Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns

United States Senate Committee on

Homeland Security & Governmental Affairs

U.S. Senator Gary Peters | Chairman

Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns

A HSGAC Majority Staff Report

Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Ransomware is a dangerous form of cyber-attack where threat actors prevent access to computer systems or threaten to release data unless a ransom is paid. It has the power to bankrupt businesses and cripple critical infrastructure – posing a grave threat to our national and economic security. The use of cryptocurrencies has further enabled ransomware attacks, particularly because cryptocurrency is decentralized and distributed and illicit actors can take steps to obscure transactions and make them more difficult to track.

In recent years, ransomware attack victims have included hospitals, school systems, local, state, and federal government agencies, as well as other critical infrastructure, including the water and energy sectors. In 2021, ransomware attacks impacted at least 2,323 local governments, schools, and healthcare providers in the United States. According to the World Economic Forum, ransomware attacks increased by 435 percent in 2020 and "are outpacing societies' ability to effectively prevent or respond to them."

Many of these attacks generated significant losses and damages for victims. A three-year comparison of the number of complaints of ransomware submitted to the Federal Bureau of Investigation (FBI) between 2018 and 2020, demonstrates a 65.7 percent increase in victim count and a staggering 705 percent increase in adjusted losses. In 2021, the agency received 3,729 ransomware complaints with adjusted losses of more than $49.2 million.

However, even these figures likely drastically underestimate the actual number of attacks and ransom payments made by victims and related losses. In fact, the FBI acknowledges that its data is "artificially low." Further evidence of this under-reporting is that the government data is significantly lower than several private sector estimates. For instance, Chainalysis, a blockchain data and analysis company that works with financial institutions, insurance and cybersecurity companies, and as a contractor for the U.S. government, reports that in 2020, malign actors received at least $692 million in cryptocurrency extorted as part of ransomware attacks, up from $152 million in 2019, close to a 300 percent increase over a two-year period. A separate study by the anti-malware company Emsisoft found that there were at least 24,770 ransomware incidents in the U.S. in 2019 and estimated their costs (including costs of downtime) at just under $10 billion.

To better understand this growing threat, U.S. Senator Gary Peters, Chairman of the Senate Homeland Security and Governmental Affairs Committee, announced in July 2020 an investigation into the role of cryptocurrency in incentivizing and enabling ransomware attacks, and the resulting harm of such attacks to victims. As a part of this ten-month investigation, Committee staff conducted interviews with federal law enforcement and regulatory agencies as well as private companies that assist ransomware victims with ransom demands. While not exhaustive, this report addresses key pieces of the larger landscape of the increasing national security threat from ransomware attacks and the use of cryptocurrency for ransom payments. The report details recommendations to address current gaps in information on ransomware attacks and use of cryptocurrency as ransom payments in these attacks.

The report finds that there is a lack of comprehensive data on the amount of ransomware attacks and use of cryptocurrency as ransom payments in these attacks. While multiple federal agencies are taking steps to address the increasing threat of ransomware attacks, more data is needed to better understand and combat these attacks. In interviews with Committee staff, federal officials and private sector companies each acknowledged the need for more compliance and data (*e.g.*, reporting of incidents and ransom payments). When more data is collected, the federal government will be in a better position to assist existing and potential cybercrime victims with prevention, detection, mitigation, and recovery. Such information also facilitates more efficient investigation and prosecution of illicit actors.

To address the current lack of information regarding the breadth and depth of the ransomware threat, Chairman Peters and Ranking Member Portman introduced the Cyber Incident Reporting Act of 2021, which passed the Senate as part of the Strengthening American Cybersecurity Act of 2022. The incident reporting provisions later became law as the Cyber Incident Reporting for Critical Infrastructure Act of 2022 in the Consolidated Appropriations Act of 2022 in March 2022. The new reporting mandates in the law will begin to address this problem. Nevertheless, as indicated by the findings in the report, the Administration and Congress must remain vigilant against this growing threat.

Almost 40 million Americans – including approximately three-in-ten Americans age 18 to 29 – have engaged in some form of investment, trade, or other legitimate use of cryptocurrencies according to a November 2021 estimate by the nonpartisan Pew Research Center. The global market value of all cryptocurrencies reached $3 trillion in 2021, up from $14 billion in 2016.

However, according to multiple agencies interviewed by Committee staff, cryptocurrency, typically Bitcoin, has become a near universal form of ransom payment in ransomware attacks, in part, because cryptocurrency enables criminals to extort huge sums of money from victims across diverse sectors with incredible speed. The payment structure's decentralized nature, as well as irregular regulatory compliance by some entities within the space and new anonymizing techniques contribute to the challenges law enforcement faces when seeking to arrest criminal actors, particularly foreign-based actors. High profile attacks, such as Colonial Pipeline, demonstrate ransomware attackers' threat to national security. The FBI's recovery of over half of the ransom paid by Colonial Pipeline, however, shows that with access to the right information, law enforcement can leverage cryptocurrency's unique features as well as other investigative techniques to track down cyber criminals and recover stolen funds.

Unfortunately, data reporting and collection on ransomware attacks and payments is fragmented and incomplete. Two federal agencies claim to host the government's one stop location for reporting ransomware attacks – the Cybersecurity and Infrastructure Agency (CISA) StopRansomware.gov website and the FBI's IC3.gov. These two websites are separate and, while the agencies state that they share data with each other, in discussions with Committee staff, ransomware incident response firms questioned the effectiveness of such communication channels' impact on assisting victims of an attack.

Many federal regulators have taken steps to address the rising threat of ransomware attacks by issuing new, and expanding existing, regulations and guidance. Generally, with respect to cryptocurrency, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) has clarified that "money service businesses", *e.g.*, persons that accept and transmit "value that substitutes for currency", are subject to key financial regulations. Over the past few years, the Securities and Exchange Commission (SEC), Internal Revenue Service (IRS), and FinCEN have each issued new guidance and regulations subjecting cryptocurrency to additional oversight. In 2021, the Department of Justice (DOJ), SEC, and the Treasury Department's Office of Foreign Assets Control (OFAC), among other agencies, also issued guidance recognizing the need for more ransomware incident reporting.

On March 9, 2022, the Biden Administration issued an Executive Order outlining a "whole-of-government" approach to examining the risks associated with the sharp increase in use of cryptocurrencies. Among other key policy priorities, the Administration recognizes that cryptocurrencies have "facilitated sophisticated cybercrime-related financial networks and activity, including through ransomware activity." The data needed to support these initiatives, among other agency efforts to tackle ransomware and cryptocurrency ransom payments, however, is fragmented and incomplete.

This limited collective understanding of the ransomware landscape and the cryptocurrency payment system blunts the effectiveness of available tools to protect national security and limits private sector and federal government efforts to assist cybercrime victims. As Russia's invasion of Ukraine continues and Russia seeks to find ways around the international finance system, the need to address these shortfalls grows. Approximately 74 percent of global ransomware revenue in 2021 went to entities either likely located in Russia or controlled by the Russian government. Further, CISA and other federal agencies have warned that Russia's invasion of Ukraine could lead to additional malicious cyber activity, including ransomware attacks, in the United States. Therefore, as the report finds, prioritizing the collection of data on ransomware attacks and cryptocurrency payments is critical to addressing increased national security threats.

I. FINDINGS OF FACT AND RECOMMENDATIONS

FINDINGS OF FACT

1. **The federal government lacks comprehensive data on ransomware attacks and use of cryptocurrency in ransom payments.** The government largely relies on voluntary reporting of ransomware attacks and cyber extortion demands, which only captures a fraction of the attacks that occur. As of July 2021, the Cybersecurity and Infrastructure Security Agency (CISA), which was created in 2018 specifically to reduce risk to the nation's cyber and physical infrastructure, estimated that only about one quarter of ransomware incidents were reported.

2. **Current reporting is fragmented across multiple federal agencies.** Data on ransomware attacks is reported to numerous federal agencies including CISA, the FBI, and the Treasury Department's FinCEN, among others. These agencies do not capture, categorize, or publicly share information uniformly.

3. **Lack of reliable and comprehensive data on ransomware attacks and cryptocurrency payments limits available tools to guard against national security threats.** The lack of data on ransomware attacks and cryptocurrency ransom payments blunts the effectiveness of available tools for fighting ransomware attacks including U.S. sanctions, law enforcement efforts, and international partnerships, among other tools.

4. **Currently available data on ransomware attacks and cryptocurrency payments limits both private sector and federal government efforts to assist cybercrime victims.** The private sector and the federal government are not able to fully and effectively assist victims to prevent or recover from ransomware attacks without a comprehensive dataset on ransomware attacks, ransom demands, and payments. Such a dataset does not currently exist.

RECOMMENDATIONS

1. **The Administration should swiftly implement the new ransomware attacks and ransom payments reporting mandate.** CISA should complete the required rulemaking as soon as possible to implement the requirements in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 signed into law as part of the Consolidated Appropriations Act of 2022, which mandates incident reporting of substantial cyber-attacks and ransomware payments against critical infrastructure. Federal agencies should implement the requirement in the law to share all cyber incident reports with CISA to enable a consolidated view of incidents from across different sectors and reported under different regulatory regimes.

2. **The federal government should standardize existing federal data on ransomware incidents and ransom payments to facilitate comprehensive analysis.** Agencies should standardize how data from existing reporting requirements for ransomware incidents and ransom payments is organized and formatted across federal government agencies to enable more comprehensive information sharing and analysis.

3. **Congress should establish additional public-private initiatives to investigate the ransomware economy.** The federal government should promote public-private partnerships to research the ransomware economy, in particular, the interrelationships between cybercriminals who conduct or facilitate ransomware attacks and the financial structures facilitated by cryptocurrencies that sustain cybercriminals' illicit activities, including privacy coins. These partnerships should also examine ransomware infrastructure to help design and promote effective countermeasures.

4. **Congress should support information sharing regarding ransomware attacks and payments including crowdsourcing initiatives.** Congress and relevant agencies should consider ways to support partners within the private, nonprofit, and academic sectors seeking to expand the collection and organization of information on ransomware attacks including by examining federal funding options and sharing anonymized data regarding ransomware attacks and payments. In addition, government agencies should collaborate with partners to identify viable crowdsourcing initiatives to pool information regarding ransomware attacks and extortion payments.

II. BACKGROUND

On July 20, 2021, U.S. Senator Gary Peters, Chairman of the Senate Homeland Security and Governmental Affairs Committee, announced an investigation into the role that cryptocurrency plays in facilitating ransomware attack payments and the consequent escalation of ransomware attacks.[1] As a part of this investigation, staff conducted interviews with federal law enforcement and regulatory agencies as well as private companies that assist ransomware victims with ransom demands. Both federal agencies and private companies raised concerns regarding the lack of visibility into the full scope of ransomware threats and cryptocurrency ransom payments. Each of the interviewees advocated for increased data collection regarding illicit actors' methods and ransom payments to better understand the ever-evolving landscape of ransomware attacks and illicit uses of cryptocurrency.

A. Ransomware Attacks and Use of Cryptocurrency as Payment

Ransomware is an increasingly threatening and continually evolving form of cryptocurrency-enabled crime.[2] The origins of ransomware can be traced to the late 1980s.[3] By 2006, near universal access to the internet and online cash-equivalent instruments enabled increased anonymity and a more global reach, thereby creating new opportunities for profitable cybercrime. Geographic limitations tied to payment mechanisms and financial regulations, however, made it difficult to generate significantly large proceeds from ransomware attacks.[4] At the time, threat actors primarily used online payment systems such as Western Union and PayPal, among other methods, to receive ransom payments.[5] Although an alternative to banks, these payment systems engaged traditional depository financial institutions to facilitate the ransom payment transfer. In countries with anti-money laundering rules, *e.g.*, the United States,

---

[1] Senate Homeland Security and Governmental Affairs Committee, *Peters Announces Investigation Into Rise of Ransomware Attacks and How Cryptocurrencies Facilitate Cybercrimes* (July 20, 2021).

[2] Chainalysis, *The 2022 Crypto Crime Report* (Feb. 2022) (go.chainalysis.com/2022-Crypto-Crime-Report.html) (hereinafter "*The 2022 Crypto Crime Report*").

[3] Kaveh Waddell, *The Computer Virus That Haunted Early AIDS Researchers*, Atlantic (May 10, 2016) (https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/). In 1989, 20,000 AIDS researchers received floppy disks infected with the AIDS Trojan, *a.k.a.* PC Cyborg virus, disguised as a questionnaire to "help determine patients' risk of contracting AIDS." The ransom note demanded that a payment be made to a P.O. Box in Panama to retrieve access to files that were encrypted after use. *Id*.

[4] *See* Bart Custers, Jan-Jaap Oerlemans, and Ronald Pool, *Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies*, European Journal of Crime, Criminal Law and Criminal Justice (2020) (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3694282) and D. Y. Huang, et al., *Tracking Ransomware End-to-end*, IEEE Symposium on Security and Privacy (2018) (ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8418627).

[5] Bart Custers, Jan-Jaap Oerlemans, and Ronald Pool, *Laundering the Profits of Ransomware*, European Journal of Crime, Criminal Law and Criminal Justice (2020) (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3694282).

regulated financial institutions are generally required to notify authorities of suspicious transactions and conduct background screenings to detect potentially illicit transactions.[6]

In 2009, Bitcoin, a type of cryptocurrency, was released and its eventual use by cybercriminals as a preferred form of ransom payment drastically transformed the ransomware business model.[7] This decentralized monetary system was designed to remove barriers to the transfer of value and allow "online payments to be sent directly from one party to another without going through a financial institution."[8] The foundational technology of cryptocurrency—blockchain—consists of a distributed ledger that is managed by its users through a peer-to-peer system. Once a Bitcoin cryptocurrency transaction is authorized by network participants, the amount of funds transferred, a timestamp, and the bitcoin addresses are stored on the blockchain and made publicly available.[9] The public ledger makes available an exact and transparent order of events which is designed to enhance trust between participants and promote security. Thus, any individual can join the network and view a history of transactions.[10]

Starting in 2012, as the use of Bitcoin and other cryptocurrencies became more widespread, ransomware encryption techniques also grew along with expansion of the digital black market.[11] This further enabled the modern wave of ransomware attacks that rely on payment via cryptocurrencies.[12]

---

[6] 31 U.S.C. § 5311 – 5330; *see also* Bart Custers, Jan-Jaap Oerlemans, and Ronald Pool, *Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies*, European Journal of Crime, Criminal Law and Criminal Justice (2020) (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3694282); Paypal, *PayPal Anti-Money Laundering and Counter-Terrorist Financing Statement* (May 11, 2009) (www.paypal.com/us/webapps/mpp/ua/aml-full) (explaining that "PayPal has robust policies and procedures to detect, prevent and report suspicious activity" and conducts background screenings to comply with OFAC (Office of Foreign Asset Control) requirements, and global sanctions).

[7] Bitcoin is spelled with a capital letter when referring to the software and community, and with a lower letter when referring to the unit of currency.

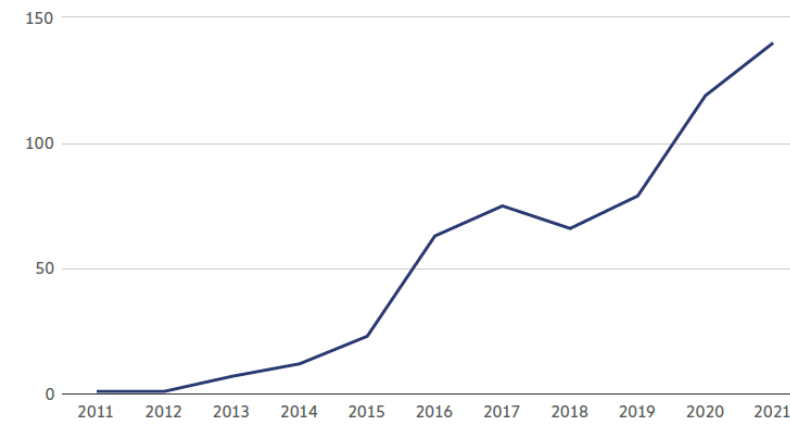
[8] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (bitcoin.org/bitcoin.pdf).

[9] Other cryptocurrency transactions make public similar information.

[10] *How to Read a Blockchain Transaction History*, Ledger (blog) (Sept. 11, 2020) (https://www.ledger.com/academy/how-to-read-a-blockchains-transaction-history).

[11] *See History of Ransomware*, CrowdStrike (June 21, 2021) (www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/); Aamir Lakhani, *Analyzing the History of Ransomware Across Industries*, Fortinet (blog) (May 17, 2021) (www.fortinet.com/blog/industry-trends/analyzing-the-history-of-ransomware-across-industries). *See also* Kurt Thomas, et al., *Framing Dependencies Introduced by Underground Commoditization*, Workshop on Economics of Information Security (2015) (elie.net/static/files/framing-dependencies-introduced-by-underground-commoditization/framing-dependencies-introduced-by-underground-commoditization-paper.pdf).

[12] *See History of Ransomware*, CrowdStrike (June 21, 2021) (www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/). *See also* Elie Bursztein, Luca Invernizzi, and Kylie McRoberts, *Unmasking the ransomware kingpins*, Elie (blog) (Oct. 2017) (https://elie.net/blog/security/unmasking-the-ransomware-kingpins/).



Source: *The 2022 Crypto Crime Report*.

Several characteristics of cryptocurrency, and particularly Bitcoin, make it one of the current ransom payment methods of choice for threat actors: large sums can be transferred more or less instantaneously worldwide; the system is decentralized and largely unregulated; it has a high level of flexibility; and the technology enables innovative approaches to maximize anonymity and make it increasingly harder for law enforcement agencies and regulators to track. In conversations with Committee staff, officials from the Department of Justice (DOJ) and the Treasury Department's Financial Crimes Enforcement Network (FinCEN) confirmed the correlation between cryptocurrency and the rise of modern ransomware attacks. As officials from DOJ told the Committee, "before cryptocurrency, ransomware attacks were difficult to monetize. With the availability of virtual currencies, however, criminals can collect ransoms much more easily. In addition, cryptocurrency payments are irreversible."[13]

The transparent nature of blockchain, however, also enables law enforcement agencies in some instances to track and interpret the flow of illicit cryptocurrency assets, to identify threat actors, and hold them accountable.[14] To make or receive a payment in bitcoin, a user must first create a Bitcoin wallet – a set of keys created using a device or program that sends and receives cryptocurrency, similar to a traditional wallet.[15] Each Bitcoin wallet contains a public key, used

[13] Letter from Peter Hyun, Acting Assistant Attorney General, Department of Justice, Letter to Chairman Peters (Apr. 29, 2022) (hereinafter "DOJ Letter"). In an interview with Committee staff, FinCEN also indicated that the agency had seen a correlation between the ease of being able to use and understand cryptocurrency, the speed of transactions, and the rise of ransomware attacks. Kevin O'Connor, Chief of Virtual Assets and Emerging Technology Section, Financial Crimes Enforcement Network, Interview with Senate Committee on Homeland Security and Governmental Affairs (July 20, 2021) (hereinafter "FinCEN O'Connor Interview").

[14] FinCEN O'Connor Interview.

[15] Jake Frankenfield, Amilcar Chavarria, and Katrina Munichiello, *Bitcoin Wallet*, Investopedia (Jan. 13, 2022) (www.investopedia.com/terms/b/bitcoin-

to receive transactions, and a private key, used to sign and send Bitcoin transactions, giving the user control over the bitcoins in that address. Bitcoin wallets do not need to be registered or associated with the person who creates them – thus making it difficult to identify the owner or user of any particular wallet. Ransomware actors will often create one cryptocurrency wallet per victim; wallets can be easily generated and are "fresh and new" for most ransomware victims.[16] Although hidden, the identity of cryptocurrency wallet address holders may sometimes be deduced by tracing the transfer of ransom payments across the blockchain.[17] Oftentimes, key information can be deduced from the point where traditional currency is used to purchase cryptocurrency—the "on-ramp"—and the final destination where the illicit cryptocurrency is converted back to traditional currency— the "off ramp".[18]

Threat actors regularly operate on the darknet, an encrypted network on the internet that has its own social networks, search engines, sites, forums and other platforms for communication and file transfer.[19] To access the darknet, users must use specific browsers, such as Tor browser, as this part of the web is inaccessible via traditional search engines, such as Google.[20] A key difference between the darknet and the part of the web that is visible to the average user, *i.e.*, the surface web or clearnet, is the degree of anonymity. Whereas sites and social networks on the clearnet may be able to establish the identity of a user as well as their IP address, the darknet is designed to be more anonymous and conceals IP addresses, making it difficult for internet activity to be traced back to the user.[21] Online black markets and underground web-forums where illicit actors connect with each other are often utilized to purchase and sell tools for cyber-attacks, including ransomware attacks.[22] These same markets and forums are also used to recruit ransomware actors, and are typically located on the darknet.[23]

---

wallet.asp#:~:text=A%20Bitcoin%20wallet%20is%20a,Bitcoin%20addresses%20and%20send%20transactions) (noting that "instead of storing physical currency, the wallet stores the cryptographic information used to access bitcoin addresses and send transactions").

[16] Kurtis Minder, Chief Executive Office, GroupSense, Interview with Senate Committee on Homeland Security and Governmental Affairs (Mar. 31, 2022) (hereinafter "Minder Interview").

[17] Bill Siegel, Chief Executive Officer, Coveware, Interview with Senate Committee on Homeland Security and Governmental Affairs (Dec. 2, 2021) (hereinafter "Siegel Interview").

[18] *See generally Crypto On and Off-Ramps – How and Where?*, Ledger (Jan. 19, 2022) (www.ledger.com/academy/crypto-on-and-off-ramps-say-what). Traditional currency is also referred to as fiat currency, real currency, or national currency. *Id*.

[19] Congressional Research Service, *Dark Web* (R44101) (Mar. 10. 2017).

[20] *Id*. Tor or "The Onion Router" is an anonymity network designed to obfuscate communications. *Id*.

[21] Kyle Chivers, *What does an IP address tell you and how it can put you at risk*, Norton (Apr. 23, 2021) (us.norton.com/internetsecurity-privacy-what-does-an-ip-address-tell-you.html). An Internet Protocol address (IP address) is a unique identifier that typically reveals the geolocation, *e.g.*, city, zip code, or area code, of the nearest internet service provider (ISP). The IP address changes each time a device is connected to a different Wi-Fi network or router. *Id*.

[22] *See* Department of Justice, *Department of Justice Launches Global Action Against NetWalker Ransomware* (Jan. 27, 2021) (www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware).

[23] Anthony M. Freed, *What is the Dark Web Ransomware Marketplace?*, Cyberreason (Oct. 19, 2021) (www.cybereason.com/blog/what-is-the-dark-web-ransomware-marketplace).

Cryptocurrency is the primary method of payment and money transmission in online black markets, to include those operating on the clearnet, as well as the darknet.[24] According to publicly available information from the U.S. Secret Service (hereinafter "Secret Service"), the widespread use of cryptocurrency enables transnational cybercrime, including ransomware for the following reasons:

> it provides a ready means for transnational criminals to convert to and from fiat currencies as well as transfer and launder proceeds of cyber-enabled crimes. Cyber criminals have additionally developed substantial networks of money mules and various digital money laundering services, such as over-the-counter brokers or exchange services and other unlicensed money services, to launder illicitly obtained funds.[25]

In conversations with Committee staff, FinCEN emphasized, "the law enforcement perspective is that we have had ransomware issues for years and we have serious issues with crimes on the darknet where cryptocurrency is really the only form of payment."[26] According to the Secret Service, cryptocurrency is increasingly almost exclusively the required method of payment demanded by ransomware attackers.[27]

B. Anatomy of a Ransomware Attack

Ransomware is a subset of malware—"an umbrella term for any malicious code or program that gives a threat actor explicit control over a system."[28] CISA describes ransomware

---

[24] Congressional Research Service, *Dark Web* (R44101) (Mar. 10. 2017); Email from United States Secret Service, Criminal Investigative Division, to Senate Committee on Homeland Security and Governmental Affairs (Apr. 14, 2022).

[25] United States Secret Service, *U.S. Secret Service Launches Cryptocurrency Awareness Hub* (Feb. 18, 2022) (www.secretservice.gov/newsroom/releases/2022/02/us-secret-service-launches-cryptocurrency-awareness-hub). "Money mules" refer to individuals who move illicit funds on someone's behalf typically to facilitate the laundering of illicit proceeds. *Money Mules Don't Be a Mule: Awareness Can Prevent Crime*, Federal Bureau of Investigation (accessed on Mar. 30, 2022) (www.fbi.gov/scams-and-safety/common-scams-and-crimes/money-mules). Over the counter (OTC) trades involve brokers acting on behalf of private parties who are seeking to trade immense volumes of cryptocurrency with enhanced privacy and anonymity. *See* Connor Dempsey, *How does crypto OTC actually work?*, Medium (Mar. 25, 2019) (medium.com/circle-research/how-does-crypto-otc-actually-work-e2215c4bb13). *See also* Rihonna Scoggins, *What an FBI Section Chief Has Learned Investigating Virtual Currencies*, Fraud Conference News (Nov. 17, 2021) (www.fraudconferencenews.com/home/2021/11/15/what-you-need-to-understand-about-virtual-currencies-nbsp) (stating that a majority of cryptocurrency transactions are facilitated through OTC desks); *see generally* Congressional Research Service, *Dark Web* (R44101) (Mar. 10. 2017) (discussing how bitcoin is used and preferred on the Dark Web).

[26] FinCEN O'Connor Interview.

[27] Email from United States Secret Service, Criminal Investigative Division, to Senate Committee on Homeland Security and Governmental Affairs (Apr. 14, 2022).

[28] Andy Patrizio, *Malware vs. ransomware: What's the difference?*, TechTarget (July 13, 2021) (whatis.techtarget.com/feature/Malware-vs-ransomware-Whats-the-difference#:~:text=Malware%20is%20an%20umbrella%20term,system%20and%20encrypts%20the%20data).

as "a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption."[29] An archetypal ransomware attack is described below and will resemble the diagram in Figure 1.[30]

Figure 1. Anatomy of a Ransomware Attack

Compiled by Senate Homeland Security and Governmental Affairs Committee, Majority.

1. **Reconnaissance**. The threat actor, often a third party affiliate, analyzes the victim's assets for weaknesses.

2. **Infiltration**. The ransomware infiltrates the victim's computer system via an attack vector, *e.g.*, social engineering tactics such as phishing or known vulnerabilities.

3. **Privilege escalation**. After gaining entry, the threat actor may attempt to escalate privileges on the device or pivot to other internal company systems with more sensitive data.

4. **Installation**. Once the threat actor has sufficient permissions, the ransomware is installed on the victim's computer to gain access to its files and systems.

5. **Exfiltration**. In some ransomware attacks, the threat actor "exfiltrates" or steals, the data in a process known as double extortion.[31] The threat actor then transfers the stolen data to storage servers accessible by the attacker.[32]

6. **Deployment and Encryption**. The threat actor then deploys the ransomware, executing malicious code to encrypt the victim's data.[33]

---

[29] Cybersecurity and Infrastructure Security Agency, Stop Ransomware (accessed on Feb. 21, 2022) (www.cisa.gov/stopransomware).

[30] *Ransomware vs. malware*, Box Communications (blog) (Oct. 27, 2021) (blog.box.com/ransomware-vs-malware).

[31] Janus Agcaoili, Miguel Ang, Earle Earnshaw, et. al., *Ransomware Double Extortion and Beyond: REvil, Clop, and Conti*, Trend Micro (June 15, 2021) (https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti).

[32] *Id.* While some ransomware attacks exfiltrate data (and may extort payment to prevent the release of that data), many of these attacks only encrypt the data. *Id.*

[33] McAfee, *What Is Ransomware?* (accessed Mar. 28, 2022) (www.mcafee.com/enterprise/en-us/security-awareness/ransomware.html).

7. **Ransom Demand**. After encryption is complete, the victim will see a message from attackers demanding a ransom (usually in cryptocurrency) in exchange for the decryption key to decrypt and allow access to the victim's files.[34] The ransomware often establishes a specific time frame during which victims must pay the ransom in order to decrypt the files, *e.g.* 24 to 48 hours, after which it threatens to either increase the ransom amount, destroy the files, or delete the decryption key. If the attack is a double extortion attack, the ransom demand would be, in addition to the decryption key, in exchange for the attacker deleting the exfiltrated files, under threat of making the files public in the event the ransom is not paid.[35]

While to date, ransom payments are most commonly made in Bitcoin, ransomware attackers also may demand payment in other cryptocurrencies such as Monero, a privacy coin. Such coins are cryptocurrencies that preserve additional anonymity beyond Bitcoin and other older cryptocurrencies "by obscuring the flow of money across their networks."[36]

[34] *Id*. Certain types of ransomware will leak a portion of stolen data prior to contacting the victim as a sort of ransom. *Id*.

[35] Coveware, *Quarterly Report: Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues* (Nov. 4, 2020) (https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report).

[36] Robert Stevens, *What Are Privacy Coins and Are They Legal?*, CoinDesk (accessed Jan. 10, 2022) (www.coindesk.com/learn/what-are-privacy-coins-and-are-they-legal).

After illicit actors gain access to a victim's computer system, the parties will typically follow the payment transaction steps depicted in Figure 2 and described below.[37]

Figure 2. Cyberextortion payment transactions

Source: *Spotlight on ransomware: Ransomware payment methods*, Emsisoft (blog) (Aug. 15, 2017).

1. Demand for ransom is made.

2. Victim may attempt to negotiate with the actors or refuse to make the payment.

3. If a victim decides to pay the ransom, they use traditional currency to purchase the demanded cryptocurrency, typically bitcoin.

4. Victim sends the ransom payment in cryptocurrency to the criminals at the digital wallet address specified in the ransom note or on a payment portal (often located on the darknet).

5. Criminals typically either "cash out", *i.e.*, exchange the cryptocurrency for traditional currency, or launder the cryptocurrency through cryptocurrency mixing services before "cashing out".

[37] Ransomware Task Force, *Combating Ransomware*, Institute for Security and Technology (Apr. 2021) (securityandtechnology.org/ransomwaretaskforce/report/).

C. U.S. Regulations, Illicit Uses of Cryptocurrency, and Ransomware Attacks

In the United States, cryptocurrency transactions are regulated under a patchwork of federal and state laws and regulations. No one regulatory agency has direct authority over virtual currencies. Further, there is no uniform definition for "cryptocurrency" under U.S. law. "Cryptocurrency" is often referred to as "virtual currency," "digital assets," "digital tokens," "cryptoassets," or "crypto."

Generally, at the federal level, the Securities and Exchange Commission (SEC) regulates the issuance of any digital asset that constitutes a security; the Commodity Futures Trading Commission (CFTC) exercises general anti-fraud and manipulation enforcement authority over cryptocurrency cash markets as a commodity in interstate commerce; the Internal Revenue Service (IRS) deems virtual currency to be property for tax purposes; the Office of the Comptroller of the Currency (OCC) regulates crypto-related activities in the banking industry; and FinCEN regulates certain uses of cryptocurrency in connection with money laundering and related financial crimes. The Bank Secrecy Act (BSA) and implementing regulations issued by FinCEN, discussed in more detail below, are the key anti-money laundering statutes and rules applicable to both traditional and virtual currency.

1. Bank Secrecy Act and Implementing Regulations

In 1970, Congress enacted the Currency and Foreign Transactions Reporting Act, commonly known as the BSA, to confront the threat of money laundering and related crimes.[38] The law establishes specific requirements for recordkeeping and reporting by private individuals, banks, and non-banking financial institutions to prevent malign actors from using U.S. financial institutions to obscure illicit funds. Subsequent laws enhanced and amended the BSA to provide additional tools to combat money laundering and to counter terrorism financing.[39]

In 2011, FinCEN, the federal agency that administers the BSA, issued regulations that have since been used to impose anti-money laundering requirements on the cryptocurrency industry.[40] In 2013, FinCEN issued interpretive guidance to clarify the applicability of the BSA and its implementing regulations to persons "creating, obtaining, distributing, exchanging,

[38] Pub. L. No. 91-508.

[39] *Id*. The BSA has been amended by the Title III of the USA PATRIOT Act of 2001 and the Anti-Money Laundering Act of 2020. *Id*. The USA PATRIOT Act—the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001" was enacted to enhance law enforcement investigatory tools to deter and punish terrorist acts in the United States and around the world. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, Pub. L. No. 107-56 (2001). In the 2021 National Defense Authorization Act (NDAA), Congress included significant reforms to the U.S. anti-money laundering (AML) regime. The NDAA includes the Anti-Money Laundering Act of 2020 (AMLA) and, within the AMLA, the Corporate Transparency Act (CTA). William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283 (2021).

[40] Pub. L. No. 91-508, as amended and 31 CFR § 1010.100(ff) (formerly 31 CFR § 103.11(uu)). *See also* 31 U.S.C. 310 (establishing FinCEN and requiring it to implement the recordkeeping, reporting, and other requirements of the BSA).

accepting, or transmitting virtual currencies."[41] The regulations clarify that "administrators" and "exchangers" are regulated as money service businesses.[42]

Pursuant to the BSA, a "money service business" (MSB) includes "money transmitters"— individuals and entities engaged in the transfer of funds, including the transmission of "value that substitutes for currency" to another location or person.[43] Per FinCEN guidance issued in May 2019, "value that substitutes for currency" includes convertible virtual currency (CVC) such as Bitcoin.[44] In 2020, the Cyber-Digital Task Force within DOJ published a cryptocurrency enforcement framework in which it reiterates that,

> [i]n the United States, individuals and entities that offer money transmitting services involving virtual assets, such as cryptocurrency exchanges and kiosks, as well as certain issuers, exchangers, and brokers of virtual assets, are considered MSBs.[45]

Thus, MSBs that engage in the transfer of cryptocurrency payments subject to U.S. jurisdiction must establish and maintain an anti-money laundering program, comply with suspicious activity and currency transaction reporting rules, among other BSA requirements for MSBs.[46] With few exceptions, they must also register with FinCEN.[47]

Note, however, certain business models involving CVC transactions can be exempt from "money transmitter" status and therefore are not subject to BSA anti-money laundering

---

[41] Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (FIN-2013-G001) (Mar. 18, 2013).

[42] *Id*. (defining "exchanger" as "a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency" and defines "administrator" as "a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency").

[43] Pub. L. No. 91-508, as amended and 31 CFR § 1010.100(ff) (formerly 31 CFR § 103.11(uu)). *See also* 31 U.S.C. 310 (establishing FinCEN and requiring agency to implement the recordkeeping, reporting, and other requirements of the BSA, as well as disseminating information to appropriate law enforcement agencies)

[44] Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (FIN-2019-G001) (May 9, 2019) (defining CVCs as a "type of virtual currency that either has an equivalent value as currency, or acts as a substitute for currency").

[45] Department of Justice, *Cryptocurrency: Enforcement Framework* (Oct. 2020).

[46] *See* 31 CFR § 1022.210 (requiring for MSBs to establish and maintain an anti-money laundering program); 31 CFR § 1022.310 (requiring for MSBs to file Currency Transaction Reports); 31 CFR § 1022.320 (requirement for MSBs to file Suspicious Activity Reports, other than for check cashing); 31 CFR § 1010.415 (requiring certain MSBs to verify the identity of the customer and create and maintain a record of each currency purchase between $3,000 and $10,000, inclusive); 31 CFR § 1010.410(e) and (f) (making rules applicable to certain transmittals of funds). *See also* Financial Crimes Enforcement Network, *BSA Requirements for MSBs* (accessed on May 3, 2022) (https://www.fincen.gov/bsa-requirements-msbs).

[47] *See* 31 CFR 1022.380. *See also* Financial Crimes Enforcement Network, Money Services Business (MSB) Registration (accessed Mar. 31, 2022).

requirements.[48] For instance, an individual or an entity that merely provides the "delivery, communication, or network access services used by a money transmitter to support money transmission services" is not subject to BSA regulatory requirements.[49] Under this exemption, CVC trading platforms that merely enable buyers and sellers to connect with each other are not subject to BSA rules.[50] Additionally, under the "integral services" exemption, businesses that provide services other than money transmission services, and which accept and transmit CVC as an integral part of providing such services, do not generally have to meet the BSA anti-money laundering requirements.[51] Ultimately, whether a person is a money transmitter under the BSA depends on the "facts and circumstances" of each case.[52]

Importantly, foreign-based MSBs that conduct activities within the United States must register with FinCEN as an MSB, and comply with anti-money laundering program, recordkeeping, monitoring, and reporting requirements. This is true even if the MSB does not have a physical presence in the U.S.[53] FinCEN specifically noted that this rule seeks to address the globalized nature of the internet, "the Internet and other technological advances make it increasingly possible for persons to offer MSB services in the United States from foreign locations."[54] Thus, foreign-located MSBs that provide services to persons in the United States such as sending virtual currency to, or receiving virtual currency from, third parties through the MSB, must comply with the BSA.[55]

---

[48] 31 CFR § 1010.100(ff)(5)(ii). *See also* Financial Crimes Enforcement Network, *Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform* (FIN-2014-R011) (Oct. 27, 2014).

[49] 31 CFR § 1010.100(ff)(5)(ii)(A). *See also* Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (FIN-2019-G001) (May 9, 2019).

[50] The trading platform becomes a money transmitter if it also facilitates trades as an intermediary. Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (FIN-2019-G001) (May 9, 2019).

[51] Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (FIN-2019-G001) (May 9, 2019). *See also* 2011 MSB Final Rule, 76 FR at 43594 (stating "persons that sell goods or provide services other than money transmission services, and only transmit funds as an integral part of that sale of goods or provision of services, are not money transmitters").

[52] 31 CFR § 1010.100(ff)(5)(ii); Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (FIN-2019-G001) (May 9, 2019).

[53] Financial Crimes Enforcement Network, *Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses*, 76 FR 43585 (July 21, 2011) (final rule); Financial Crimes Enforcement Network, *Foreign-Located Money Service Businesses* (FIN-2019-A001) (Feb. 15, 2012). The 2011 rule revised FinCEN regulations such that an entity qualifies as an MSB based on its activity within the United States, not its physical presence. The final rule states that the definition of an MSB includes, "[a] person wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the United States." *Id*.

[54] Financial Crimes Enforcement Network, *Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses*, 76 Fed. Reg. 43585 (July 21, 2011) (final rule).

[55] Financial Crimes Enforcement Network, *Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses*, 76 Fed. Reg. 43585 (July 21, 2011) (final rule).

2. Federal Reporting Requirements for Transmitters of Virtual Currency

Administrators and exchangers, as defined by the FinCEN regulations, of virtual currency become money transmitters when they either exchange "traditional currency to cryptocurrency" or exchange "one cryptocurrency to another cryptocurrency."[56] Like brick and mortar financial institutions, such money transmitters must collect, keep, and report to authorities details regarding certain transactions involving cryptocurrency under the BSA.[57] This is true regardless of whether the money transmitter is operating in traditional currency, nonanonymized CVC, or anonymity-enhanced CVC (AEC). According to FinCEN, "a money transmitter cannot avoid its regulatory obligations because it chooses to provide money transmission services using anonymity-enhanced CVC" or with an "added feature of concealing the source of the transaction."[58]

The BSA's reporting requirements provide law enforcement and regulators with a certain degree of visibility into suspicious transactions and certain transactions involving more than $10,000 in currency. Specifically, money transmitters that handle cryptocurrency pursuant to the BSA must meet the following reporting requirements:

- **Suspicious Activity Reports**: Money transmitters that handle virtual currency must file "Suspicious Activity Reports" (SARs) for "suspicious" transactions that involve or aggregate funds of $2,000 or more.[59] A transaction is "suspicious" where the individual or entity "knows, suspects, or has reason to suspect that a transaction" (or a pattern of transactions) either: i) "involves funds derived from illegal activity"; ii) is designed to evade any BSA regulations; iii) has no "business or apparent lawful purpose"; or iv)

[56] Department of Justice, *Cryptocurrency: Enforcement Framework* (Oct. 2020); *see* Bank Secrecy Act, 31 U.S.C. 5311-5330 (1970). FinCEN regulations apply to exchangers regardless of whether they are directly brokering transactions or are parties to transactions; Financial Crimes Enforcement Network, *Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System* (FIN-2014-R012) (Oct. 27, 2014); Financial Crimes Enforcement Network, *Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform* (FIN-2014-R011) (Oct. 27, 2014).

[57] *See generally* 31 C.F.R. Part 1022 (identifying BSA requirements applicable to MSBs) and Department of Justice, *Cryptocurrency: Enforcement Framework* (Oct. 2020). Note unlike banking financial institutions, MSBs are not required to implement "Know Your Customer" programs (KYC) under the BSA. However, MSBs must implement an anti-money laundering compliance program that is "reasonably designed to prevent the [MSB] from being used to facilitate money laundering and the financing of terrorist activities." The program must be "commensurate with the risks posed by the location and size of, and the nature and volume of the financial services provided…." 31 CFR §1022.210; *see also* Letter from Charles P. Rettig, Department of the Treasury, Internal Revenue Service to Senator Margaret Wood Hassan (Dec. 21, 2021) (https://www.hassan.senate.gov/imo/media/doc/crypto.pdf).

[58] Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (FIN-2019-G001) (May 9, 2019).

[59] *See* 31 CFR Chapter X; Financial Crimes Enforcement Network, *Money Services Business (MSB) Suspicious Activity Reporting* (accessed on Mar. 30, 2022) (www.fincen.gov/money-services-business-msb-suspicious-activity-reporting).

"involves the use of the financial institution to facilitate criminal activity."[60] To comply with the BSA, the MSB must have an adequate SAR program that "requires identifying a business purpose for the subject transactions and a legitimate source of funds."[61] Financial institutions are not limited to the circumstances above and may voluntarily file a report alerting FinCEN of a possible violation of any law or regulation in connection with a suspicious transaction.[62]

- **Currency Transaction Reports**: Money transmitters that handle virtual currency must file "Currency Transaction Reports" (CTRs) on transactions involving more than $10,000 in currency conducted by, or on behalf of, one person in a single day.[63] This includes multiple transactions that aggregate to more than $10,000. The report must include personal identification information regarding the individual conducting the transaction. Note CTR requirements are triggered only by physical transfers of currency exceeding $10,000.[64] Accordingly, a ransomware payment may trigger a CTR filing if the victim used more than $10,000 in physical cash to obtain cryptocurrency for the payment. Similarly, cashing out of illicit ransom proceeds of more than $10,000 at a cryptocurrency kiosk may trigger the CTR requirement.

3. Application of BSA and FinCEN Regulations Within the Context of Ransomware Attacks

[60] 31 CFR §1022.320. *See* Financial Crimes Enforcement Network, *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments* (FIN-2020-A006) (Oct. 1, 2020) (providing a list of ransomware-related financial red flag indicators to assist financial institutions in detecting suspicious transactions associated with ransomware attacks). *See also* Financial Crimes Enforcement Network, *FinCEN Penalizes Peer-to-Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws* (April 18, 2019) (www.fincen.gov/news/news-releases/fincen-penalizes-peer-peer-virtual-currency-exchanger-violations-anti-money).

[61] Letter from Charles P. Rettig, Department of the Treasury, Internal Revenue Service to Senator Margaret Wood Hassan (Dec. 21, 2021) (www.hassan.senate.gov/imo/media/doc/crypto.pdf)

[62] Financial Crimes Enforcement Network, *FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Instructions* (Oct. 2012) (https://www.fincen.gov/sites/default/files/shared/FinCEN%20SAR%20ElectronicFilingInstructions-%20Stand%20Alone%20doc.pdf) and Financial Crimes Enforcement Network, *Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021* (June 30, 2021) (www.fincen.gov/sites/default/files/shared/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf).

[63] 31 CFR § 1010.330; *see also* Financial Crimes Enforcement Network, *FinCEN Penalizes Peer-to-Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws* (Apr. 18, 2019) (www.fincen.gov/news/news-releases/fincen-penalizes-peer-peer-virtual-currency-exchanger-violations-anti-money); Financial Crimes Enforcement Network, *Notice to Customers: A CTR Reference Guide* (accessed on Apr. 1, 2022) (www.fincen.gov/sites/default/files/shared/CTRPamphlet.pdf). "Currency" is defined as, "[t]he coin and paper money of the United States or any other country, which is circulated and customarily used and accepted as money." Financial Crimes Enforcement Network, *FinCEN Form 104: Currency Transaction Report* (Mar. 2011) (https://www.irs.gov/pub/irs-tege/fin104_ctr.pdf#page=3).

[64] Transfers by means of bank check, bank draft, wire transfer, or other written orders do not trigger CTR obligations. Financial Crimes Enforcement Network, *FinCEN Form 104: Currency Transaction Report* (Mar. 2011) (https://www.irs.gov/pub/irs-tege/fin104_ctr.pdf#page=3).

With respect to pursuing ransomware attackers, FinCEN told the Committee that the BSA reporting requirements are critical for assisting law enforcement:

> The requirements of the BSA — registration with FinCEN, maintaining an effective AML program, and meeting recordkeeping and reporting requirements — help shed light on where transactions may originate and where they are, or are likely to be, cashed out. This assists law enforcement pursue ransomware attackers. Ultimately, ransomware actors have to cash out, and the BSA establishes rules for the financial institutions that facilitate these transactions.[65]

The following table illustrates how anti-money laundering regulations apply to certain cryptocurrency business models and other businesses that ransomware attackers and/or victims may use to convert, send, receive, or cash out, traditional or virtual currency in connection with a ransom payment.[66] Specifically, the table identifies which entities meet the definition of an MSB and thus, are subject to FinCEN rules for money laundering prevention, *e.g.*¸ implementation of a risk-based AML program, registration with FinCEN, SAR & CTR reporting, and recordkeeping. Whether a party is regulated pursuant to the BSA, however, depends on the "facts and circumstances" of a particular case. The information below is general in nature and is provided to illustrate the complexity and myriad of players that may be involved in a ransom payment process.

[65] FinCEN O'Connor Interview.

[66] The information in the table was compiled by Majority staff on the Senate Homeland Security and Governmental Affairs Committee.

BUSINESS / TRADING PLATFORM	DESCRIPTION	RANSOMWARE-RELATED EXAMPLE(S)	MSB (Y/N)
CVC Exchange	- Acts as middleman between buyers and sellers - Enables trade of fiat-to-crypto or crypto-to-crypto	Victim sets up account, transmits real currency to the account to purchase CVC and requests that the exchange send the ransom in CVC to perpetrator's digital wallet address	MSB: Y (may be exempt if merely connects buyers and sellers)
Peer-to-Peer (P2P) Exchanger	- Individual operates as a P2P exchange "whether or not on a regular basis" - Engages in money transmission	Victim uses P2P exchanger to obtain and send large CVC amount to settle ransom or attacker uses P2P exchanger to launder illicit ransom proceeds	MSB: Y (may be exempt if trades are conducted on an infrequent basis and not for profit)
Wallet Host	- Third-party, *e.g.*, CVC exchange, hosts users' digital currency wallet - Host has control over private keys and trades funds on behalf of user	Victim requests that wallet host send the demanded ransom amount in CVC from hosted wallet to perpetrator's address	MSB: Y
Unhosted Wallet	- Individual self-hosts digital wallet on personal device - Typically used in P2P exchanges	Attacker uses unhosted wallets to quickly and covertly transfer large sums of money	MSB: N (if used for personal purchases without third-party authorization) Rule proposed in Dec. 2020 would create specific rules for banks and MSBs involved in unhosted wallets transactions; scheduled for Sept. 2022 if FinCEN follows through
Digital Forensic Incident Response (DFIR) Firm	- Assists victims with responding to cyber-attacks - May facilitate ransom payments to perpetrators	DFIR firm handles the conversion of client's real currency to CVC and transfers CVC to perpetrator's designated account	MSB: Y (must receive and transmit value) (integral exemption may apply)
Over-the-counter (OTC) Desk	- Engages in purchase and sale of CVC on behalf of party without middleman - Enables transfer of large CVC amounts with added anonymity	Victim uses OTC platform to exchange significant sums of real currency for CVC to pay ransom or attacker uses noncompliant OTC platform to launder illicit proceeds	MSB: Y
Virtual Currency Kiosk / ATM	- Standalone machine in retail stores - Used by owner to accept fiat from a customer and transmit the same value in CVC (or vice versa)	Attacker uses kiosk known to have weak customer identification standards or a noncompliant kiosk to cash out illicit funds	MSB: Y (kiosk owner qualifies; not required to report kiosk's location or specific kiosks)
Transmitter of Anonymity-enhanced CVC (AEC)	Transmits: a) CVC payment structured to conceal public information or b) CVC specifically engineered to prevent tracing	Attacker demands payment in Monero	MSB: Y
Mixer / Tumbler	Provides CVC anonymizing services and are in the business of transmitting money	Attacker uses service to launder illicit funds	MSB: Y (if transacting CVC exchanges)

Foreign-based MSB	Conducts business within the U.S. and likely does not have a U.S. location	Attacker uses MSB located in foreign country with little or no AML requirements to retrieve ransom from U.S.-based victim	MSB: Y
Darknet Marketplace	Marketplaces that facilitate CVC transactions	Facilitates ransomware purchase in CVC	MSB: Y

The following provides examples of scenarios where existing BSA regulations enable financial regulators and law enforcement to have visibility into a ransomware attack, in order of likelihood. These scenarios focus on the application of the BSA regulations to ransomware attacks and do not take into account an attack being reported in public sources, an attack being made public through litigation, state incident or breach reporting with public disclosures, law enforcement authorities to investigate and identify cyber-crimes, national security capabilities to identify foreign threats, or other regulatory regimes where victims are required to report cybersecurity incidents, including ransomware attacks.[67]

- **Most likely**. A ransom payment transaction of more than $2,000 is made and at least one entity involved in the transaction is regulated pursuant to the BSA. The regulated entity chooses to comply with FinCEN regulations. The entity correctly identifies the transaction as suspicious and files a SAR.[68]

- **Less likely**. A ransom payment transaction of more than $2,000 is made. The mode of transfer used to facilitate the transaction either is not regulated by the BSA or the counterparties and/or regulated entities choose not to comply with anti-money laundering regulations. The likelihood also decreases if the accounts used throughout the ransom payment process are primarily unhosted or a regulated entity fails to identify suspicious transactions. In this case, law enforcement or regulators may not become aware of the ransomware attack or ransom payment.

- **Least likely**. No ransom payment transaction occurs or a ransom payment transaction totaling less than $2,000 is made. The likelihood that law enforcement or regulators will become aware of the attack is highly unlikely based solely on BSA regulations.

[67] Different critical infrastructure sectors require the reporting of cybersecurity incidents at various thresholds, as does the SEC for publicly traded companies. *E.g.*, Transportation Security Administration, *Security Directive: Enhancing Pipeline Cybersecurity* (Security Directive Pipeline-2021-01) (May 28, 2021) (expiring on May 28, 2022) and Department of Homeland Security, *Ratification of Security Directive*, 86 Fed. Reg. 38209 (July. 20, 2021) (ratification of directive) and 17 CFR § 229, 249 (requiring public companies to report material cybersecurity risks and incidents that trigger disclosure obligations).

[68] *See* Financial Crimes Enforcement Network, *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments* (FIN-2020-A006) (Oct. 1, 2020) (providing a list of ransomware-related financial red flag indicators to assist financial institutions in detecting suspicious transactions associated with ransomware attacks).

4. U.S. Sanctions Policy

Ransomware victims (or agents working on their behalf) that decide to make a ransom payment in cryptocurrency must comply with U.S. sanctions laws and regulations.[69] The Department of Treasury's Office of Foreign Assets Control (OFAC) generally prohibits U.S. persons from engaging in business with individuals and entities on the agency's Specially Designated Nationals and Blocked Persons List (SDN List). Additionally, in most sanctions programs, any transaction, including by a non-U.S. person, that causes a U.S. person to violate the sanctions prohibitions, is also prohibited. Accordingly, parties must screen cryptocurrency transactions against OFAC's SDN list and undertake appropriate steps to prevent the transfer of CVC to sanctioned persons or jurisdictions.[70]

On September 21, 2021, OFAC issued an updated advisory to highlight the sanctions risks associated with ransomware payments and the proactive steps companies that assist victims of ransomware can take to mitigate such risks.[71] The guidance emphasizes that a person subject to U.S. jurisdiction may be held liable even if they did not have reason to know that the transaction was prohibited.[72]

D. Compliance

Due to the level of real or perceived regulatory and law enforcement scrutiny associated with compliant, regulated financial institutions, criminals frequently opt to enlist the services of financial institutions that do not conduct any meaningful anti-money laundering checks.[73] This continues to be the case in the cryptocurrency space. In particular, the ever-increasing demand for criminals to convert or cash out their illicitly acquired cryptocurrency – especially in the context of ransomware payments – has resulted in the rise of a host of exchanges, OTC brokers, unlicensed MSBs, and professional laundering platforms that conduct little to no inquiries into transactions or transactional counterparties and therefore are criminal in design.[74]

In an interview with Committee staff, Kevin O'Connor, Chief of Virtual Assets and Emerging Technology Section at FinCEN, stressed that the key to addressing the use of cryptocurrency in money laundering is ensuring compliance with BSA requirements for regulated entities. O'Connor told the Committee,

---

[69] *See* Department of Treasury, Questions on Virtual Currency (accessed May 16, 2022) (https://home.treasury.gov/policy-issues/financial-sanctions/faqs/560); Office of Foreign Assets Control, *Sanctions Compliance Guidance for the Virtual Currency Industry* (Oct. 2021) (https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf).

[70] Financial Crimes Enforcement Network, *Advisory on Illicit Activity Involving Convertible Virtual Currency* (FIN-2019-A003) (May 9, 2019).

[71] Department of Treasury, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Sep. 21, 2021) (home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf).

[72] *Id.*

[73] Email from United States Secret Service, Criminal Investigative Division, to Senate Committee on Homeland Security and Governmental Affairs (Apr. 14, 2022).

[74] *Id.*

> I think that is one of the reasons it is important to ensure that financial institutions, like virtual asset service providers, comply with the BSA because they are required to verify customer identity and maintain records and information. If financial institutions do not comply with these requirements it will make identifying illicit activity and disrupting bad actors more difficult. When you start looking at decentralized finance, you have to ask how U.S. law enforcement and regulators are going to collect and obtain the same information under the existing regulatory scheme.[75]

O'Connor highlighted compliance concerns with respect to peer-to-peer transactions, foreign-located MSBs, and professional money laundering services, stating that,

> Three examples where we see a greater degree of noncompliance are individual Peer-to-Peer exchangers, foreign-located MSBs, and cryptocurrency mixing services. FinCEN has observed that individual Peer-to-Peer exchangers are less likely to be registered with FinCEN and less likely to meet recordkeeping and reporting requirements under the BSA. We also see noncompliance with foreign-located MSBs that do business in whole or substantial part in the United States. FinCEN has been clear that these financial institutions have obligations under the BSA and its implementing regulations. For example, FinCEN—in coordination with law enforcement—took action against BTC-e, a Russia-based virtual asset service provider that did business in the U.S. and was cashing out 95 percent of ransomware proceeds at the time according to open source reporting. With respect to professional money laundering services like mixers and tumblers, FinCEN's enforcement action against the mixing service Helix highlighted the existing requirements currently imposed on these types of entities as financial institutions under the BSA. The good news is that, overall, we are seeing greater compliance by virtual asset service providers and as a result, more suspicious activity reports being filed with FinCEN.[76]

Similarly, senior staff at SEC's Strategic Hub for Innovation and Financial Technology (FinHub), told the Committee that Bitcoin markets will typically register with FinCEN and states for anti-money laundering purposes. However, many secondary trading platforms are not in compliance.[77] When a business fails to register with the proper regulatory authority, the SEC

---

[75] FinCEN O'Connor Interview.

[76] *Id. See also* Financial Crimes Enforcement Network, *In Matter of: BTC-e a/k/a Canton Business Corporation and Alexander Vinnik Citation* (No. 2017-03) (July 26, 2017) (assessment of Civil Money Penalty); Catalin Cimpanu, *95% of All Ransomware Payments Were Cashed out via BTC-e Platform*, Bleeping Computer (July 27, 2017) (https://www.bleepingcomputer.com/news/security/95-percent-of-all-ransomware-payments-were-cashed-out-via-btc-e-platform/); Financial Crimes Enforcement Network, *In the Matter of: Larry Dean Harmon d/b/a Helix* (No. 2020-2).

[77] Strategic Hub for Innovation and Financial Technology, Securities and Exchange Commission, Interview with Senate Committee on Homeland Security and Governmental Affairs (Sept. 9, 2021).

interviewee emphasized that there is a "huge gap in oversight."[78] In terms of anti-money laundering regulation and enforcement, the interviewee further stated, under these circumstances "the most serious issues are no recordkeeping and reporting" which means that "sometimes [it's impossible to] figure out who is running the platform."[79] This concern is particularly growing as transactions move into the decentralized financial (DeFi) space, an emerging financial technology that builds upon and expands the decentralized nature of Bitcoin and its blockchain.[80]

Cryptocurrencies' global nature, decentralized structure, speed of payment transfers and irreversibility, as well as opportunities for enhanced privacy and anonymity can be used in multiple ways by threat actors to facilitate non-compliance. According to FinCEN, some CVCs "appear to be designed with the express purpose of circumventing anti-money laundering/countering the financing of terrorism controls."[81] In other cases, unregistered entities may misrepresent the nature of their business to conceal their money transmission activity and avoid compliance.[82] As described by FinCEN above, many foreign-located MSBs that are subject to the BSA fail to adhere to anti-money laundering requirements and frequently facilitate payments in and out of the United States for illicit actors.[83] OFAC has also taken action against certain individuals for violating OFAC regulations and exchanging cryptocurrencies into traditional currency on behalf of ransomware actors.[84]

E. Recent Ransomware Attacks

In recent years, ransomware attack victims have increasingly targeted critical infrastructure, including hospitals, school systems, local, state, and federal government agencies, as well as major utilities including the water and energy sector. In 2021, ransomware attacks impacted at least "2,323 local governments, schools and healthcare providers" in the United States.[85] As detailed below, this number likely drastically underestimates the actual number of

[78] *Id*.

[79] *Id*.

[80] *Id*.

[81] Financial Crimes Enforcement Network, *Advisory on Illicit Activity Involving Convertible Virtual Currency* (FIN-2019-A003) (May 9, 2019).

[82] *Id*.

[83] *See In the matter of BTC-E a/k/a Canton Business Corporation and Alexander Vinnik*, Financial Crimes Enforcement Network (2017-03) (July 26, 2017). In January 2017, FinCEN assessed civil money penalties against BTC-e (a.k.a. Canton Business Corporation), a foreign-located money transmitter conducting business in the United States, and its alleged owner and operator, Alexander Vinnik, for failure to comply with anti-money laundering regulations. The MSB "attracted and maintained a customer base that consisted largely of criminals who desired to conceal proceeds from crimes such as ransomware." *Id*.

[84] Department of Treasury, *Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses* (Nov. 28, 2018) (home.treasury.gov/news/press-releases/sm556). On November 28, 2018, OFAC designated two Iranian individuals on the SDN list for exploiting illicit finance vulnerabilities in the cyber space and weak anti-money laundering controls. The individuals assisted with the exchange of bitcoin ransom payments into Iranian rial on behalf of Iranian ransomware attackers. *Id*.

[85] Emsisoft Malware Lab, *The State of Ransomware in the US: Report and Statistics 2021*, Emsisoft (blog) (Jan. 18, 2022) (blog.emsisoft.com/en/40813/the-state-of-ransomware-in-the-us-report-and-statistics-2021/).

attacks.[86] Victims also included police departments and manufacturing facilities, among many others.[87]

Ransomware attacks may generate significant losses and damages for victims by causing widespread system outage, economic loss, and reputational damage. Ransomware attackers have increasingly targeted supply chains, including those within critical infrastructure. In some cases, the attacks resulted in supply chain paralysis, causing collateral damage to businesses and customers and creating significant national security risks. Recent attacks include:

- **Education Sector**: In 2020, there were 50 documented instances of publicly reported ransomware attacks against U.S. public K-12 school districts across 25 different states.[88] Certain attackers took sensitive data, such as personal data of students and educators, and threatened to release the data if their ransom demands were not met. The attackers exposed personal information of at least 560,000 students and 56,000 staff in seven school districts. Reports claim that certain extortion demands exceeded $1 million.[89] Fifteen school districts across 13 states had closures and class cancellations as a result of ransomware attacks, a figure that was three times as high as in 2019.[90]

- **Health and Public Health Sector**: In 2021, malign actors targeted at least 68 healthcare providers including multiple hospitals and multi-hospital health systems. The impacted organizations operated a total of 1,203 sites.[91] These attacks can significantly impact patient care, such as preventing use of electronic health records, preventing staff from knowing which patients were scheduled for appointments, delaying surgeries, or forcing cancer patients to go elsewhere for radiation treatment.[92]

---

[86] Emsisoft Malware Lab, *The State of Ransomware in the US: Report and Statistics 2021*, Emsisoft (Blog) (Jan. 18, 2022) (blog.emsisoft.com/en/40813/the-state-of-ransomware-in-the-us-report-and-statistics-2021/). The estimated attacks "do not take into account attacks on third party service and solution providers that impacted the public sector," among other attacks. *Id*.; *see also* Tara Seals, *Kronos Ransomware Outage Drives Widespread Payroll Chaos*, threatpost (blog) (Dec. 13, 2021) (threatpost.com/kronos-ransomware-outage-payroll-chaos/176984/).

[87] Senate Committee on the Judiciary, Testimony Submitted for the Record of Executive Assistant Director for Cybersecurity Eric Goldstein, Cybersecurity and Infrastructure Agency, *Hearing on America Under Cyber Siege: Preventing and Responding to Ransomware Attacks*, 117th Cong. (July 27, 2021) (S. Hrg. 117-XX).

[88] Douglas A. Levin, *The State of K-12 Cybersecurity: 2020 Year in Review*, K-12 Cybersecurity Resource Center and the K12 Security Information Exchange (Mar. 10, 2021) (k12cybersecure.com/wp-content/uploads/2021/03/StateofK12Cybersecurity-2020.pdf).

[89] *Id*.

[90] *Id*.

[91] Emsisoft Malware Lab, *The State of Ransomware in the US: Report and Statistics 2021*, Emsisoft (blog) (Jan. 18, 2022) (blog.emsisoft.com/en/40813/the-state-of-ransomware-in-the-us-report-and-statistics-2021/); *see also* HHS Cybersecurity Program, *Ransomware Trends 2021* (June 3, 2021) (www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf).

[92] Stacy Weiner, *The growing threat of ransomware attacks on hospitals*, Association of American Medical Colleges (July 20, 2021) (https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals).

- **Colonial Pipeline**: On May 7, 2021, Colonial Pipeline, which supplies close to half of all fuel consumed on the East Coast, including gasoline, diesel, and jet fuel, was the victim of a ransomware attack that prompted the operator to shut the pipeline down for five days.[93] Colonial Pipeline paid a ransom of 75 bitcoin (about $4.4 million) to obtain a decryption key from the hackers which was expected to help restore access to its systems. However, the decryption tool was exceedingly slow, forcing the company to rely on its business continuity planning tools to bring back operational capacity. It is believed that the attackers also threatened to release 100 gigabytes of stolen data had the ransom not been paid.[94] On June 7, 2021, DOJ, in collaboration with private industry, retrieved 63.7 bitcoins of the original ransom payment, approximately $2.3 million.[95]

- **Kaseya Virtual System Administrator ("Kaseya VSA")**: On July 2, 2021, a sophisticated supply chain ransomware attack leveraged a vulnerability in Kaseya VSA software, which is used by managed IT service providers with a large amount of small- to medium-sized businesses. Attackers exploited a vulnerability in the VSA software to distribute malicious updates containing ransomware to customers, resulting in service outages for an estimated 800 to 1,500 companies. As publicly reported, Kaseya obtained a decryption key from the FBI that successfully recovered access to files that were encrypted during the ransomware attack.[96] The company did not pay the demanded $70 million ransom.

---

[93] Sara Morrison, *How a major oil pipeline got held for ransom*, Vox Recode (June 8, 2021) (www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices). Colonial Pipeline was concerned that the ransomware attackers might have obtained information allowing for future attacks to be launched against vulnerable parts of the pipeline. The closures were aimed at preventing the spread of ransomware to other parts of the systems. *Id.*

[94] *Hackers Breached Colonial Pipeline Using Compromised* Password, Bloomberg (June 4, 2021) (www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password).

[95] Sara Morrison, *How a major oil pipeline got held for ransom*, Vox Recode (June 8, 2021) (www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices); *Hackers Breached Colonial Pipeline Using Compromised* Password, Bloomberg (June 4, 2021) (www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password); Department of Justice, *Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside* (June 7, 2021) (www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside).

[96] The FBI had obtained a decryption key to restore access to the victims' locked computers; however, the agency waited three weeks prior to providing the key to Kaseya. Certain analysts estimate that the victims, which included schools, hospitals and a small town in Maryland, could have saved millions of dollars in recovery costs with earlier access to the decryption key. According to public reports, the FBI withheld the key, with the agreement of other federal agencies, because it was planning to carry out an operation to disrupt the hackers, a group known as REvil, and the bureau did not want to tip them off. *FBI had a key to help Kaseya ransomware victims but delayed using* it, Washington Post (Sep. 21, 2021) (www.washingtonpost.com/politics/2021/09/21/fbi-had-key-help-kaseya-ransomware-victims-delayed-using-it/). *See also* Department of Justice, *Ukrainian Arrested and Charged with Ransomware Attack on Kaseya* (Nov. 8, 2021) (www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya) and Department of Justice, *Sodinokibi/REvil Ransomware Defendant Extradited to United States and Arraigned in Texas* (Mar. 9, 2022) (www.justice.gov/opa/pr/sodinokibirevil-ransomware-defendant-extradited-united-states-and-arraigned-texas).

Ransomware actors reap astounding profits from victims' losses. Chainalysis, a cryptocurrency analysis contractor for the U.S. government by spending, reports that in 2020, malign actors received at least $692 million in cryptocurrency extorted in ransomware attacks, up from $152 million in 2019.[97] According to DigitalMint, a company that facilitates acquisition of cryptocurrency on behalf of ransomware victims to resolve ransom demands, such figures are likely understated. DigitalMint estimates that the total amount of cryptocurrency ransomware payments likely reached closer to $1 billion in 2020.[98] According to one estimate, the average ransomware payment size in 2021 reached $118,000, up from $88,000 in 2020 and $25,000 in 2019.[99] At least 140 ransomware families received payments from victims in 2021—a new all-time high.[100]

In addition, victims' losses often include costs associated with business interruption, remediation, and rebuilding. In addition, organizations can face exposure to reliant third-party claims "if their computer systems remain inoperable or their data is lost."[101] Victims may also be subject to significant reputational damage. In interviews with Committee staff, both the private sector and law enforcement reiterated the severe threat ransomware attacks can create for small to medium-sized businesses stating that "one ransomware attack may be enough to cause small-to-medium sized companies to go out of business."[102]

Ransomware actors are increasingly highly adept at using more sophisticated methods shifting tactics to avoid detection. Available data has shown that the threat of ransomware attacks is growing.[103] The World Economic Forum found that ransomware attacks increased by

---

[97] *The 2022 Crypto Crime Report*; Danny Nelson, *Inside Chainalysis' Multimillion-Dollar Relationship With the US Government*, CoinDesk (Feb. 10, 2020) (www.coindesk.com/business/2020/02/10/inside-chainalysis-multimillion-dollar-relationship-with-the-us-government/). By 2019, Chainalysis had government contracts with ten federal agencies, departments and bureaus including CFTC, U.S. Drug Enforcement Agency (DEA), FBI, U.S. Immigration and Customs Enforcement (ICE), IRS, SEC, and the Transportation Security Administration (TSA), among other agencies. More recently, in 2021, Chainalysis held 21 contracts with six different agencies, including for software licenses, training, and blockchain analysis. USA Spending, Spending by Prime Award (accessed May 2, 2022) (www.usaspending.gov/search/?hash=89319dae3b34df861a7e06de84dc8d60).

[98] MacKenzie Sigalos, *When ransomware strikes, this company helps victims make bitcoin payments*, CNBC (June 10, 2021) (www.cnbc.com/2021/06/10/digitalmint-helps-ransomware-victims-make-bitcoin-payments.html#:~:text=Since%20January%202020%2C%20DigitalMint%20says,a%20median%20payment%20of%20%24800%2C000).

[99] *The 2022 Crypto Crime Report*. Estimates of average ransom payments vary by source. For instance, Palo Alto reported that the average ransomware payment was $312,000 in 2020 and had reached $850,000 in the first quarter of 2021. John Davis, *Palo Alto Networks Leads Efforts to Combat Ransomware*, paloalto networks (blog) (May 14, 2021) (www.paloaltonetworks.com/blog/2021/05/policy-rtf-combating-ransomware/?utm_source=ransomware.org&utm_medium=link).

[100] *The 2022 Crypto Crime Report*.

[101] Oliver Sepulveda, *Third-Party Liability for Ransomware Attacks, Are You Covered?*, Daily Business Review (Dec. 2, 2020) (https://www.shutts.com/news-Third-Party-Liability-for-Ransomware-Attacks-Are-You-Covered).

[102] DOJ Letter. *See also* Minder Interview.

[103] *See* Cybersecurity and Infrastructure Security Agency, *2021 Trends Show Increased Globalized Threat of Ransomware* (AA22-040A) (Feb. 9, 2022) (www.cisa.gov/uscert/ncas/alerts/aa22-040a).

435 percent in 2020 and "are outpacing societies' ability to effectively prevent or respond to them."[104]

In communications with Committee staff, DOJ confirmed this threat. Whereas previously ransomware actors would primarily conduct large scale random attacks against consumers, more recently, certain threat actors have conducted targeted, high-impact attacks against businesses. According to DOJ, attackers used to primarily "conduct a "Spray and Pray" attack, in which they would send a spam link to multiple recipients," and then "the victim would click on the link, which installed malware onto the victim's machine."[105] As of recently, "ransomware attacks are more targeted, with attackers specifically researching victims, determining how to enter specific systems, and assessing what they will do once they gain access to the victim's system."[106] Attackers now also increasingly use the "tactic of not only encrypting a victim's only copy of information but also exfiltrating sensitive data from victims and threatening to release that information to the public if a ransom is not paid."[107] This technique is called a double extortion attack.[108]

Similarly, since 2020, cybercriminals have shown a growing preference for Monero, a form of cryptocurrency that grants more privacy than Bitcoin and claims to be untraceable.[109] Cybersecurity companies which assist clients with detection, mitigation, and prevention of cybersecurity risks as well as ransomware incident response firms, such as Coveware and LMG Security, have also seen an increase in ransom demands made in Monero, or other privacy coins.[110] With respect to the federal government, the IRS has had to develop new partnerships with private companies to attempt to develop a tool or solution for tracing Monero transactions.[111] In conversations with Committee staff, regulators expressed concern over the use of privacy coins, noting that there is a "substantial difference between more transparent cryptocurrency and more opaque transactions."[112] Law enforcement and regulators face issues

---

[104] World Economic Forum, *The Global Risks Report 2022* (2022) (www.weforum.org/reports/global-risks-report-2022).

[105] DOJ Letter.

[106] *Id*.

[107] *Id*.

[108] Janus Agcaoili, Miguel Ang, Earle Earnshaw, et. al., *Ransomware Double Extortion and Beyond: REvil, Clop, and Conti*, Trend Micro (June 15, 2021) (https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti).

[109] Andrew Hayward, *IRS Dishes Out $1.25 Million for Data Firms to Crack Monero*, Decrypt (Sep. 30, 2020) (decrypt.co/43451/irs-1-million-contracts-data-firms-crack-monero).

[110] Siegel Interview; Sherri Davidoff, Chief Executive Officer, LMG Security, Interview with Senate Committee on Homeland Security and Governmental Affairs (Nov. 5, 2021) (hereinafter "Davidoff Interview"). LMG Security noted that while cyber criminals prefer privacy coins, ransom payments are seldom, if ever, made in privacy coins. Rather, cyber criminals may subsequently exchange a ransom paid in bitcoin to a privacy coin via a P2P exchange in the hopes of preventing the payment from being traced via the bitcoin public ledger. Davidoff Interview.

[111] Andrew Hayward, *IRS Dishes Out $1.25 Million for Data Firms to Crack Monero*, Decrypt (Sep. 30, 2020) (decrypt.co/43451/irs-1-million-contracts-data-firms-crack-monero).

[112] FinCEN O'Connor Interview.

concerning cryptocurrency "with anonymity built into them" as it "becomes increasingly difficult to trace" transactions involving such virtual currencies.[113]

Further, ransomware actors are continuously testing new methods of attack that have the potential to increase the ransomware threat and maximize profits.[114] For instance, in November 2021, FBI warned private industry that ransomware actors are targeting firms involved in time-sensitive financial events, such as mergers and acquisitions.[115] The FBI determined that ransomware attackers research publicly available information such as a victim's stock valuation, as well as material nonpublic information, which they threaten to disclose if victims do not pay a ransom quickly.[116] One ransomware group that is known for experimenting with novel tactics encouraged stock traders to contact the threat actor in order to obtain insider information so that "they can short sell [the ransomware victim's] stock before any data is leaked and the news goes public."[117]

F. National Security Threat

1. Professionalization of Ransomware Actors and the Rise of Digital Black Markets

According to cybersecurity authorities in the United States, Australia, and the United Kingdom, many ransomware attacks are executed by well-organized groups, with the market continually becoming more professionalized.[118] Jeremy Sheridan, Assistant Director of the Office of Investigations at Secret Service, testified before Congress in July 2021 that,

> [t]oday's ransomware gangs employ a vast array of specialists, from malware developers to human resources departments to public relations teams. They

---

[113] *Id.*

[114] For instance, since the summer of 2021, certain ransomware gangs appear to have been recruiting insiders, *i.e.*, rogue employees, to help them gain corporate network access in return for a significant fee. *See* Bill Toulas, *Ransomware gangs increase efforts to enlist insiders for attacks*, BleepingComputer (Jan. 24, 2022) (www.bleepingcomputer.com/news/security/ransomware-gangs-increase-efforts-to-enlist-insiders-for-attacks/).

[115] Federal Bureau of Investigation, *Ransomware Actors Use Significant Financial Events and Stock Valuation to Facilitate Targeting and Extortion of Victims* (20211101-001) (Nov. 1, 2021) (www.ic3.gov/Media/News/2021/211101.pdf). *See also Ransomware Attackers Begin to Eye Midmarket Acquisition Targets*, Wall Street Journal (Mar. 1, 2022) (www.wsj.com/amp/articles/ransomware-attackers-begin-to-eye-midmarket-acquisition-targets-11646130601) (suggesting a correlation between ransomware attacks and merger and acquisition deals).

[116] Federal Bureau of Investigation, *Ransomware Actors Use Significant Financial Events and Stock Valuation to Facilitate Targeting and Extortion of Victims* (20211101-001) (Nov. 1, 2021) (www.ic3.gov/Media/News/2021/211101.pdf).

[117] Bradley Barth, *Ransomware gang offers traders inside scoop on attack victims so they can short sell their stocks*, SC Media (Apr. 23, 2021) (www.scmagazine.com/news/security-news/ransomware/ransomware-gang-offers-traders-inside-scoop-on-attack-victims-so-they-can-short-sell-their-stocks).

[118] Cybersecurity and Infrastructure Security Agency, *2021 Trends Show Increased Globalized Threat of Ransomware* (AA22-040A) (Feb. 9, 2022) (www.cisa.gov/uscert/ncas/alerts/aa22-040a).

meticulously gather information on victim organizations and set extortion prices based on the information they collect.[119]

Ransomware actors also employ "independent services to negotiate payments, assist victims with making payments, and arbitrate payment disputes between themselves and other cyber criminals."[120] In addition, facilitated by the ease of cryptocurrency, the proliferation of ransomware contributed to the growth of an online black market where novice threat actors can access tools needed to conduct a ransomware attack.

The development of Ransomware-as-a-Service (RaaS) over the last decade has been a key factor in facilitating the professionalization of ransomware attackers. RaaS "is a business model between ransomware operators and affiliates in which affiliates pay to launch ransomware attacks developed by operators." [121] Ransomware operators typically provide affiliates with technology and support for ransomware attacks in exchange for a fee and/or a cut of the ransom proceeds depending on the revenue model.[122] Ransomware operators sometimes even develop RaaS kits, which "may include 24/7 support, bundled offers, user reviews, forums," and even assist affiliates "to develop their own ransomware variant."[123] As a result of its success, the RaaS market is competitive and incorporates traditional business practices, such as marketing campaigns, white papers, and a social media presence. Attackers can be "highly professionalized, leveraging expert third-party partnerships, an internal division of labor that mirrors the way legitimate businesses are organized, and economies of scale to grow their margins."[124] RaaS has significantly lowered the technical barrier of entry into the ransomware economy.

Digital black markets continue to expand in large part due to the consistently high payments in cryptocurrency from ransom victims combined with the low costs and developed infrastructure and networks that facilitate ransomware attacks. Notably, costs for ransomware tools range from $5 to more than $100 depending on the ransomware family, or may instead be based on a cut of proceeds.[125] Public information on profits from reported ransomware attacks

---

[119] Senate Committee on the Judiciary, Testimony Submitted for the Record of Jeremy Sheridan, Office of Investigations, United States Secret Service, U.S. Department of Homeland Security, *Hearing on Responding to Ransomware*, 117th (July 27, 2021) (S. Hrg. 117-XX) (www.secretservice.gov/sites/default/files/reports/2021-07/USSS-Testimony-AD-Jeremy-Sheridan-7-27-2021.pdf).

[120] Cybersecurity and Infrastructure Security Agency, *2021 Trends Show Increased Globalized Threat of Ransomware* (AA22-040A) (Feb. 9, 2022) (www.cisa.gov/uscert/ncas/alerts/aa22-040a).

[121] Kurt Baker, *Ransomware As A Service (RAAS) Explained*, CrowdStrike (Feb. 7, 2022) (www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/).

[122] *Id*.

[123] *Id*.

[124] Horizon2.ai, *The ransomware threat landscape has changed: here's how defenders must adapt*, Cybersecurity Dive (Dec. 6, 2021) (https://www.cybersecuritydive.com/spons/the-ransomware-threat-landscape-has-changed-heres-how-defenders-must-adap/610815/).

[125] Anthony M. Freed, *What is the Dark Web Ransomware Marketplace?*, Cyberreason (Oct. 19, 2021) (www.cybereason.com/blog/what-is-the-dark-web-ransomware-marketplace). *See also* Mayra Rosario Fuentes,

suggest that certain ransomware groups have amassed budgets that are likely comparable with the budgets of nation-state organizations.[126] These criminal organizations use illicit gains to expand operations, specialize, and improve products, similar to legitimate businesses. More effective ransomware reinforces the organizations' business model and attracts more bad actors. It has also resulted in attacks that are less expensive and easier to conduct.[127]

2. Money Laundering Facilitation

After receiving ransom payments from victims, certain illicit actors will take advantage of the cryptocurrency payment structure to launder their profits.[128] Traditionally, money laundering follows three steps: 1) placement, 2) layering, and 3) integration.[129] Within the context of cryptocurrency, placement occurs when actors receive the ransomware payment and place it in a laundering tool; layering occurs within the laundering tool where illicit and legitimate funds are combined; and integration occurs when the funds are removed and appear to have been legally obtained.[130] Andrew Winerman, Acting Associate Director, Strategic Operations Division at FinCEN explained in conversations with Committee staff how ransomware actors make use of certain aspects of the cryptocurrency payment structure to launder ransom payments,

> [ransomware] [a]ttackers will try and launder what they obtain, they will receive funds in unhosted wallets and then they go to town with every technique to try and cash it out at a foreign exchange that isn't tracking.[131]

Specific laundering tools unique to the cryptocurrency ecosystem render it more difficult for authorities to trace payments back to the ransomware actors under investigation.[132] These laundering tools include mixers, also known as tumblers. In the most basic terms, these services attempt to combine cryptocurrency from a variety of sources, including ransom payments with transactions involving unrelated parties and / or "clean" cryptocurrency in order to obscure the

---

Shifts in Underground Markets, Past, Present, and Future, TrendMicro (2020) (documents.trendmicro.com/assets/white_papers/wp-shifts-in-the-underground.pdf).

[126] Microsoft, *Microsoft Digital Defense Report* (Oct. 2021) (query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi?id=101738).

[127] *Id*.

[128] Lavender Baj, *What the Heck Is a Crypto Tumbler And Is It Even Legal?*, Gizmodo (June 28, 2021) (www.gizmodo.com.au/2021/06/cryptocurrency-tumblers-mixers-explained/).

[129] Financial Crimes Enforcement Network, History of Anti-Money Laundering Laws (accessed on Mar. 16, 2022) (www.fincen.gov/history-anti-money-laundering-laws#:~:text=Money%20laundering%20is%20the%20process,into%20the%20legitimate%20financial%20system).

[130] *Bitcoin Money Laundering: How Criminals Use Crypto*, Elliptic (blog) (Sept. 18, 2019) (www.elliptic.co/blog/bitcoin-money-laundering).

[131] Andrew Winerman, Acting Associate Director, Strategic Operations Division, Financial Crimes Enforcement Network, Interview with Senate Committee on Homeland Security and Governmental Affairs (July 20, 2021).

[132] Email from United States Secret Service, Criminal Investigative Division, to Senate Committee on Homeland Security and Governmental Affairs (Apr. 14, 2022).

source and intended destination of a given transactional counterparty (individual or institution).[133] Such techniques pose serious risks and threats when used for illicit activity as they aim to render transactions increasingly anonymous.[134] Similarly, the lucrative nature of ransomware has resulted in an increased demand by criminals for mixing / tumbling services.[135]

According to DOJ, a major concern with the international nature of cryptocurrency is a lack of compliance with anti-money laundering laws across jurisdictions.[136] Some international jurisdictions even have a "complete absence of such regulation and supervision."[137] Inconsistent application of these laws leaves gaps in regulation and enforcement. This inconsistency also negatively impacts law enforcement's "ability to investigate, prosecute, and prevent criminal activity involving or facilitated by" cryptocurrency.[138]

Mr. Winerman from FinCEN explained in conversations with Committee staff the growing anti-money laundering threat created by jurisdictional arbitrage,

> [w] hile we think regulations are in a good place, there is clearly a lot of ransomware activity going on with cashing out in foreign exchanges in jurisdictions that aren't doing a great job at regulating.[139]

He further stated, "[i]n [the] future…improved ways to launder money and decentralized finance" would enhance the threat created by ransomware and cryptocurrency ransom payments.[140]

3. Russia/Ukraine Conflict

As Russia's attack on Ukraine continues, ensuring that policymakers have a comprehensive understanding of the ransomware threat is critical to defend against cyber-attacks by cybercriminals operating in or supported by the Russian government or other malign countries. On March 7, 2022, FinCEN issued an alert providing examples of red flags to assist CVC exchangers and administrators as well as other financial institutions in identifying

---

[133] *Id*.

[134] *Id*.

[135] *Id*.

[136] Department of Justice, *Cryptocurrency: Enforcement Framework* (Oct. 2020) (www.justice.gov/archives/ag/page/file/1326061/download).

[137] *Id*.

[138] *Id*.

[139] Andrew Winerman, Acting Associate Director, Strategic Operations Division, Financial Crimes Enforcement Network, Interview with Senate Committee on Homeland Security and Governmental Affairs (July 20, 2021).

[140] *Id*.

suspected Russian sanctions evasion activity by both state actors and oligarchs.[141] The alert warns financial institutions of the dangers posed by Russian-related ransomware campaigns, stating that the institutions may "observe attempted or completed transactions tied to CVC wallets or other CVC activity associated with sanctioned Russian, Belarusian, and other affiliated persons."[142] Further, according to public reports, one ransomware group has specifically expressed support for the Russian invasion of Ukraine and have warned of possible attacks against "enemies of the Kremlin if they respond to Russia's invasion."[143]

III. DATA COLLECTION ON RANSOMWARE ATTACKS AND PAYMENTS IS FRAGMENTED AND INCOMPLETE

U.S. laws, regulations and guidance have been issued to require, or strongly encourage, cyber incident reporting. Historically, federal agencies have had to rely on voluntarily reported information from victims and the private sector to gain a better understanding of the threat of ransomware and cryptocurrency ransom payments. For instance, in interviews with Committee staff, Bill Siegel, Chief Executive Officer (CEO) for Coveware, a ransomware incident response firm, explained that they regularly share with FBI, and other local, state, and federal law enforcement, aggregated data obtained from their clients' cases.[144] To address the current lack of comprehensive information regarding the breadth and depth of the ransomware threat, Chairman Peters and Ranking Member Portman introduced the Cyber Incident Reporting Act of 2021, which passed the Senate as part of the Strengthening American Cybersecurity Act of 2022. The incident reporting provisions of this bill recently were signed into law as the Cyber Incident Reporting for Critical Infrastructure Act of 2022 within the Consolidated Appropriations Act of 2022. The new reporting mandates for critical infrastructure in the law will begin to address this problem, however the law provides CISA time to complete a regulatory rulemaking process and therefore have not yet been implemented at the time of this report.

Private entities, among other third parties, collect most of the publicly available data in this field. These cybersecurity entities include software companies, like Microsoft; computer security companies, such as McAfee and Emsisoft; cryptocurrency analysis and blockchain data platforms, like Chainalysis; cyberinsurance companies, such as Resilience Insurance; and sector-specific organizations, like the K-12 Cybersecurity Resource Center.[145] These companies and

---

[141] FinCEN, *FinCEN Provides Financial Institutions with Red Flags on Potential Russian Sanctions Evasion Attempts* (Mar. 7, 2022) (www.fincen.gov/news/news-releases/fincen-provides-financial-institutions-red-flags-potential-russian-sanctions).

[142] *Id*.

[143] Christopher Bing, *Russia-based ransomware group Conti issues warning to Kremlin foes*, Reuters (Feb. 25, 2022) (www.reuters.com/technology/russia-based-ransomware-group-conti-issues-warning-kremlin-foes-2022-02-25/).

[144] Siegel Interview.

[145] Microsoft, Our company (accessed Mar. 8, 2022) (www.microsoft.com/en-us/about/company); Emsisoft, Why Emsisoft (accessed Mar. 8, 2022) (www.emsisoft.com/en/company/about/); McAFee, About McAfee (accessed Mar. 8, 2022) (www.mcafee.com/en-us/consumer-corporate/about.html); Chainalysis, What we do (accessed Mar. 8, 2022) (www.chainalysis.com/company/); Resilience Insurance, About (accessed Mar. 8, 2022) (www.resilienceinsurance.com/about/); The K-12 Cybersecurity Resource Center, About (accessed Mar. 8, 2022) (k12cybersecure.com/about/).

organizations generally rely on voluntarily reported client data or publicly available information. As such, there are significant gaps in private sector data on the threat of ransomware attacks and the extent to which cryptocurrency ransom payments fuel the ransomware economy.

A. Data Collection by U.S. Government Agencies

Although there is significant coordination between regulatory and law enforcement agencies on open ransomware cases, to date, data on ransomware attacks and cryptocurrency ransom payments is not accessible and searchable across government agencies. In discussions with the Committee, the agencies interviewed (DOJ, SEC, and FinCEN) emphasized their close collaboration with federal regulatory and international counterparts on open cases.[146]

In interviews with the Committee, one company explained that they began collecting data on ransomware trends and aggregating statistics on ransomware payments and attack vectors to fill this void.[147] Coveware's CEO told the Committee in interviews,

> [W]e were found[ed] in 2018 because we felt like this was a very large problem with very little data collected on it and that struck us as odd that there was a large problem with little firsthand data. There was no go-to centralized data out there about what happens during these attacks. It took us a couple of months, and we meandered our way into a gap in incident response services.[148]

Government agencies collect data on cyber incidents, including ransomware, under a patchwork of laws, regulations, and guidance. These efforts seek to protect homeland security and critical infrastructure, facilitate and protect law enforcement actions, and promote foreign policy goals, among other purposes, while protecting victim privacy rights.[149] For instance, pursuant to the Anti-Money Laundering Act of 2020 (AMLA), FinCEN must publish threat

[146] *See* DOJ Letter; FinCEN O'Connor Interview; Division of Enforcement, Securities and Exchange Commission, Interview with Senate Committee on Homeland Security and Governmental Affairs (Sept. 9, 2021).

[147] Siegel Interview.

[148] Siegel Interview.

[149] *See* 45 CFR 164.308(a)(6); Department of Health and Human Services, Office of Civil Rights, *Fact Sheet: Ransomware and HIPAA* (accessed Mar. 28, 2022) (www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html); Federal Bureau of Investigation, *Ransomware Victims Urged to Report Infections to Federal Law Enforcement* (Sept. 15, 2016) (www.ic3.gov/Media/Y2016/PSA160915); Department of the Treasury, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Sept. 21, 2021) (home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf).

pattern and trend information with respect to incidents of cybercrime including ransomware affecting regulated financial institutions.[150] The data is collected from SARs.

Law enforcement and certain regulatory agencies encourage victims of ransomware to report attacks. Key federal contacts for reporting ransomware attacks include:

1. CISA
    - StopRansomware.gov – This website allows victims to report ransomware attacks and presents itself as "the U.S Government's official one-stop location for resources to tackle ransomware more effectively" and offers victims the option of reporting an attack.[151]

    - CISA Incident Reporting System – The CISA Incident Reporting System provides a secure web-enabled means of voluntarily reporting computer security incidents to CISA, including ransomware attacks.[152]

    - As of July 2021, CISA, which was created in 2018 specifically to reduce risk to the nation's cyber and physical infrastructure, estimated that only about one quarter of ransomware incidents were reported.[153]

    - Pursuant to the newly-passed Cyber Incident Reporting for Critical Infrastructure Act, critical infrastructure entities, as defined through a CISA rulemaking, will have to report within 72 hours of having a reasonable belief that a substantial cyber incident (also defined in the rulemaking) has occurred, and within 24 hours of making a ransomware ransom payment.[154]

2. FBI
    - IC3.gov – IC3.gov allows victims and third parties to report any cyber-attack, including ransomware attacks.[155] This portal enables the FBI to build a narrow

[150] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, Sec. 6001-6511 (2021). *See also* Financial Crimes Enforcement Network, *Financial Trend Analysis Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021* (June 30, 2021).

[151] Cybersecurity and Infrastructure Security Agency, Stop Ransomware (accessed on Mar. 3, 2022) (StopRansomware.gov).

[152] Cybersecurity and Infrastructure Security Agency, CISA Reporting System (accessed on Mar. 3, 2022) (us-cert.cisa.gov/forms/report). *See also* Cybersecurity and Infrastructure Security Agency, Report Incidents, Phishing, Malware, or Vulnerabilities (Mar. 3, 2022) (www.cisa.gov/uscert/report).

[153] Gerrit De Vynck, *Many ransomware attacks go unreported. The FBI and Congress want to change that.*, Washington Post (July 27, 2021) (https://www.washingtonpost.com/technology/2021/07/27/fbi-congress-ransomware-laws/).

[154] Consolidated Appropriations Act of 2022, Pub. L. No. 117-103, Sec. 2242 (2022).

[155] Federal Bureau of Investigation, Internet Crime Compliance Center (accessed on Feb. 25, 2022) (IC3.gov).

data universe on ransomware attacks for further analysis and future use.[156] FBI claims that IC3 is "the central point" for internet crime reporting.[157]

- Local FBI field offices – Ransomware victims can also report ransomware incidents to local FBI field offices as opposed to IC3.gov.[158] If local FBI field offices compile victim complaints of ransomware incidents, this information does not appear to be publicly available.

Public agencies at the state level also collect limited data on cyber incidents. Generally, mandatory reporting requirements are limited to data breaches involving personally identifiable information.[159] All 50 states, as well as D.C., Puerto Rico, and the Virgin Islands, have laws addressing applicability, definitions, notice requirements, and exemptions in connection with such reporting requirements.[160] In 2021, 45 states considered legislation relating to cybersecurity and reporting requirements.[161] Three of those states, Indiana, Louisiana, and North Dakota, have passed and implemented legislation requiring public entities to report ransomware attacks.[162] Entities in states with general cyber incidents reporting legislation may also need to report ransomware attacks depending on the state's requirements.[163]

B. Artificially Low Reporting

Based on the submissions made via FBI's IC3.gov website, the agency publishes an annual "Internet Crime Report" compiling data on the number of internet crimes (including ransomware) and losses reported annually. In 2020, FBI received 791,790 cybercrime complaints, a 69 percent increase from 2019.[164] Of these, 2,474 complaints constituted

---

[156] DOJ Letter.

[157] Internet Crime Compliance Center, *Internet Crime Report 2020*, Federal Bureau of Investigation (2020) (www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf).

[158] *See* Federal Bureau of Investigation, *Ransomware Victims Urged to Report Infections to Federal Law Enforcement* (Sep. 15, 2016) (www.ic3.gov/Media/Y2016/PSA160915).

[159] National Conference of State Legislatures, *Security Breach Notification Laws* (Apr. 15, 2021) (www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx).

[160] *Id*.

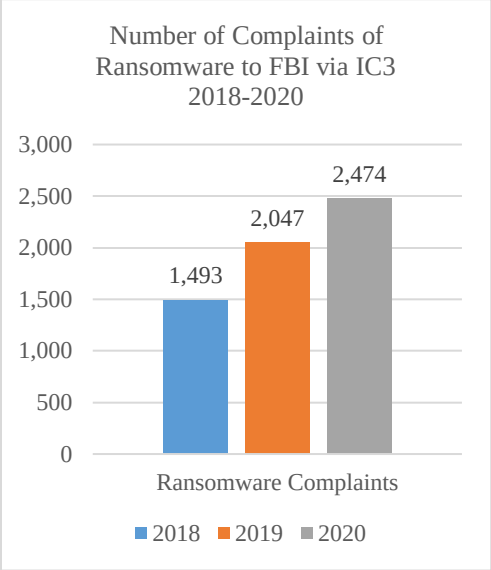
[161] *Id*.

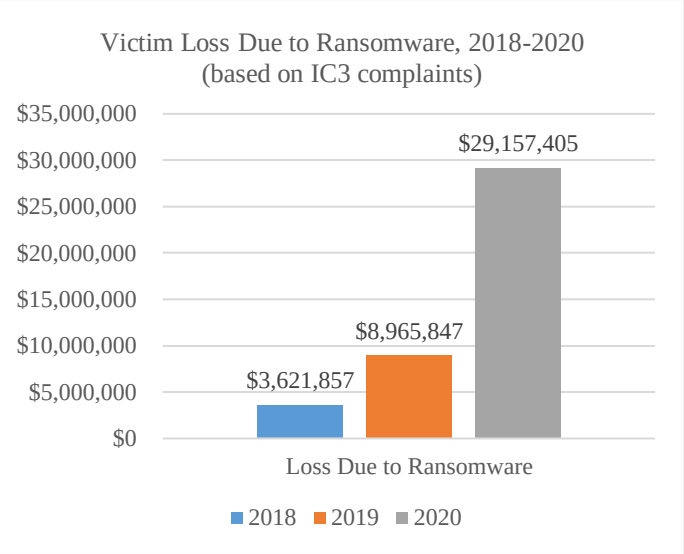
[162] National Conference of State Legislatures, *Computer Crime Statutes* (May. 4, 2022) (https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx).

[163] National Conference of State Legislatures, *Computer Crime Statutes* (May. 4, 2022) (https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx) (stating that North Carolina requires reporting of cyber incidents generally (which may include ransomware attacks).

[164] Federal Bureau of Investigation, *Internet Crime Report 2020* (Mar. 17, 2021) (https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf).

ransomware incidents with adjusted losses of over $29.1 million.[165] A three-year comparison of the number of complaints of ransomware submitted to IC3 demonstrates a 65.7 percent increase in victim count and a staggering 705 percent increase in adjusted losses.[166]





The report notes, however, that the ransomware data is "artificially low" because the data only considers attacks reported through IC3, excluding reports to FBI field offices. In addition, the information "does not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by a victim."[167] The report also notes that "in some cases, victims do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate."[168]

Security and privacy experts have noted that IC3 ransomware data is a "subset of a subset" of data.[169] Some argue that the figures are "incredibly low" and "inconsistent" due to the fact that victims will generally report an incident to their local field office.[170] The FBI's figures on ransomware may also be low due to lack of awareness on the part of victims regarding when and how ransomware incidents should be reported.[171] Despite FBI initiatives designed to

---

[165] Federal Bureau of Investigation, *Internet Crime Report 2020* (Mar. 17, 2021) (https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf).

[166] *Id*.

[167] Federal Bureau of Investigation, *Internet Crime Report 2020* (Mar. 17, 2021) (https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf).

[168] *Id*.

[169] Alexander Culafi, *FBI IC3 report's ransomware numbers are low*, TechTarget (Mar. 18, 2021) (www.techtarget.com/searchsecurity/news/252498133/FBI-IC3-reports-ransomware-numbers-are-low-experts-say).

[170] *Id*.

[171] Kyle Johnson and Mike O. Villegas, *Best practices for reporting ransomware attacks*, Tech Target (Mar. 2021) (www.techtarget.com/searchsecurity/answer/What-are-some-best-practices-for-reporting-ransomware-attacks).

educate potential victims regarding the reporting process, organizations may remain hesitant to voluntarily report the occurrence of an attack for a myriad of reasons including concerns regarding brand damage, regulatory oversight, civil legal actions, and loss of revenue.[172]

Further evidence of this under-reporting is that the numbers reported by FBI are drastically lower than several private sector estimates. For instance, one private sector study found that there were at least 24,770 ransomware incidents in the U.S. in 2019 and estimated their costs (including costs of downtime) at just under $10 billion.[173]

The FBI has since made improvements in its data collection process. In June 2021, the IC3 began tracking reported ransomware incidents in the critical infrastructure sector, specifically.[174] For instance, in the most recent version of the Internet Crime Report published on March 22, 2022, the FBI identified that IC3 received 649 complaints from organizations belonging to a critical infrastructure sector.[175] The report breaks down critical infrastructure into 16 different sectors.[176] Of those 16 sectors, "IC3 reporting indicated 14 sectors had at least 1 member that fell victim to a ransomware attack in 2021."[177] In addition, the FBI indicated that IC3 had received 3,729 ransomware complaints with adjusted losses of more than $49.2 million in 2021.[178] In another improvement over the 2020 annual report, the FBI also discusses the evolution of ransomware tactics and techniques and provides general recommendations for protecting computer systems against ransomware attacks.[179] Still, the agency acknowledges that the overall ransomware loss rate is "artificially low" due to the reasons described above, notably

---

[172] Alexander Culafi, *FBI IC3 report's ransomware numbers are low* (Mar. 18, 2021) (www.techtarget.com/searchsecurity/news/252498133/FBI-IC3-reports-ransomware-numbers-are-low-experts-say); *see* Federal Bureau of Investigation, Infragard (accessed on Feb. 22, 2022) (www.infragard.org/Application/Account/Login).

[173] Alexander Culafi, *FBI IC3 report's ransomware numbers are low*, TechTarget (Mar. 18, 2021) (www.techtarget.com/searchsecurity/news/252498133/FBI-IC3-reports-ransomware-numbers-are-low-experts-say). Emsisoft conducted a study that derives the number of reported incidents from submissions to ransomware identification service ID Ransomware. Every submission to this service represents a confirmed incident. In 2019, there was a total of 452,151 submissions. According to Emsisoft, at least 24,770 of these submissions were ransomware incidents in the U.S. Note, however, Emsisoft estimates that only approximately 25 percent of public and private sector organizations affected by ransomware use the "ID Ransomware" website. *See* Emsisoft Malware Lab, *Report: The cost of ransomware in 2020. A country-by-country analysis*, Emsisoft (blog) (Feb. 11, 2020) (blog.emsisoft.com/en/35583/report-the-cost-of-ransomware-in-2020-a-country-by-country-analysis/). *See also* Malware Hunter Team, *ID Ransomware* (access Mar. 3, 2022) (id-ransomware.malwarehunterteam.com/index.php).

[174] Federal Bureau of Investigation, *Internet Crime Report 2021* (Mar. 22, 2022) (https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf).

[175] *Id*.

[176] *Id*. *See also* Cybersecurity and Infrastructure Security Agency, Critical Infrastructure Sectors (accessed May 16, 2022) (https://www.cisa.gov/critical-infrastructure-sectors).

[177] Federal Bureau of Investigation, *Internet Crime Report 2021* (Mar. 22, 2022) (https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf).

[178] *Id*.

[179] Federal Bureau of Investigation, *Internet Crime Report 2021* (Mar. 22, 2022) (https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf).

lack of data from FBI field offices and insufficient data from victims on losses, among other reasons.[180]

C. Impact of Irregular Reporting on Law Enforcement Agencies and the Private Sector

DOJ emphasized that "victim reporting is essential in ransomware attack investigations. Learning about each ransomware attack helps the Department create an overall picture of the actions of the ransomware actors and protect against future attacks."[181] In discussing tracking cryptocurrency ransom payments that are being laundered, FinCEN added that "the best thing is to have the financial information, we could have more actionable data through improved reporting."[182]

Similarly, when speaking with Committee staff, Sherri Davidoff, the CEO of LMG Security, a cybersecurity consulting, research and training firm, explained that a lack of reporting requirements and incentives results in underreporting, which causes experts in this area to "not have a clear understanding of the problem and inhibits development of effective solutions."[183] Coveware has close to 100 percent of its clients proactively reporting ransomware incidents to law enforcement, oftentimes to FBI field offices.[184] However, since the agencies collect a standard subset of incident data during the initial reporting, law enforcement often needs to reconnect with the victim in order to collect further statements and evidence in the proper format necessary for investigating, securing indictments, and prosecuting cases.[185] When law enforcement attempts to re-contact the victims to gather more information, the company estimates 25 percent or less of clients engage.[186] This can make it very difficult to complete the investigation and indictment process.

With respect to reporting, instructions on both the FBI and CISA websites suggest that victims of cybercrimes need only submit one complaint to ensure that law enforcement within multiple agencies will be notified of the attack. However, these instructions lack clarity. The CEO of LMG Security told Committee staff that there is not a clear responsibility for victims to report incidents.[187] Generally, LMG Security emphasized that the process for victims who are seeking to "do the right thing" is confusing and expensive which works against U.S. national security interests.[188] Coveware's CEO, Bill Siegel, told Committee staff that, while their clients

[180] *Id*.

[181] DOJ Letter.

[182] FinCEN O'Connor Interview.

[183] Davidoff Interview (adding that the lack of detection capabilities throughout the U.S. contributes to the epidemic of cyber extortion attacks).

[184] Siegel Interview.

[185] *Id*.

[186] *Id*.

[187] Davidoff Interview.

[188] *Id*.

almost unanimously proactively share data with law enforcement, reporting is made more difficult when it is unclear which agency a victim should report to or when dealing with an inexperienced government contact. According to Coveware's CEO,

> [a ransomware victim] could contact the wrong branch of law enforcement and that could be a distraction. The right branch would know they can't take up all the company's attention when they are trying to save their business.[189]

Similarly, the majority of victims that work with GroupSense, a digital risk protection services company, regularly choose to report an incident to either CISA and/or the FBI. When reporting to law enforcement, GroupSense's CEO, Kurtis Minder, and his team provide all relevant information including cryptocurrency wallets included in ransom notes.[190] In some cases, the FBI claimed that they would return the ransom money. According to Mr. Minder however, the FBI's efforts have been unfruitful suggesting that threat actors are finding ways to move money without using a major exchange subject to FBI jurisdiction or otherwise accessible by the FBI.[191]

With more comprehensive data on ransomware attacks, ransom payments, and the role of cryptocurrency, law enforcement and CISA would be able to better track and share trends and tactics used by bad actors. Ransomware actors rarely employ novel, never-before-seen techniques. Testifying before Congress, Jeremy Sheridan, Assistant Director for the Office of Investigations at Secret Service, said "many new ransomware strains built upon those that came before them, adding layers of encryption and obfuscation, making defense and mitigation efforts far more challenging."[192]

In communications with Committee staff, DOJ confirmed that data from reported incidents can shed light on the techniques of an attack which is critical for helping identify ransomware actors, monitoring BSA compliance, and prosecuting wrongdoers. DOJ explained that "increased data on ransom payments and instructions from ransomware actors can further assist law enforcement agencies with monitoring Bank Secrecy Act compliance, prosecuting wrongdoers, and identifying potential loopholes" in anti-money laundering regulations in the cyberspace.[193] As of July 2021, DOJ had 40 different ransomware investigations and prosecutions that were open.[194] DOJ also explained, however, that existing means to gather data

---

[189] Siegel Interview.

[190] Minder Interview.

[191] *Id.*

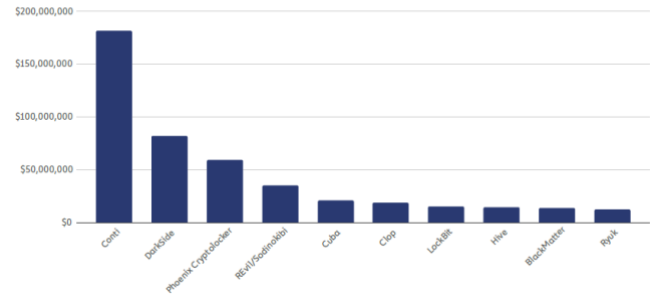
[192] Senate Committee on the Judiciary, Testimony Submitted for the Record of Jeremy Sheridan, Office of Investigations, United States Secret Service, U.S. Department of Homeland Security, *Hearing on Responding to Ransomware*, 117th (July 27, 2021) (S. Hrg. 117-XX) (www.secretservice.gov/sites/default/files/reports/2021-07/USSS-Testimony-AD-Jeremy-Sheridan-7-27-2021.pdf).

[193] DOJ Letter.

[194] *Id.* The 40 cases represent investigations and prosecutions being handled by the Computer Crime and Intellectual Property Section of Criminal Division at the Department of Justice alone. The cases are broken down by ransomware variant. Of the 40 cases, "each case represents more than one ransomware attack, and one case may

from certain foreign countries that host threat actors combined with the borderless nature of cryptocurrency can make it particularly difficult to capture illicit actors.

Further, reports have shown that ransomware attackers tend to rebrand themselves and launch new ransomware strains in order to evade law enforcement and continue pursuing ransom opportunities. Thus, a small number of ransomware groups appear to be behind a large number of ransomware attacks. For example, on May 19, 2022, reports identified that the Conti ransomware gang, a group that the U.S. government considers one of the most threatening, had officially terminated their operations. They were reported to now have partnered with other smaller ransomware gangs to continue conducting attacks.[195]



Source: *The 2022 Crypto Crime Report*.

Similarly, data regarding the ransomware actors' money laundering practices suggest that only a handful of cryptocurrency businesses receive funds from ransomware wallet addresses. One study found that between 2020 and 2021, 56 percent of funds sent from ransomware wallet addresses were transferred to only six cryptocurrency businesses — three large international exchanges, one high-risk exchange based in Russia, and two mixing services.[196] When speaking with Committee staff, GroupSense's CEO, Kurtis Minder, shared that ransomware actors continue to develop new tactics to avoid detection. For instance, he shared that threat actors now may move and store illicit funds on the darknet for an extended period of time before resurfacing to the clearnet to cash out. This tactic seeks to "wait out" cybersecurity companies and victims until they move on.

With more information, law enforcement will also be able to better understand ransomware actors and can alert victims when they are attacked by terrorist or criminal

involve hundreds of victims that involve every federal district." As cases proceed, in some instances, the investigative team determines that certain variants are deployed by the same individuals and the cases may be merged. *Id*.

[195] *See* Lawrence Abrams, *Conti ransomware shuts down operation, rebrands into smaller units*, BleepingComputer (May 19, 2022) (www.bleepingcomputer.com/news/security/conti-ransomware-shuts-down-operation-rebrands-into-smaller-units/) (announcing that Conti had partnered with numerous well-known ransomware operations enabling the cybercrime syndicate to "gain[…] mobility and greater evasion of law enforcement by splitting into small 'cells,' all managed by central leadership"). *See also* Sergiu Gatlan, *US offers $15 million reward for info on Conti ransomware gang*, BleepingComputer (May 7, 2022) (www.bleepingcomputer.com/news/security/us-offers-15-million-reward-for-info-on-conti-ransomware-gang/).(stating that the U.S. Department of State is offering up to $15 million for information regarding the leadership and co-conspirators of the Conti ransomware gang).

[196] *The 2022 Crypto Crime Report*.

organizations.[197] In an interview with the Committee, Bill Siegel from Coveware reiterated that "[t]here is a clear need for enhanced coordination between the government and industry, particularly as it relates to information sharing and incident reporting."[198] In his testimony before Congress in July 2021, Assistant Director Sheridan testified that,

> [t]he U.S. Government needs access to timely, actionable information. If victim companies fail to report ransomware attacks early, or if they fail to report them at all, it hinders law enforcement's ability to assist them with asset recovery or to prevent future incidents.[199]

Similarly, also testifying before Congress in July 2021, Eric Goldstein, Executive Assistant Director for CISA, stated,

> CISA must work with all possible partners to gain increased visibility into national risks. With increased visibility, we can better identify adversary activity across sectors, which allows us to produce more targeted guidance, understand the degree to which adversary activity across sectors is increasing risk, and identify particular incidents requiring a specialized CISA response team. Our partnership with [the Transportation Security Agency] to develop two Security Directives requiring reporting of cybersecurity incidents to CISA is an important step and an example of such collaboration. We look forward to working with Congress to further encourage reporting of cybersecurity incidents to the federal government in order to further enable this essential visibility.[200]

Incomplete reporting on ransomware attacks and cryptocurrency ransom payments obscures the vast disparity in victims' experiences and challenges with recovering from an attack. Aggregated and anonymized data from increased incident reporting could help inform policies regarding potential federal assistance for excessively burdened ransomware victims. Increased reporting may also shed light on the specific burdens faced by small- and medium-sized businesses, such as inability to access high cost prevention methods and the drastic economic consequences of these attacks.[201] In an interview with Committee staff, Mr. Minder from GroupSense, suggested that Congress consider providing assistance to small and medium-

---

[197] Siegel Interview (explaining that Coveware keeps its own, more comprehensive, list of cryptocurrency wallets associated with terrorist or criminal organizations, created from data they collect from their clients in light of perceived inadequacies with existing government data).

[198] *Id*.

[199] Senate Committee on the Judiciary, Testimony Submitted for the Record of Jeremy Sheridan, Office of Investigations, United States Secret Service, U.S. Department of Homeland Security, *Hearing on Responding to Ransomware*, 117th (July 27, 2021) (S. Hrg. 117-XX) (www.secretservice.gov/sites/default/files/reports/2021-07/USSS-Testimony-AD-Jeremy-Sheridan-7-27-2021.pdf).

[200] Senate Committee on the Judiciary, Testimony Submitted for the Record of Executive Assistant Director for Cybersecurity Eric Goldstein, Cybersecurity and Infrastructure Agency, *Hearing on America Under Cyber Siege: Preventing and Responding to Ransomware Attacks*, 117th Cong. (July 27, 2021) (S. Hrg. 117-XX).

[201] Minder Interview.

sized businesses impacted by ransomware attacks in light of the disproportionate burden on such companies.[202]

D. Evolving Federal Response to Increase Incident Reporting and Expand Available Data on Ransomware Attacks and Cryptocurrency Ransom Payments

Agencies have recently taken steps – both regulatory and law enforcement centered – that recognize the national security risk of ransomware and/or that seek to address information deficiencies in connection with such attacks. However, certain challenges have limited agencies' progress to date.

FinCEN. As described above, pursuant to the AMLA, FinCEN periodically publishes threat pattern and trend information with respect to incidents of cybercrime in financial institutions.[203] The information is derived from financial institutions' SARs, as described above. FinCEN's experience with SARs reporting demonstrates the benefit of clearer reporting incentives and intelligence sharing among relevant agencies, such as a more comprehensive threat assessment and better deployment of resources.[204] These reports also help to develop appropriate risk management strategies to identify, report, and mitigate cyber-events and cyber-enabled crime and to reveal additional patterns of suspicious behavior and identify suspects.[205]

However, the dataset is far from comprehensive due to lack of compliance and the fact that entities subject to FinCEN regulations are only required to file reports when they observe suspicious activity, among other limitations. Thus, it is highly likely that significant money laundering activity remains unreported.

OFAC. OFAC imposes sanctions on malicious cyber actors and others who "materially assist, sponsor, or provide financial, material, or technological support" for ransomware attacks.[206] In its 2020 Guidance on threats posed by ransomware attacks, OFAC warns companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and

---

[202] *Id*.

[203] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, Sec. 6001-6511 (2021). *See also* Financial Crimes Enforcement Network, *Financial Trend Analysis Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021* (June 30, 2021).

[204] Financial Crimes Enforcement Network, *Financial Trend Analysis Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021* (June 30, 2021).

[205] *Id*.

[206] Department of the Treasury, *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Oct. 1, 2020) and Department of the Treasury, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Sept. 21, 2021). In 2013, for example, "a ransomware variant known as Cryptolocker was used to infect more than 234,000 computers, approximately half of which were in the United States. OFAC designated the developer of Cryptolocker, Evgeniy Mikhailovich Bogachev, in December 2016." *Id*.

incident response, that they may risk violating OFAC regulations if such transactions have a sanctions nexus, such as involvement of a sanctioned party or property.[207]

In discussions with Committee staff, however, LMG Security said that victims and third party agents face difficulties identifying which cryptocurrency wallets may be subject to U.S. sanctions. According to LMG Security, while OFAC keeps a list of sanctioned wallets, the OFAC Sanctions List Search Tool is not built to allow easy cryptocurrency address lookups, creating a barrier to victims seeking to access this information so that they can remain in compliance with OFAC sanctions.[208] LMG Security also explained that criminals routinely create brand new cryptocurrency wallets that have not previously been used, and then launder the funds, making it hard for OFAC to have a complete list of wallets associated with criminal organizations and terrorist groups.[209] Coveware, an incident response firm that assists victims with settling ransom demands, told the Committee that OFAC's list is not updated as sanctioned ransomware threat actors change their brands and tactics. Therefore, Coveware created its own list of threat actor groups.[210]

DOJ. On June 3, 2021, DOJ issued a memorandum to all federal prosecutors entitled, "Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion."[211] The DOJ guidance instructs U.S. attorney's offices across the country to coordinate ransomware investigations with the recently formed Ransomware and Digital Extortion Task Force.[212] The internal guidance states,

> [t]o ensure we can make necessary connections across national and global cases and investigations, and to allow us to develop a comprehensive picture of the national and economic security threats we face, we must enhance and centralize our internal tracking of investigations and prosecutions of ransomware groups and the infrastructure and networks that allow these threats to persist.[213]

According to DOJ, the procedures outlined in the guidance indicate that the agency has elevated investigations of ransomware attacks to a similar priority as terrorism.[214] Accordingly, all U.S

---

[207] Department of the Treasury, *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Oct. 1, 2020).

[208] *See* Davidoff Interview. *See also* Office of Foreign Assets Control, Sanctions List Search (accessed May 2, 2022) (https://sanctionssearch.ofac.treas.gov).

[209] Davidoff Interview.

[210] Siegel Interview.

[211] Department of Justice, Office of the Deputy Attorney General, *Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion* (June 3, 2021).

[212] Department of Justice, Office of the Deputy Attorney General, *Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion* (June 3, 2021).

[213] *Id*.

[214] Christopher Bing, *Exclusive: U.S. to give ransomware hacks similar priority as terrorism*, Reuters (June 3, 2021) (www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/) (quoting John Carlin, principal associate deputy attorney general at DOJ, " 'We've used this model around terrorism before but never with ransomware' ".

attorney's offices are now expected to file "urgent reports" with DOJ headquarters in "**every** instance" in which a U.S. attorney's office "learns of either a new ransomware or digital extortion attack in its District, or an attack believed to be related to an ongoing ransomware or digital extortion investigation or case it is conducting" that meets certain conditions.[215]

CISA. To address the current lack of information regarding the ransomware threat, Chairman Peters and Ranking Member Portman introduced the Cyber Incident Reporting Act of 2021, which passed the Senate as the Strengthening American Cybersecurity Act of 2022, of which its incident reporting provisions recently became law as the Cyber Incident Reporting for Critical Infrastructure Act of 2022 on March 15, 2022.[216] Critical infrastructure entities, as defined through a CISA rulemaking, will have to report within 72 hours of having a reasonable belief that a substantial cyber incident (also defined in the rulemaking) has occurred. A substantial cyber incident may include a ransomware attack. The same entities will have to report within 24 hours of making a ransomware payment, regardless of whether the ransomware attack met the threshold of a substantial cyber incident. CISA has two years after passage of the Act to issue the notice of proposed rulemaking, and another 18 months to issue the final rule.

SEC. The SEC requires public companies to report material cybersecurity risks and incidents that trigger disclosure obligations.[217] However, on March 9, 2022, SEC proposed a new rule to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies.[218] The proposal came after findings that current disclosure practices are inadequate. According to the SEC, certain disclosures may "contain insufficient detail" and staff has found that current reporting "is

---

[215] Department of Justice, Office of the Deputy Attorney General, *Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion* (June 3, 2021) (stating that urgent reports should be filed for an attack believed to be related to an ongoing investigation that is "(a) a major development in the case; (b) a law enforcement emergency; or (c) an event affecting the Department that is likely to generate national media or Congressional attention") (emphasis in original).

[216] Consolidated Appropriations Act of 2022, Pub. L. No. 117-103, Sec. 2242 (2022).

[217] 17 CFR § 229, 249. *See also* U.S. Securities and Exchange Commission, *Commission Statement and Guidance on Public Company Cybersecurity Disclosures* 83 FR 8166 (Feb. 26, 2018) (Interpretation) (outlining SEC's views with respect to cybersecurity disclosure requirements under the federal securities laws as they apply to public operating companies) and Division of Corporation Finance, *CF Disclosure Guidance: Topic No. 2 – Cybersecurity* (Oct. 13, 2011) (https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm) (stating that certain disclosure requirements may impose an obligation to disclose cybersecurity risks and incidents, *e.g.*, when necessary to make other required disclosures not misleading, even if the requirements do not explicitly refer to cybersecurity matters).

[218] U.S. Securities and Exchange Commission, *SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies* (Mar. 9, 2022) (www.sec.gov/news/press-release/2022-39) and U.S. Securities and Exchange Commission, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* 87 FR 16590 (Mar. 23, 2022) (Proposed Rule). *See also* U.S. Securities and Exchange Commission, *Cybersecurity Risk Management for Investment Advisers Registered Investment Companies, and Business Development Companies* 87 FR 13524 (Mar. 9, 2022) (Proposed Rule) (proposing rule to "require advisers to report significant cybersecurity incidents affecting the adviser, or its fund or private fund clients, to the Commission on a confidential basis").

inconsistent, may not be timely, and can be difficult to locate."[219] The proposed rules recognize that cybersecurity is an emerging risk for public companies and that both companies and investors need to evaluate public companies' cybersecurity practices and incident reporting.[220]

SEC staff told the Committee that they have been looking at the policies and procedures of issuers and investment advisers to determine whether they are acting sufficiently to protect individuals when ransomware incidents occur. The agency is considering how to address victims within its jurisdiction that fail to take steps to develop proper controls and policies as well as those that fail to disclose ransoms that have been paid.[221]

Transportation Security Administration. Following the May 2021 ransomware attack against Colonial Pipeline, the Department of Homeland Security's Transportation Security Administration issued two security directives to address the cybersecurity threat to pipeline systems and associated infrastructure. Security Directive Pipeline-2021-01, effective May 28, 2021, requires TSA-specified owners and operators to report cybersecurity incidents resulting in operational disruption, among other incidents, to CISA within 12 hours after the incident is identified.[222] On July 3, 2021, the Transportation Security Oversight Board issued a notification of ratification of the directive in which it stated that the directive is set to expire on May 28, 2022.[223]

Office of the Comptroller of the Currency, Federal Reserve System, and Federal Deposit Insurance Corporation. In November 2021, the OCC, Federal Reserve System, and Federal Deposit Insurance Corporation issued a final rule imposing computer-security incident notification requirements on banking organizations and their bank service providers. Effective April 1, 2022, a banking organization is required to notify its primary federal regulator of any

---

[219] U.S. Securities and Exchange Commission, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* 87 FR 16590 (Mar. 23, 2022) (Proposed Rule) (indicating that staff observed that certain companies failed to report publicly disclosed cyber incidents and that smaller reporting companies generally provide less cybersecurity disclosure than larger registrants). *See also* Moody's Investors Service, *Research Announcement, Cybersecurity disclosures vary greatly in high-risk industries* (Oct. 3, 2019) (www.moodys.com/research/Moodys-Cybersecurity-disclosures-vary-greatly-in-high-risk-industries--PBC_1196854) (stating that corporate cyber disclosures can vary greatly among companies in high-risk sectors which makes it more difficult to analyze a company's cyber posture and could hurt investor confidence as cyberattacks increase in frequency).

[220] U.S. Securities and Exchange Commission, *SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies* (Mar. 9, 2022) (www.sec.gov/news/press-release/2022-39).

[221] SEC Interview. *See also* Travis Brennan, Ryan C. Wilkins, and Katie Beaudin, *As Ransomware Attacks Increase, The SEC Takes Notice* (Sep. 10, 2020) (www.lexology.com/library/detail.aspx?g=732a036d-86cf-4c89-84f1-a8db50470cb9) (stating that some ransomware attacks are publicly known but are not disclosed in SEC filings).

[222] Transportation Security Administration, *Security Directive: Enhancing Pipeline Cybersecurity* (Security Directive Pipeline-2021-01) (May 28, 2021).

[223] Department of Homeland Security, *Ratification of Security Directive*, 86 Fed. Reg. 38209 (July. 20, 2021) (ratification of directive).

"computer-security incident" that rises to the level of a "notification incident" within 36 hours.[224] Bank service providers are required to notify each affected banking organization customer once it is determined that the incident caused, or is reasonably likely to cause, a material service disruption or degradation. The rule is expected to "help promote early awareness of emerging threats to banking organizations and the broader financial system."[225] Increased early awareness is intended to help "agencies react to these threats before they become systemic."[226]

IV. LACK OF COMPREHENSIVE OR CONSOLIDATED DATA ON RANSOMWARE ATTACKS AND CRYPTOCURRENCY RANSOM PAYMENTS LIMITS TOOLS AVAILABLE TO GUARD AGAINST NATIONAL SECURITY THREAT

The lack of consolidated data regarding the universe of ransomware attacks and the role that cryptocurrency plays in facilitating illicit acts limit the tools available to guard against national security threats. The United Nations and the U.S. have recently observed nations using cryptocurrencies to evade sanctions.[227] According to public reports, "hacking techniques like ransomware could help Russians [extort] digital currencies and make up revenue lost to sanctions."[228] In light of the ongoing invasion of Ukraine by Russia, a comprehensive understanding of illicit cryptocurrency use and ransomware is critical to ensure compliance with U.S. sanctions policy and mitigate damaging cybercrime.

Criminal groups in Russia are well-experienced in executing ransomware attacks. According to a 2022 Chainalysis study, about 74 percent of global ransomware revenue, or more than $400 million worth of cryptocurrency, went to ransomware strains that are "highly likely to be affiliated with Russia."[229] Russia is also at the center of cryptocurrency-based money laundering associated with cybercrimes, including ransomware. Chainalysis found that most of the funds extorted from ransomware attacks are "laundered through services primarily catering to Russian users."[230] Taking further action to increase the federal government's collective awareness of the ransomware landscape and associated uses of cryptocurrency, could provide

[224] Office of the Comptroller General, *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers*, 86 Fed. Reg. 223 (Nov. 23, 2021) (final rule).

[225] *Id*.

[226] *Id*.

[227] *Russia Could Use Cryptocurrency to Blunt the Force of U.S. Sanctions*, New York Times (Feb. 23, 2022) (www.nytimes.com/2022/02/23/business/russia-sanctions-cryptocurrency.html?partner=slack&smid=sl-share). Reports indicate that Russian entities are finding workarounds to make up revenue lost due to U.S. sanctions such as developing its own central bank digital currency. *Id*.

[228] *Id*.

[229] *The 2022 Crypto Crime Report*.

[230] *The 2022 Crypto Crime Report*.

lawmakers with more information when deliberating measures to enhance the government's ability to target Russian cybercriminals.

As barriers to the deployment of ransomware lower with pre-designed ransomware tools and RaaS, and cryptocurrency obfuscation tools and techniques become enhanced, ransomware attacks will likely continue to grow, and continue to threaten U.S. national security.[231] For instance, ransomware toolkits are readily available for purchase on the darknet, which RaaS operators can lease to affiliates who conduct attacks. Certain exchanges, namely nested exchanges are known to conduct lax anti-money laundering checks, or none at all, and to provide cryptocurrency trading services through a regulated exchange to avoid attention from law enforcement in connection with illicit transactions. Such exchanges oftentimes "support money laundering, scammers, and ransomware payments."[232] Providing analysts the ability to access and query data held by all federal agencies tracking ransom payments and the wallets being used to receive ransom payments, within the bounds of privacy and security rules, would likely improve analysts' ability to track the evolution of cryptocurrency platforms that support cybercriminal activity.

[231] Yaya J. Fanusie, *Cryptocurrency Laundering Is a National Security Risk*, Lawfare (Mar. 27, 2021) (www.lawfareblog.com/cryptocurrency-laundering-national-security-risk).

[232] *What Are Nested Exchanges and Why Should You Avoid Them?* Binance Academy (Dec. 2021) (academy.binance.com/en/articles/what-are-nested-exchanges-and-why-should-you-avoid-them). *See also Russia Could Use Cryptocurrency to Blunt the Force of U.S. Sanctions*, New York Times (Feb. 23, 2022) (www.nytimes.com/2022/02/23/business/russia-sanctions-cryptocurrency.html?partner=slack&smid=sl-share) (identifying "nesting" as a potential money-laundering technique that Russia could use to evade U.S. sanctions).

CONCLUSION

The majority of ransomware attacks go unreported and ransoms based in cryptocurrency continue to be paid against FBI guidance.[233] The continuing flow of ransom payments has encouraged illicit actors and contributed to a growing threat to businesses, the public, and to national security. The lack of comprehensive data on these attacks prevents the U.S. government from developing a full picture of cyber threats.

The Administration states that it has made countering ransomware attacks a priority. In October 2021, it brought together representatives from 30 countries to discuss how to disrupt "the financial systems that make ransomware profitable" and "the ransomware ecosystem," among other ways to fight back against ransomware attacks.[234] On March 9, 2022, the Biden Administration issued an Executive Order outlining a "whole-of-government" approach to examining the risks associated with the sharp increase in use of cryptocurrencies.[235] Among other key policy priorities, the Administration recognizes that cryptocurrencies have "facilitated sophisticated cybercrime-related financial networks and activity, including through ransomware activity."[236] The Executive Order also recognizes that cryptocurrencies present "heighten[ed] risks of crimes such as money laundering, terrorist and proliferation financing, fraud and theft schemes, and corruption."[237] Among other requirements, President Biden is directing federal agencies to develop coordinated plans to address "digital-asset-related illicit finance and national security risks."[238]

The data needed to support these initiatives, among other agency efforts to tackle ransomware and cryptocurrency ransom payments, remains fragmented and incomplete. The lack of comprehensive ransomware incident and ransom payment reporting contributes to a lack of data on matters that are priorities in the Biden Administration's national security agenda. Further, this limited collective understanding of the ransomware landscape and the cryptocurrency payment system blunts the effectiveness of available tools to protect national security. As Russia's invasion of Ukraine continues and Russia seeks to find ways around the international finance system, the need to address these shortfalls grows.

---

[233] Federal Bureau of Investigation, Ransomware (accessed Mar. 3, 2022) (www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware#:~:text=The%20FBI%20does%20not%20support,this%20type%20of%20illegal%20activity) and *see also* Sarah N. Lynch, *FBI Director Wray Urges companies to stop paying ransoms to hackers*, Reuters (June 23, 2021) (www.reuters.com/technology/fbi-director-wray-urges-companies-stop-paying-ransoms-hackers-2021-06-23/) (quoting FBI Director Chris Wray, "[i]n general, we would discourage paying the ransom because it encourages more of these attacks, and frankly, there is no guarantee whatsoever that you are going to get your data back").

[234] *See* White House, *Fact Sheet: Ongoing Public U.S. Efforts to Counter Ransomware* (Oct. 13, 2021) (www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/).

[235] Exec. Order No. 14067, 87 FR 14143 (Mar. 14, 2022).

[236] *Id*.

[237] *Id*.

[238] *Id*.

To address the lack of understanding of the true scope of the problem and the size of the ransomware market, Chairman Peters and Ranking Member Portman introduced the Cyber Incident Reporting Act of 2021, which passed the Senate as part of the Strengthening American Cybersecurity Act of 2022, of which its incident reporting provisions recently became law as the Cyber Incident Reporting for Critical Infrastructure Act on March 15, 2022. The Administration should prioritize timely implementation of the new law's reporting requirements. The rules implementing the reporting process should be standardized and easily understood such that victims under the duress of an attack are not unduly burdened by the reporting process.

To ensure that the potential influx of ransomware attack-related data is used effectively, Congress should consider exploring whether federal agencies responsible for processing the data have sufficient resources to do so in a timely and effective manner and assess the level of resources that would be needed, if not. Further, given the extent to which the federal government relies on partnerships with the private, nonprofit, and academic sectors at home and abroad, Congress should consider effective ways for federal agencies to share data on ransomware attacks and payments. Finally, in light of ransomware threat actors' growing technological capabilities, any actions aimed at increasing government datasets on the ransomware ecosystem and cryptocurrency ransom payments must be done in conjunction with efforts to track and circumvent ransomware attackers' attempts to conduct increasingly sophisticated attacks.