” (November 2016) and FinCEN Guidance, [FIN-2009-G002](#), “Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act,” (June 16, 2009).