CRYPTOCURRENCY AND RANSOMWARE ATTACKS: CIRCUMVENTING THE BSA AND MLCA

JENNIFER GUILLEN*

I. INTRODUCTION

Ransomware is a highly costly and increasingly prevalent form of malware attack that continues to harm a wide range of private businesses, hospitals, schools, governments, and public institutions around the world.[1] Not only do these attacks cost victims millions of dollars each year, but they also disrupt access to medical care and divert public resources by targeting and affecting critical infrastructure, posing a serious threat to national security.[2]

The overwhelming majority of ransomware payments are made using cryptocurrency, also referred to as virtual currency or convertible virtual currency ("CVC") in this Note.[3] Ransomware attacks are committed using the internet and can thus be perpetrated from anywhere.[4] Additionally, investigating, prosecuting, and identifying ransomware attackers is difficult because of the inherently decentralized, anonymous, and less-regulated nature of cryptocurrency.[5] While ransomware attacks have posed serious threats to individuals and businesses since the late 1980s, modern advances in technology have increased both the prevalence and severity of such attacks, and have led to the rise of ransomware-as-a-service ("RaaS").[6] RaaS

* J.D. Candidate 2023, University of Southern California Gould School of Law. A big thank you to Professor Eileen Decker for her guidance throughout the drafting of this Note.

[1] INST. FOR SEC. & TECH. & RANSOMWARE TASK FORCE, COMBATING RANSOMWARE 7–10 (2021), https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf.

[2] *Id.* at 8–9.

[3] FIN. CRIMES ENF'T NETWORK, FINANCIAL TREND ANALYSIS: RANSOMWARE TRENDS IN BANK SECRECY ACT DATA BETWEEN JANUARY 2021 AND JUNE 2021 9 (2021), https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf; INST. FOR SEC. & TECH. & RANSOMWARE TASK FORCE, *supra* note 1, at 14. While the three terms are not completely interchangeable, for the purposes of this Note, CVC is a type of cryptocurrency that can be directly converted into real currency, and cryptocurrency is a type of virtual currency. Mitchell Grant, *Digital Money*, INVESTOPEDIA, https://www.investopedia.com/terms/d/digital-money.asp [https://perma.cc/QAZ9-4NHS] (last updated Sept. 27, 2021); Jake Frankenfield, *Virtual Currency*, INVESTOPEDIA, https://www.investopedia.com/terms/v/virtual-currency.asp [https://perma.cc/47DL-VDY7] (last updated Sept. 30, 2021).

[4] INST. FOR SEC. & TECH. & RANSOMWARE TASK FORCE, *supra* note 1, at 15.

[5] *See generally* FIN. CRIMES ENF'T NETWORK, ADVISORY ON RANSOMWARE AND THE USE OF THE FINANCIAL SYSTEM TO FACILITATE RANSOM PAYMENTS 2 (Oct. 1, 2020), https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf; INST. FOR SEC. & TECH. & RANSOMWARE TASK FORCE, *supra* note 1, at 14. *See also* Shawn Turner, Note, *U.S. Anti-Money Laundering Regulations: An Economic Approach to Cyberlaundering*, 54 CASE W. RES. L. REV. 1389, 1407 (2004).

[6] For a timeline of major ransomware attacks since the initial AIDS Trojan/PC Cyborg attack in 1989, see Julian Dossett, *A Timeline of the Biggest Ransomware Attacks: Bitcoin and Other Cryptocurrencies Have Become a Key Tool in Online Crime*, CNET (Nov. 15, 2021), https://www.cnet.com/personal-finance/crypto/a-timeline-of-the-biggest-ransomware-attacks/ [https://perma.cc/5A7U-C2AK]. RaaS has been connected to the proliferation of ransomware attacks, as RaaS makes ransomware attacks an easily

is "a business model between ransomware operators and affiliates in which affiliates pay to launch ransomware attacks developed by operators;" as a result, ransomware has unfortunately become a dangerous tool available even to the most technically unsophisticated criminal actor.[7] Ransomware attacks as they exist today, on a multi-million dollar global scale, started with the CryptoLocker outbreak in 2013, and have continued with increasingly sophisticated and costly attacks, including CryptoWall in 2014, WannaCry, Peyta, and NotPetya in 2017, and DarkSide in 2021.[8] The rising number of cyberattacks, particularly against U.S. targets, has even prompted the Biden administration to make cybersecurity, especially ransomware, a top priority, showing the urgent need for a comprehensive strategy to deter future ransomware attacks.[9]

First, Part II of this Note will define ransomware and explain how ransomware attacks are facilitated using cryptocurrency. Then, Part III will examine two existing United States federal anti-money laundering ("AML") laws, the Bank Secrecy Act and the Money Laundering Control Act of 1986, and their applicability to cryptocurrency.[10] Part IV will analyze the Bank Secrecy Act and the Money Laundering Control Act of 1986, to show that these statutes are poorly applicable to peer-to-peer ("P2P") cryptocurrency payments made to ransomware attackers. Next, Part IV will assess the Biden administration's response to the ransomware issue so far. Finally, Part V will make brief policy recommendations about how to mitigate the facilitation of ransomware attacks using cryptocurrency.[11]

---

accessible tool for criminal actors and enterprises, no matter their level of technological sophistication. *See* Juliana De Groot, *A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time*, DIGIT. GUARDIAN (Dec. 1, 2020), https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time [https://perma.cc/MC4K-BCYE]; INST. FOR SEC. & TECH. & RANSOMWARE TASK FORCE, *supra* note 1, at 14–18, 28–34.

[7] Kurt Baker, *Ransomware as a Service (RaaS) Explained*, CROWDSTRIKE (Feb. 7, 2022), https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/ [https://perma.cc/B52X-GYDJ]. RaaS models can include paying a group to conduct a ransomware attack, getting access to a "build your own ransomware package," and assistance in setting up a victim payment portal and managing a leak site. *Id.*

[8] *See* Dossett, s*upra* note 6; De Groot, *supra* note 6; Alex Hern, *WannaCry, Peyta, NotPetya: How Ransomware Hit the Big Time in 2017*, THE GUARDIAN (Dec. 30, 2017), https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware [https://perma.cc/8STX-KYCP].

[9] The Biden Administration continues to prioritize efforts to counter ransomware attacks on U.S. targets, improve overall U.S. cybersecurity, and increase international cooperation. *See* Press Release, White House, Fact Sheet: Ongoing Public U.S. Efforts to Counter Ransomware (Oct. 13, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/ [https://perma.cc/9MDC-G6NP]; Exec. Order No. 14,028, 86 Fed. Reg. 26,633 (May 12, 2021); Andrew Solender, *'I Will Not Stand Idly By': Biden Says Cybersecurity Will be 'Top Priority' After Giant Hack*, FORBES (Dec. 17, 2020), https://www.forbes.com/sites/andrewsolender/2020/12/17/i-will-not-stand-idly-by-biden-says-cybersecurity-will-be-top-priority-after-giant-hack/?sh=402678165159 [https://perma.cc/TM47-C5XE].

[10] Anti-money laundering laws are laws "intended to prevent criminals from disguising legally obtained funds as legitimate income." Will Kenton, *Anti Money Laundering (AML) Definition*, INVESTOPEDIA (Oct. 20, 2021), https://www.investopedia.com/terms/a/aml.asp [https://perma.cc/6JUP-GKVU]. Typically, these laws focus on financial institutions. *Id.* American AML laws include the Bank Secrecy Act (1970), the Money Laundering Control Act (1986), the Anti-Drug Abuse Act of 1988, the Annunzio-Wylie Anti-Money Laundering Act (1992), the Money Laundering Suppression Act (1994), the Money Laundering and Financial Crimes Strategy Act (1998), the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), and the Intelligence Reform & Terrorism Prevention Act of 2004. *History of Anti-Money Laundering Laws*, FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/history-anti-money-laundering-laws [https://perma.cc/98P5-Z4VW] (last visited Nov. 1, 2021).

[11] This Note's assessment of the Biden Administration is current as of November 1, 2021.

II. THE RELATIONSHIP BETWEEN RANSOMWARE AND CRYPTOCURRENCY

A. THE RANSOMWARE THREAT

Ransomware is malware that, once it infects a computer system or network, encrypts files on that system or network and renders those files entirely unusable unless the victim pays a ransom.[12] While ransomware can infiltrate a system or network through a variety of methods, it is most commonly spread through spoofed emails that trick individuals within an organization into opening attachments that contain the malware, a technique also known as "phishing."[13] Losing the encrypted data by failing to pay the ransom can cripple the ability of businesses and institutions to operate, such as by delaying patient treatments at hospitals, diverting public resources otherwise earmarked for public programs, and losing vital customer, vendor, payment, and other business data that is essential for day-to-day operations.[14] Moreover, the potential sale or leak of the stolen data after a ransomware attacker first demands a ransom to decrypt the data and then demands an additional ransom to also not release the data publicly, also known as a "double extortion," carries huge privacy implications for individuals.[15] Furthermore, the U.S. government, and other governments and enforcement agencies around the world, generally advise against paying the ransom and may possibly even sanction victims who meet the ransomware attackers' demands. [16] However, for many individuals and businesses, not paying the ransom could unfortunately be even more harmful to their businesses and personal lives than the costly ransom itself.

Ransomware attacks are increasing in number and severity, not just in the United States, but around the world.[17] In 2021, there was a one hundred

---

[12] INST. FOR SEC. & TECH. & RANSOMWARE TASK FORCE, *supra* note 1, at 11.

[13] FIN. CRIMES ENF'T NETWORK, *supra* note 3, at 11.

[14] INST. FOR SEC. & TECH. & RANSOMWARE TASK FORCE, *supra* note 1, at 7–10*; see also How Ransomware Is a Big Problem for Small Business—And What to Do About It*, INSUREON: INSUREON SMALL BUS. BLOG, https://www.insureon.com/blog/how-ransomware-is-a-big-problem-for-small-business [https://perma.cc/56TP-2R6K]. Potential implications for individuals, either through losing personal information or facing delays in receiving essential health services, have been made especially visible during the COVID-19 pandemic, during which there has been a significant growth (up 34% from 2019 in 2020) in the number of ransomware attacks against the health care sector. Ruti Gafni & Tal Pavel, *Cyberattacks Against the Health-Care Sectors During the COVID-19 Pandemic*, 30 INFO. & COMPUT. SEC. 137, 142–44 (2022).

[15] INST. FOR SEC. & TECH. & RANSOMWARE TASK FORCE, *supra* note 1, at 9.

[16] *See* INST. FOR SEC. & TECH. & RANSOMWARE TASK FORCE, *supra* note 1, at 49–50; OFF. FOREIGN ASSETS CONTROL, UPDATED ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS (Sept. 21, 2021), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf (detailing an updated advisory issued by the Department of the Treasury's Office of Foreign Assets Control (OFAC) regarding sanction risks associated with ransomware payments); Raphael Satter, *Companies May Be Punished for Paying Ransoms to Sanctioned Hackers—U.S. Treasury*, REUTERS (Oct. 1, 2020), https://www.reuters.com/article/us-treasury-cyber/companies-may-be-punished-for-paying-ransoms-to-sanctioned-hackers-u-s-treasury-idUSKBN26M77U [https://perma.cc/CQ8V-2J33]; S.M. Irwin & Caitlin Dawson, *Following the Cyber Money Trail: Global Challenges When Investigating Ransomware Attacks and How Regulation Can Help*, 22 J. MONEY LAUNDERING CONTROL 110, 113 (2019).

[17] *See* Geoff Blaine, *Tipping Point: SonicWall Exposes Soaring Threat Levels, Historic Powers Shifts in New Report*, SONICWALL (Mar. 16, 2021), https://blog.sonicwall.com/en-us/2021/03/sonicwall-exposes-soaring-threats-historic-power-shifts-in-new-report/ [https://perma.cc/S8AH-Z8UE](reporting that worldwide, Ransomware attacks are up 62% from 2020 to 2021); Ramarcus Baylor, Jeremy Brown

and forty-eight percent increase in global ransomware attacks.[18] In the United States, in the first six months of 2021 alone, FinCEN received 635 ransomware-related Suspicious Activity Reports ("SARs") related to 458 transfers with a total value of five hundred and ninety million dollars, which is a forty-two percent increase from all of 2020 and represents the highest total value in a decade.[19] Moreover, projections for the rest of 2021 anticipate that the value of ransomware-related transactions made by American victims of ransomware attacks will be more than the "previous ten years combined."[20]

B. CRYPTOCURRENCY AND CRIME

Since existing AML legislation in countries like the United States focuses on financial institutions, cryptocurrency and other associated internet technologies that circumvent those traditional institutions are increasingly used to facilitate crime, as evidenced by the prevalent demand for cryptocurrency in lieu of cash for ransomware payments.[21]

While an in-depth analysis of cryptocurrency is beyond the scope of this Note, cryptocurrency is virtual currency that largely emerged in 2009 with the invention of Bitcoin.[22] Cryptocurrency is entirely intangible, as it is made up of a string of digital code representing balances in a blockchain ledger.[23]

& John Martineau, *Extortion Payments Hit New Records as Ransomware Crisis Intensifies*, PALO ALTO NETWORKS (Aug. 9, 2021), https://www.paloaltonetworks.com/blog/2021/08/ransomware-crisis/ [https://perma.cc/J4JZ-3VRZ] (reporting that the average ransomware payment climbed 82% in 2021 from $312,000 to $570,000); Emsisoft Malware Lab, *The Cost of Ransomware in 2021: A Country-by-Country Analysis*, EMSISOFT BLOG (Apr. 27, 2021), https://blog.emsisoft.com/en/38426/the-cost-of-ransomware-in-2021-a-country-by-country-analysis/ [https://perma.cc/4EGN-YZZR] (reporting ransom demand costs and downtimes for various countries); Press Release, G7, Ransomware Annex to G7 Statement (Oct. 13, 2020), https://home.treasury.gov/system/files/136/G7-Ransomware-Annex-10132020_Final.pdf (G7 finance ministers and central bank governors stating concerns from the G7 over "malicious cyber-attacks, especially ransomware").

[18] *The Year of Ransomware Continues with Unprecedented Late-Summer Surge*, SONICWALL, https://www.sonicwall.com/news/sonicwall-the-year-of-ransomware-continues-with-unprecedented-late-summer-surge/ [https://perma.cc/XBJ6-8L2Z].

[19] FIN. CRIMES ENF'T NETWORK, *supra* note 3, at 1–3.

[20] *Id.* at 3.

[21] *See* Turner, *supra* note 5, at 1407; INST. FOR SEC. & TECH. & RANSOMWARE TASK FORCE, *supra* note 1, at 14; FIN. CRIMES ENF'T NETWORK, *supra* note 3, at 9. Cryptocurrency has also been used to facilitate terrorism, drug trafficking, and organized crime around the world due to its decentralized, extraterritorial, and anonymous nature. *E.g.*, James Martin, *Lost on the Silk Road: Online Drug Distribution and the 'Cryptomarket'*, 4 CRIMINOLOGY & CRIM. JUST., 351, 352–56 (2014); Angela S. M. Irwin & George Milad, *The Use of Crypto-Currencies in Funding Violent Jihad*, 19 J. MONEY LAUNDERING CONTROL 407, 407–11 (2016).

[22] Bitcoin is a type of cryptocurrency that emerged largely due to a famous 2008 white paper published under a pseudonym: Satoshi Nakamoto. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008), https://bitcoin.org/bitcoin.pdf; *see also* Chad Albrecht, Kristopher McKay Duffin, Steven Hawkins & Victor Manuel Morales Rocha, *The Use of Cryptocurrencies in the Money Laundering Process*, 22 J. MONEY LAUNDERING CONTROL 210, 212–13 (2019); Ben Gilbert & David Rosenthal, *The Complete History and Analysis of Bitcoin*, ACQUIRED, at 28:22–36:20 (Jan. 18, 2021), https://www.acquired.fm/episodes/bitcoin [https://perma.cc/74HX-Y4Y6]. The concept of cryptocurrency, however, goes back to American Cryptographer David Chaum in 1983, who proposed electronic cash "which emulated fiat currency but allowed greater levels of privacy and security" using an "untraceable payment system . . . [and] blind signatures to prevent financial institutions from linking transactions to users." Irwin & Dawson, *supra* note 16, at 121.

[23] *See* INST. FOR SEC. & TECH. & RANSOMWARE TASK FORCE, *supra* note 1, at 14; Albrecht et al., *supra* note 22, at 212–13; *Bitcoin Exchanges*, BITCOIN, https://bitcoin.org/en/exchanges#international [https://perma.cc/MD68-49ET]. For examples of P2P exchanges, U.S. and international, that allow direct transfer without intermediaries see Carol Goforth, *The Lawyer's Cryptionary: A Resource for Talking to Clients About Crypto-Transactions*, 41 CAMPBELL L. REV. 47, 58 (2019).

The virtual currency can be traded either directly peer-to-peer ("P2P")—between two users without any intermediary—or through a financial intermediary such as a traditional bank or cryptocurrency exchange.[24] Each individual "coin" constitutes a small portion of the blockchain on which the coin is encrypted, and users called "miners" maintain a public ledger, which provides a record of all transactions that anyone can access by constantly validating transactions and who owns which coins.[25]

Depending on the type of cryptocurrency, the total supply can be finite, such as with Bitcoin, to create built-in scarcity and decrease the risk of inflation.[26] Cryptocurrency exchanges function like other traditional currency exchanges do, by operating as an online platform that allows users to exchange different virtual currencies or to convert virtual currencies to real currencies.[27] Cryptocurrency exchanges are either "centralized" or "decentralized"—the former involves the exchange acting as an intermediary that monitors transactions and holds users' private keys and wallets, while the latter does not involve the exchange acting in an intermediary role, instead just serving as a forum to connect potential buyers and sellers.[28]

Cryptocurrency coins are stored in encrypted "wallets," either on a mobile device, desktop, or in hardware form, with different kinds of wallets providing users with varying levels of control and privacy.[29] Users can then exchange cryptocurrency using public and private keys, which are generated for one-time use for each individual transaction.[30] The public key allows users to receive a transfer of coins, akin to providing a bank account number

---

[24] INST. FOR SEC. & TECH. & RANSOMWARE TASK FORCE, *supra* note 1, at 14; Albrecht et al., *supra* note 22, at 212–13; *Bitcoin Exchanges*, *supra* note 23; Goforth, *supra* note 23.

[25] This is an accurate description of Bitcoin and other types of cryptocurrencies. However, there are differences between different types, such as the accessibility of the blockchain ledger. On Bitcoin, see Albrecht et al., *supra* note 22, at 212–13; Gilbert & Rosenthal, *supra* note 22; s*ee also* Jake Frankenfield, *Cryptocurrency Explained with Pros and Cons for Investment*, INVESTOPEDIA, https://www.investopedia.com/terms/c/cryptocurrency.asp [https://perma.cc/A7NL-SKQB] (last updated Oct. 30, 2021). Without going into too much detail the so-called "mining" of cryptocurrency "is the process by which . . . transactions are verified and recorded on the blockchain. . . . [Miners] use powerful computers to complete complex mathematical functions called hashes" and it is through mining that "new blocks of Bitcoin transactions are verified and added to the . . . blockchain." Wayne Duggan, *Bitcoin Mining Definition*, U.S. NEWS (Jan. 25, 2022), https://money.usnews.com/investing/term/bitcoin-mining#:~:text=Bitcoin%20mining%20is%20the%20process,complex%20mathematical%20functions%20called%20hashes. Anyone can mine, though a powerful computer is necessary, and the networked effect allows cryptocurrency users to trust the public ledger even without having to rely on a central authority like a government to verify that transactions are legitimate. *Id.*

[26] Andria van der Merwe, *A Taxonomy of Cryptocurrencies and Other Digital Assets*, 41 REV. BUS. 30, 32 (2021). For a discussion of the difference between fixed and unlimited supply cryptocurrency see Dany Chetverikov, *Fixed vs. Unlimited Supply in Crypto and Fiat*, NIMERA (Sept. 29, 2020), https://www.nimera.io/blog/crypto-fixed-vs-unlimted-supply [https://perma.cc/PR3L-SCF4].

[27] Nathan Reiff, *What Are Centralized Cryptocurrency Exchanges*, INVESTOPEDIA (last modified Aug. 27, 2021), https://www.investopedia.com/tech/what-are-centralized-cryptocurrency-exchanges/ [https://perma.cc/X6CL-8KWF].

[28] *Id*; Lakshit Madaan, *Centralized vs. Decentralized Exchange: Which Is the Best*, LINKEDIN (Oct. 31, 2021), https://www.linkedin.com/pulse/centralized-vs-decentralized-exchange-which-best-lakshit-madaan/?trk=articles_directory [https://perma.cc/HYM3-UXMV].

[29] *See Storing Bitcoins*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Storing_bitcoins [https://perma.cc/W6W9-3T7Z].

[30] *See* Jake Frankenfield, *Private Key*, INVESTOPEDIA, [hereinafter Frankenfield, *Private Key*], https://www.investopedia.com/terms/p/private-key.asp [https://perma.cc/WQJ9-T4JL] (last updated June 29, 2020); Jake Frankenfield, *Public Key*, INVESTOPEDIA, [hereinafter Frankenfield, *Public Key*], https://www.investopedia.com/terms/p/public-key.asp [https://perma.cc/JC4T-DXCF] (last updated June 24, 2021); Gilbert & Rosenthal, *supra* note 22, at 28:22–55:21.

to which to send money.[31] Then, the private key, which is linked to the public key and is stored in the user's digital wallet, is used by recipients to decrypt the transaction and withdraw the coins from the public key address to their personal wallet.[32]

Thus, a cryptocurrency transfer occurs as follows:

1) a sender enters their private key, which is stored in their wallet, into a "cryptographic hash" that lets the "network software validate a new entry on the [public] ledger," showing the change in ownership of the coin;
2) the coin is then sent to a receiver's provided public key address, just like a bank account number, and;
3) only the receiver's private key can decrypt the transfer and withdraw the coin from the public key address to the receiver's private wallet.[33]

Transactions are recorded in the public ledger using only the public key address of both the receiver and the sender, and not their names or any other identifying information, thus preserving the anonymity of both parties.[34]

The underlying idea of cryptocurrency is to create a decentralized anonymous exchange for currency that is not controlled by any government and does not have to rely on financial institutions to serve as intermediaries to facilitate payments.[35] Instead, the blockchain verifies that users are trading coins they actually have, allows anyone to review the ledger to verify transactions, and lets users trade directly with one another, P2P, without any intermediary.[36] Additional benefits of cryptocurrency also include overall "lower costs and fees, . . . fewer risks for merchants, . . . increased speed and transfer/payment, and . . . less susceptibility to government manipulation. . . ."[37]

While the distributed ledger structure of cryptocurrency means that ransomware payments can be traced using the public ledger, payments still remain difficult to trace back to individuals because of the anonymous and decentralized nature of exchanges made using cryptocurrency.[38] Even though miners monitor transactions and managers update the public ledger, they do not know who is on either side of the transaction or the source of the money.[39] Users remain anonymous because transactions are tied to public keys that are generated for one-time use and then discarded and are not tied to personal identifying information.[40] In other words, one can see that a transaction occurred but cannot identify the sender or recipient.

---

[31] Frankenfield, *Public Key*, *supra* note 30.

[32] *Id.*

[33] *See* Nakamoto, *supra* note 22*;* Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 86 Fed. Reg. 3897, at 5 (proposed Jan. 15, 2021), [hereinafter Requirements] https://public-inspection.federalregister.gov/2020-28437.pdf.

[34] *See* Requirements, *supra* note 33; Gilbert & Rosenthal, *supra* note 22.

[35] *See* Nakamoto, *supra* note 22; Gilbert & Rosenthal, *supra* note 22.

[36] *See* Nakamoto, *supra* note 22; Gilbert & Rosenthal, *supra* note 22; Frankenfield, *supra* note 25.

[37] Kevin V. Tu & Michael Meredith, *Rethinking Virtual Currency Regulation in the Bitcoin Age*, 90 WASH. L. REV. 271, 282 (2015).

[38] Mohammed Ahmad Naheem, *Exploring the Links Between AML, Digital Currencies and Blockchain Technology*, 22 J. MONEY LAUNDERING CONTROL 515, 517–18 (2019).

[39] *Id.*

[40] *Id.*

The most popular cryptocurrency is Bitcoin, but there are many other types of cryptocurrencies and some are more privacy-focused than others.[41] For example, transactions made using Monero "are made anonymous by use of an integrated mixing process automatically applied to every transaction" instead of making all transactions visible on the public ledger.[42] The use of cryptocurrency like Monero can thus further complicate tracing and recovering ransomware payments. [43] With the growth in popularity of cryptocurrency like Bitcoin, there has also been a corresponding "growth of an industry of virtual currency based businesses designed to facilitate Bitcoin transactions."[44] Various third-party entities provide services such as exchanging Bitcoin into traditional, also known as fiat, currency, storing users' Bitcoins for them, facilitating transfers between users; some major online vendors and companies have even started accepting Bitcoin as a method of payment.[45] As a result, virtual currency has become increasingly easier to use and exchange, thus making it accessible to more and more users, including both the victims and perpetrators of ransomware attacks.[46]

When cryptocurrency is used to pay a ransom in a ransomware attack, to further complicate tracing funds, ransomware attackers will move the funds quickly out of their wallets to avoid detection and obfuscate the funds' source, making it very difficult to trace the origin of the coins and tie the coins to an identifiable group or individual.[47] This tactic to launder cryptocurrency involves three steps: placement, layering, and integration.[48] "Placement" means that the source of the money is hidden after it is received, such as by withdrawing the funds to an unhosted private wallet or converting the funds several times to different currencies.[49] "Layering," which is easier to do with cryptocurrency than with real currency, means moving the funds by creating "multiple complex financial transactions including wire

[41] Goforth, *supra* note 23, at 74 (discussing a variety of cryptocurrencies, including Bitcoin and Monero). Other popular cryptocurrencies include Ethereum, Stellar, Binance Coin, Cardano, and the often-teased Dogecoin. John Hyatt, *Decoding Crypto: The 10 Most Popular Cryptocurrencies*, NASDAQ (Aug. 5, 2021), https://www.nasdaq.com/articles/decoding-crypto%3A-the-10-most-popular-cryptocurrencies-2021-08-05.

[42] Goforth, *supra* note 23, at 74.

[43] *Id.*

[44] Tu & Meredith, *supra* note 37, at 273.

[45] *Id.* For examples of companies that accept cryptocurrency as forms of payment, including Microsoft, Paypal, and Newegg, see Andrew Lisa, *10 Major Companies That Accept Bitcoin*, GOBANKINGRATES (Jan. 31, 2022), https://www.gobankingrates.com/money/business/10-major-companies-that-accept-bitcoin/. In addition, to highlight the growing popularity and mainstream acceptance of Bitcoin, in 2021 El Salvador became the first country in the world to adopt bitcoin as legal tender. Oscar Lopez & Ephrat Livni, *In Global First, El Salvador Adopts Bitcoin as Currency*, N.Y. TIMES (Oct. 7, 2021), https://www.nytimes.com/2021/09/07/world/americas/el-salvador-bitcoin.html [https://perma.cc/B3KH-JM39].

[46] Tu & Meredith, *supra* note 37, at 285–91.

[47] *See* INST. FOR SEC. & TECH. & RANSOMWARE TASK FORCE, *supra* note 1*;* FIN. CRIMES ENF'T NETWORK, *supra* note 3, at 9.

[48] John W. Bagby, David Reitter & Philip Chwistek, *An Emerging Political Economy of the Blockchain: Enhancing Regulatory Opportunities*, 88 UMKC L. REV. 419, 469–70 (2019). An unhosted wallet is a cryptocurrency wallet that "is not hosted by a third-party financial system." *Requirements for Certain Transactions Involving Certain Convertible Virtual Currency or Digital Assets Frequently Asked Questions (FAQs)*, U.S. DEP'T TREASURY (Dec. 18, 2020) [hereinafter *Requirements*], https://home.treasury.gov/system/files/136/2020-12-18-FAQs.pdf. Because no financial institution is involved as an intermediary, unhosted wallets make "determin[ing] who is accessing or in control of the use of cryptocurrencies in [a] . . . wallet" much more difficult. *Id.* As a result, unhosted wallets are frequently used to further criminal activity. *Id.*

[49] *Requirements*, *supra* note 48.

transfers, monetary instruments, and asset purchases or sales" that "may also involve moving funds to other countries."[50] Finally, "[i]ntegration" means the funds are converted into real currency or real assets so they can "reenter legitimate economy," at which point tracing their origins is incredibly difficult.[51] In addition to these methods, while law enforcement agencies could theoretically track a ransom by carefully analyzing transactions on the public blockchain ledger with the help of tracking technology, technologically-savvy ransomware attackers will use "anonymization services like Dark Wallet and Bitcoin Fog" to further anonymize transactions by "piggybacking" on non-illicit transactions, similar to how traditional money laundering works, to comingle legitimate and illicit cryptocurrency funds and disperse them among various new addresses.[52] Thus, combining the already anonymous and decentralized nature of cryptocurrency with these aforementioned anonymization services and a Tor Browser, makes tracing ownership of coins in order to be able to prosecute individual ransomware attackers extremely difficult.[53]

Because ransomware attacks are predominantly financially motivated, regulatory attempts by the U.S. government have largely focused on regulating cryptocurrency exchanges.[54] The U.S. government has historically used Know Your Customer ("KYC") requirements and existing AML legislation, to minimize the availability of those cryptocurrency payment systems and thus decrease the profitability of ransomware.[55] But even if centralized cryptocurrency exchanges are used instead of trading directly P2P, they are primarily foreign exchanges and often in jurisdictions with "opaque ownership structures" or "inadequate AML . . . compliance standards" that may not employ KYC requirements, may not report suspicious transactions, or may not otherwise cooperate with U.S. AML enforcement efforts.[56] Thus, because the focus of existing AML laws is on financial institutions or, by extension, cryptocurrency exchanges, the only opportunity that the U.S. government has to exercise influence over cryptocurrency transactions is when transfers use more traditional financial intermediaries or when individuals act as intermediaries themselves; as a result, some transfers, such as P2P transactions, remain beyond the government's reach.[57]

---

[50] *Id.*

[51] *Id.*

[52] Irwin & Dawson, *supra* note 16, at 122.

[53] *Id.* A Tor Browser protects users' privacy on the internet by routing traffic "through three random servers (also known as relays) . . . then sends the traffic out onto the public internet." *About Tor Browser*, THE TOR PROJECT, https://tb-manual.torproject.org/about/ [https://perma.cc/L7EF-KG8T] (last visited Nov. 1, 2021). As a result, it becomes extremely difficult to identify a user or their real location based on the user's IP address because the connection will appear to be "a connection coming from the Tor network instead of [the user's] real IP address." *Id.*

[54] The conclusion that ransomware attacks are primarily financially motivated is supported by both the demand for a ransom as well as the continued growth of the ransomware-as-a-service ("RaaS") business model. *See* INST. FOR SEC. & TECH. & RANSOMWARE TASK FORCE, *supra* note 1, at 14–18, 28–34.

[55] *See* James A. Sherer, Melinda L. McLellan, Emily R. Fedeles & Nichole L. Sterling, *Ransomware—Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web,* 23 RICH. J. L. & TECH. 1, 18–20 (2017).

[56] FIN. CRIMES ENF'T NETWORK, *supra* note 3, at 12.

[57] *See id.*; FIN. CRIMES ENF'T NETWORK, FIN-2013-G001, APPLICATION OF FINCEN'S REGULS. TO PERS. ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES 3–5 (Mar. 18, 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

III. EXISTING ANTI-MONEY LAUNDERING LAWS AND CRYPTOCURRENCY

While the Bank Secrecy Act and the Money Laundering Control Act of 1986 are not the only AML laws in the U.S. used to combat the use of cryptocurrency to facilitate crime like ransomware attacks, they are two of the biggest pieces of legislation and are thus subjects of analysis for this Note regarding their applicability to ransomware cryptocurrency payments.

A. THE BANK SECRECY ACT

The Bank Secrecy Act ("BSA") is AML legislation that Congress enacted in 1970 to prevent financial institutions from being used as money-laundering intermediaries.[58] The BSA creates reporting and recordkeeping requirements for a financial institution to, among other requirements, create "certain reports or records that are highly useful in—criminal, tax, or regulatory investigations . . ." and to establish an information-sharing network with the government to help facilitate the tracking of and prevent the "laundering of money and financing of terrorism."[59] Specifically, the reporting and recordkeeping requirements include filing various reports with the government, keeping all records required under the Act for five years, "keep[ing] records of cash purchases of negotiable instruments" between three thousand dollars and ten thousand dollars, "fil[ing] reports of cash transactions exceeding ten thousand dollars (daily aggregate amount), and reporting suspicious activity, by filing SARs, that might be linked to money laundering or other criminal activities."[60] In addition, the BSA requires financial institutions to "develop, administer, and maintain" internal AML programs "that ensur[e] and monito[r] compliance with the BSA," which includes establishing internal controls to ensure compliance, independent testing for compliance, appointing a compliance officer, and providing specialized bank personnel training.[61] Failure to comply with the BSA, including the failure to establish and maintain a proper AML program, can result in substantial civil and criminal penalties.[62] In sum, the applicability and efficacy of the BSA thus relies on the assistance of regulated financial entities to assist the U.S. government in "identif[ying] and investigati[ng] suspicious transactions and customers."[63]

In 1995, Congress established the Financial Crimes Enforcement Network ("FinCEN") to "implement, administer, and enforce compliance

---

[58] *See* LILIAN B. KLEIN, BANK SECRECY ACT/ANTI-MONEY LAUNDERING, 1 (2008); *FinCEN's Mandate from Congress*, FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/resources/statutes-regulations [https://perma.cc/9GKB-WVFQ]; Turner, *supra* note 5, at 1402.

[59] 31 U.S.C. § 5311.

[60] FIN. CRIMES ENF'T NETWORK, *supra* note 58*; see also* Catherine Martin Christopher, *Whack-A-Mole: Why Prosecuting Digital Currency Exchanges Won't Stop Online Money Laundering*, 18 LEWIS & CLARK L. REV. 1, 7 (2014); KLEIN, *supra* note 58, at 12–13.

[61] KLEIN, *supra* note 58, at 9–11*; see also* DENNIS COX, HANDBOOK OF ANTI-MONEY LAUNDERING 134–35 (2014).

[62] Stan Sater, *Do We Need KYC/AML: The Bank Secrecy Act and Virtual Currency Exchanges*, 73 ARK. L. REV. 397, 404 (2020) (explaining that civil penalties can range from $500–50,000 for negligent violations and "$25,000 or the amount of the transaction, whichever is greater.").

[63] Tu & Meredith, *supra* note 37, at 322.

with" the BSA.[64] As well, Congress amended the BSA to help improve the tracing of money laundering over wire transfers and to address the circumvention of the BSA, by expanding BSA requirements beyond traditional financial institutions.[65] The BSA was also amended in 2002 by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("Patriot Act"), which added KYC requirements for banks to take reasonable steps to identify customers, expanded asset-seizure power, and further expanded the applicability of the BSA to actors within the financial services sector, foreign banks, and individual "money transmitters."[66] In addition, the passage of the Patriot Act in 2002 established FinCEN as "an official Bureau within the Treasury Department 'to support law enforcement efforts and foster interagency and global cooperation against domestic and international financial crimes.' "[67]

In the United States, because cryptocurrency is regulated as a Money Services Business ("MSB") instead of as currency, its regulation falls under the Bank Secrecy Act.[68] However, when FinCEN released guidance clarifying the applicability of the BSA to virtual currency in 2013, it stated that an individual user of virtual currency "is not an MSB under FinCEN's regulations and therefore not subject to MSB registration, reporting, and recordkeeping regulations," but that an administrator or exchanger is; as a result, the applicability of the BSA is not straightforward.[69] Merely accepting or sending virtual currency is not enough to subject an individual to BSA regulation; the user would have to be providing money-transmission services as an intermediary by either selling or exchanging cryptocurrency.[70] Thus, users, including investors and miners of cryptocurrency, may not be regulated as money transmitters by FinCEN under the BSA.[71] In 2019, FinCEN released additional guidance stating that the BSA applies to certain business models that deal in or facilitate the exchange of CVC, such as centralized cryptocurrency exchanges.[72] Finally, both the 2013 and 2019 FinCEN guidances were codified in the Anti-Money Laundering Act ("AMLA") of 2020.[73]

[64] FIN. CRIMES ENF'T NETWORK, *supra* note 58.

[65] *See* Turner, *supra* note 5, at 1403; Danton Bryans, Note, *Bitcoin and Money Laundering: Mining for an Effective Solution,* 89 IND. L.J. 441, 456 (2014).

[66] *See* Christopher, *supra* note 60, at 9; COX, *supra* note 61, at 128–32; Turner, *supra* note 5, at 1404.

[67] Sater, *supra* note 62, at 402.

[68] Irwin & Dawson, *supra* note 16, at 119.

[69] FIN. CRIMES ENF'T NETWORK, *supra* note 58, at 1.

[70] *See id*.

[71] Tu & Meredith, *supra* note 37, at 306.

[72] FIN. CRIMES ENF'T NETWORK, FIN-2019-G001, APPLICATION OF FINCEN'S REGULS. TO CERTAIN BUS. MODELS INVOLVING CONVERTIBLE VIRTUAL CURRENCIES 3–5 (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

[73] H.R. Con. Res. 6395, 116th Cong. (2021) (enacted) (cited as the "William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021"); *see also Anti-Money Laundering Act of 2020*, FIN. CRIMES ENF'T NETWORK (2021), https://www.fincen.gov/sites/default/files/shared/20210615%20AMLA%20FinCEN%20One%20Pager_FINAL.pdf; Selva Ozelli, *The United States Updates Its Crypto AML/CFT Laws*, COIN TEL. (Jan. 24, 2021), https://cointelegraph.com/news/the-united-states-updates-its-crypto-aml-cft-laws [https://perma. cc/H3RN-CV6C].

B. THE MONEY LAUNDERING CONTROL ACT OF 1986

The Money Laundering Control Act of 1986 ("MLCA") makes money laundering, knowingly assisting in money laundering, engaging in transactions involving property derived from criminal activity, or structuring transactions to avoid reporting requirements, a federal crime.[74] The Act was passed in response to both "the widespread non-compliance of banks with the reporting requirements of the BSA"[75] and money launderers circumventing BSA reporting requirements by ensuring their transactions never exceeded ten thousand dollars.[76] The MLCA addressed these issues by criminalizing any attempt to structure payments to avoid BSA reporting requirements, expanding the applicability of AML legislation to individuals by defining, in general terms, a wider range of laundering activities by individuals, and by greatly expanding the list of entities included under the umbrella of "financial institution."[77] The MLCA is codified in two U.S. Code sections: 18 U.S.C. § 1956 and 18 U.S.C. § 1957. To be convicted under either section, the individual engaging in the transaction must be using funds derived from specified unlawful activity ("SUA"). While the government must be able to tie the money involved in the transaction to SUA, the defendant does not have to know that the money originated from SUA.[78] The defendant only needs to be aware that the money involved in the transaction was not derived from a legitimate source.[79] If convicted under either section, an individual can face up to twenty years in prison as well as substantial criminal and civil penalties.[80]

Section 1956 is concerned with transactions involving money derived from SUAs where the transaction is accomplished: "(1) with the intent to promote SUA, (2) with the intent to evade taxation, (3) knowing the transaction is designed to conceal laundering, or (4) knowing the transaction is designed to avoid AML reporting requirements."[81] To prosecute an individual under section 1956, the government must show: "(A) knowledge; (B) the existence of proceeds derived from a specified unlawful activity; (C) the existence of a financial transaction; and (D) intent to conceal, promote, or evade."[82] Section 1956(7) specifically defines which activities constitute SUA and thus confines application of the MLCA to transactions involving proceeds derived from crimes that fall within the list in section 1956(7) and, by extension, 18 U.S.C. § 1961(1).[83] The list is extensive and if the

[74] Turner, *supra* note 5, at 1405; Jonathan P. Straub, Note, *The Prevention of E-Money Laundering: Tracking the Elusive Audit Trail*, 25 SUFFOLK TRANSNAT'L L. REV. 515, 524 (2002).
[75] Tu & Michael Meredith, *supra* note 37, at 323.
[76] Straub, *supra* note 74.
[77] *Id.*; *see* 18 U.S.C. §§ 1956–57.
[78] Turner, *supra* note 5, at 1405–06.
[79] *Id.*
[80] Criminal penalties include "fines of up to $500,000 or twice the value of the property involved in the transaction, whichever is greater" and civil penalties include "fines of $10,000 or the value of the property, funds, or monetary instruments involved in the transaction, whichever is greater." Christopher, *supra* note 60, at 4.
[81] 18 U.S.C. § 1956*; see also* Bryans, *supra* note 65, at 459–60.
[82] Emily Wood, *Money Laundering*, 58 AM. CRIM. L. REV. 1223, 1230 (2021).
[83] 18 U.S.C. §§ 1956, 1961(1).

government can show the transaction's funds are derived from SUA on that list, an individual can be convicted under the MLCA.[84]

Section 1957 prohibits "knowingly engag[ing] or attempt[ing] to engage in a monetary transaction in criminally derived property that is of a value greater than ten thousand dollars and is derived from [SUA]."[85] In addition, a monetary transaction is defined as "the deposit, withdrawal, transfer, or exchange, in or affecting interstate or foreign commerce, of funds or a monetary instrument by, through, or to a financial institution including any transaction that would be a financial transaction under § 1956(c)(4)(B)."[86] Thus, the elements the government must prove to convict under section 1957 are: (1) an individual knowingly engaged or attempted to engage in (2) a monetary transaction exceeding ten thousand dollars (3) involving a financial institution (4) and the property being exchanged is derived from SUA.[87] Section 1957 is more easily applied than section 1956 because it does not require proof of specific criminal intent or knowledge nor does the sender or receiver actually need to launder funds; rather, the sender or receiver just needs to attempt to do so.[88]

IV. APPLYING EXISTING AML LAWS TO RANSOMWARE CRYPTOCURRENCY PAYMENTS

In recent history, the U.S. government has had some successes using the BSA and MLCA to prosecute criminal intermediaries who use cryptocurrency to facilitate illicit activities. In October 2013, Silk Road, a website that facilitated the exchange of illicit goods and services using Bitcoin, was shut down by the FBI and the site's operator was convicted for violating the BSA.[89] Also in 2013, Liberty Reserve, a website that allowed users to trade its virtual currency without requiring identifying information and that was used extensively for crime, was shut down and its administrators were charged under the MLCA for conspiracy to commit money laundering.[90] More recently, in 2015, Ripple Labs, a cryptocurrency provider, was fined seven hundred thousand dollars under the BSA for failing to establish proper AML programs.[91] And in 2021, the cryptocurrency exchange BitMEX was fined one hundred million dollars for failing to implement a compliant AML program and report suspicious activities.[92]

---

[84] Wood, *supra* note 82.

[85] 18 U.S.C. § 1957*; see also* Wood, *supra* note 82, at 1229.

[86] 18 U.S.C. § 1957(f)(1).

[87] Andres Rueda, *The Implications of Strong Encryption Technology on Money Laundering*, 12 ALB. L. J. SCI. & TECH. 1, 11 (2001).

[88] *See* Bryans, *supra* note 65, at 460.

[89] Silk Road can be thought of as the Amazon of the dark web: an online black market where users could primarily purchase various illicit substances. *See* Gilbert & Rosenthal, *supra* note 22, at 1:04:54–1:16:30; Lawrence Trautman, *Virtual Currencies; Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox*, 20 RICH. J. L. & TECH. 1, 91–93 (2014); Sater, *supra* note 62, at 421–22.

[90] Trautman, *supra* note 89, at 86–91.

[91] Malcolm Campbell-Verduyn, *Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance*, 69 CRIME L. & SOC. CHANGE 283, 290 (2018).

[92] *FinCEN Announces $100 Million Enforcement Action Against Unregistered Futures Commission Merchant BitMEX for Willful Violations of the Bank Secrecy Act,* FIN. CRIMES ENF'T NETWORK (Aug. 10, 2021), https://www.fincen.gov/news/news-releases/fincen-announces-100-million-enforcement-action-against-unregistered-futures [https://perma.cc/9ABY-NKDD].

However, these successful applications of the BSA and MLCA were to intermediary money transmitters, but both the BSA and MLCA are much harder to apply to non-intermediary individuals that trade P2P.

A. THE BANK SECRECY ACT

The difficulty in applying the BSA to individual ransomware attackers likely stems from the fact that the BSA was written to apply to the financial institutions that existed at the time that the BSA was originally passed in 1970, long before the technology enabling cryptocurrency exchanges existed. Resultingly, the BSA is not readily applicable to cryptocurrency transactions that do not involve a traditional financial institution, such as the P2P cryptocurrency transactions between individual users, and in this case, between ransomware attackers and their victims.

First, while FinCEN confirmed in its 2019 guidance that the BSA applies to cryptocurrency exchanges, the applicability of the BSA to individuals is not so straightforward.[93] While the BSA *can* apply to individuals, it can only apply to certain types of individuals who qualify as "money transmitters," and are thus considered a Money Services Business ("MSB") that is subject to BSA reporting and recordkeeping requirements and must register with the government within 180 days of beginning operations.[94] In its 2013 guidance, FinCEN differentiated between users, administrators, and exchangers.[95] A user is "a person [who] obtains virtual currency to purchase goods or services."[96] FinCEN clarified that merely obtaining CVC and using that virtual currency to "purchase real or virtual goods or services" does not transform a user into a MSB subject to BSA regulation because that behavior does not constitute money transmission.[97] Relatedly, FinCEN also made clear that a user who "converts Bitcoin into real currency or another convertible virtual currency will not be deemed an exchange of convertible virtual currency based upon such conversion, so long as the conversion is 'solely for the user's own purposes.'"[98] On the other hand, the other two categories of individuals, exchangers and administrators, are subject to BSA regulation because they are considered money transmitters and thus qualify as MSBs.[99] FinCEN defines an exchanger as "a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency."[100] FinCEN defines an administrator as "a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has

---

[93] *See* FIN. CRIMES ENF'T NETWORK, *supra* note 72, at 23–24.

[94] FIN. CRIMES ENF'T NETWORK, *supra* note 57, at 1–3; *see also* Money Services Business (MSB) Information Center, INTERNAL REVENUE SERV., https://www.irs.gov/businesses/small-businesses-self-employed/money-services-business-msb-information-center#:~:text=An%20MSB%20is%20generally%20any,in%20one%20or%20more%20transactions [https://perma.cc/9UUP-BA2W].

[95] FIN. CRIMES ENF'T NETWORK, *supra* note 57, at 2.

[96] *Id.* at 1–2.

[97] *See* FIN. CRIMES ENF'T NETWORK, *supra* note 57.

[98] James Gatto & Elsa S. Broeker, *Bitcoin and Beyond: Current and Future Regulation of Virtual Currencies*, 9 OHIO ST. ENTREPRENEURIAL BUS. L.J. 429, 436 (2015) (quoting FIN. CRIMES ENF'T NETWORK, FIN-2014-R001, APPLICATION OF FINCEN'S REGULATIONS TO VIRTUAL CURRENCY MINING OPERATIONS, (Jan. 30, 2014), https://www.fincen.gov/sites/default/files/shared/FIN-2014-R001.pdf).

[99] *Id.* at 2–3.

[100] *Id.* at 2.

the authority to redeem (to withdraw from circulation) such virtual currency."[101]

The important similarity here is that both the exchanger and the administrator act as an intermediary who facilitates the transfer of money between third parties, whereas the user just exchanges virtual currency directly with other users for his or her own use and is thus outside the BSA's jurisdiction.[102] As a result, only if a ransomware attacker routes payments through an intermediary, such as a centralized exchange or a third-party P2P exchanger, does the BSA apply to the ransomware attacker; but the BSA does not apply if money is sent to the attacker directly from the victim because the ransomware attacker is then just considered a user under the BSA.[103] Put simply, if the ransomware attacker just receives a cryptocurrency ransom and then uses that ransom to either directly purchase something or converts the ransom to real or other virtual currency, the BSA does not apply. However, once the attacker then converts the ransom into another currency or otherwise begins to launder the cryptocurrency, applying the BSA becomes difficult, even if financial intermediaries are used later in the money-laundering process.

Next, the following portions of FinCEN's 2019 guidance are most applicable to ransomware attackers who use cryptocurrency for ransom payments and illustrate the difficulty of applying the BSA to: (1) wallets, which is how users can receive and send cryptocurrency transfers and store their coins, and (2) decentralized cryptocurrency exchanges.[104]

The applicability of the BSA to wallets depends on four criteria: "(a) who owns the value; (b) where the value is stored; (c) whether the owners interact directly with the payment system where the CVC runs; and, (d) whether the person acting as the intermediary has total independent control over the value."[105] If a wallet is 'hosted,' this means that a third party uses a website or mobile application to store cryptocurrency for its user by holding onto the user's private key and facilitating and overseeing the user's transactions,[106] similar to services tied to having a bank account with a traditional bank. Providers of a hosted wallet are generally subject to BSA requirements if they are located within or do any substantial business in the U.S.[107] This means that if a ransomware attacker uses a hosted wallet to

[101] *Id.*

[102] *Id.* at 2–3. While the BSA's applicability was expanded to include a broader definition of "money transmitter" through the passage of the Patriot Act in 2001, ransomware attackers can still fall outside of BSA regulatability when they are not an individual "engag[ed] as a business in an informal money transfer" or part of a group of individuals "engag[ing] as a business in facilitating the transfer of money;" mere users remain untouchable by the BSA. Turner, *supra* note 5, at 1404. Resultingly, BSA requirements to register with the federal government, report suspicious activities, and develop an effective AML program only apply to MSBs. *See also* Money Services Business (MSB) Information Center, INTERNAL REVENUE SERV., https://www.irs.gov/businesses/small-businesses-self-employed/money-services-business-msb-information-center#:~:text=An%20MSB%20is%20generally%20any,in%20one%20or%20more%20transactions [https://perma.cc/KCR8-4TPD]; *Am I an MSB?*, FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/am-i-msb [https://perma.cc/85HS-E2RB].

[103] *See* FIN. CRIMES ENF'T NETWORK, *supra* note 57.

[104] FIN. CRIMES ENF'T NETWORK, *supra* note 72, at 15–24.

[105] *Id.* at 15.

[106] *How to Set up a Crypto Wallet*, COINBASE, https://www.coinbase.com/learn/tips-and-tutorials/how-to-set-up-a-crypto-wallet [https://perma.cc/8YSJ-FGZY] (explaining how to set up a crypto wallet).

[107] FIN. CRIMES ENF'T NETWORK, *supra* note 72, at 15–17; *Requirements*, *supra* note 48, at 9–10.

receive a ransomware payment and the government is able to trace that payment to that wallet, even if they were not able to identify the wallet's owner, hosted wallet providers could face BSA sanctions if they are located in or do any substantial business in the U.S. The due diligence that a hosted wallet provider must perform on its users depends on who the wallet owner is: applicable for the purposes of this Note, if the owner is a user, the provider must comply with KYC requirements to "verify[] and monitor[] both the user's identity and profile," consistent with their reporting requirements under the BSA.[108] To use a centralized exchange, a user must use that exchange's wallet in order to trade cryptocurrency funds through the exchange, so the BSA is readily applicable to exchanges conducted through a hosted wallet by placing BSA requirements both on the exchange operator by nature of its MSB status and due to its provision of a hosted wallet.[109]

On the other hand, an unhosted wallet does not require an intermediary to execute transactions on a user's behalf, which means that users do not share their private key and retain full control over their wallet to conduct transactions P2P, often with other users who are also using unhosted wallets.[110] In this case, the BSA is not directly applicable, because the owner of the wallet does not qualify as a money transmitter since the user's transaction "never involve[s] a regulated financial intermediary," nor indirectly applicable to users through the provider of their wallet.[111] Thus, while the BSA remains applicable to hosted wallets, the use of unhosted wallets for P2P transfers represents an outlier from BSA applicability.[112]

Decentralized exchanges ("DEXs"), also known as P2P exchanges or CVC trading platforms, function truly P2P, as opposed to centralized exchanges, which are actively involved intermediaries in trades between users on their platforms.[113] Users never share control over their wallet by sharing their private key with the exchange so that the exchange can conduct transactions on behalf of the users and host the their private wallet.[114] Instead, users transact directly with one another using "self-executing agreements written in code called smart contracts."[115] DEXs thus only serve as a forum to link buyers and sellers; while DEXs are overall used a lot less frequently than centralized exchanges, DEXs allow for greater anonymity and are thus popular for exchanging cryptocurrency obtained through illicit means.[116] If a DEX "only provides a forum where buyers and sellers of CVC post their bids and offers . . . , but the parties themselves settle any matched transactions through an outside venue (either through individual wallets or

[108] FIN. CRIMES ENF'T NETWORK, *supra* note 72, at 16.

[109] Dennis Chu, *Broker-Dealers for Virtual Currency: Regulating Cryptocurrency Wallets and Exchanges*, 118 COLUM. L. REV. 2323, 2326–27 (2018). Centralized exchanges act as intermediaries to conduct trades between users by hosting all the involved wallets, holding on to those wallets' private keys, and holding funds in escrow. The majority of cryptocurrency exchanges are centralized exchanges. *See* Reiff, *supra* note 27.

[110] FIN. CRIMES ENF'T NETWORK, *supra* note 72, at 15–17; *Requirements*, *supra* note 48, at 9–10.

[111] FIN. CRIMES ENF'T NETWORK, *supra* note 72, at 15–16; *Requirements*, *supra* note 48, at 10.

[112] *Requirements*, *supra* note 48, at 11.

[113] Reiff, *supra* note 27.

[114] *What Are Decentralized Exchanges, and How Do DEXs Work*, COINTELEGRAPH, https://cointelegraph.com/defi-101/what-are-decentralized-exchanges-and-how-do-dexs-work [https://perma.cc/B6QL-EBKE].

[115] *Id.*

[116] *Id.*

other wallets not hosted by the trading platform), the trading platform does not qualify as a money transmitter" subject to BSA regulation.[117] As a result, users are not subjected to KYC requirements and DEXs have no recordkeeping or reporting requirements under the BSA. In sum, if ransomware attackers use a DEX to find other users to conduct a P2P transfer with which to launder the attackers' ransomware payment, neither the users nor the decentralized exchange would fall within BSA jurisdiction since the decentralized exchange is not considered an MSB.[118]

Finally, additional difficulties can arise when ransomware attackers exchange virtual currency from ransoms through: (1) unregistered entities, entities that do not register with FinCEN as MSBs and thus do not report transactions, such as darknet marketplaces that are available over "anonymized overlay networks that require specific software . . . vetting, or configurations to access" and are predominately used to exchange illicit goods and services; (2) unregistered P2P exchangers who may misrepresent themselves or misstate the nature of their business; or (3) unregistered foreign-located MSBs who do not adhere to BSA AML requirements.[119] While all three of these entities are money transmitters subject to BSA regulation if they do any substantial business in the U.S., they highlight jurisdictional and extraterritorial problems tied to cryptocurrency because they can avoid BSA regulation by not registering with FinCEN.[120] These entities can accomplish this because they are either not traditional exchange intermediaries that would normally be subject to BSA regulation or they operate out of countries that do not cooperate with U.S. AML efforts.[121]

In sum, the BSA is not applicable to individuals if they are only exchanging currency P2P and ransomware attackers can safely make use of unhosted wallets and decentralized exchanges to receive their ransoms without falling under the BSA's jurisdiction.[122]

B. THE MONEY LAUNDERING CONTROL ACT OF 1986

While the MLCA focuses less on traditional financial institutions than the BSA does, the absence of a financial institution in P2P cryptocurrency transactions and the requirement that an individual's monetary transaction be

[117] FIN. CRIMES ENF'T NETWORK, *supra* note 72, at 23–24; Mika Nonaka, Jenny Konko & Cody Gaffney, *FinCEN Issues Guidance to Synthesize Regulatory Framework for Virtual Currency*, 20 J. INV. COMPLIANCE 54, 54–55 (2019).

[118] *Id.*

[119] FIN. CRIMES ENF'T NETWORK, FIN-2019-A003, ADVISORY ON ILLICIT ACTIVITY INVOLVING CONVERTIBLE VIRTUAL CURRENCY 3–6 (May 9, 2019), https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf. Russia was linked to the SolarWinds attack in 2020 and the U.S. and Russia continue to clash on cybersecurity policy. *See* Lubomir Tassev, *U.S. Sanctions Russian Crypto Broker SUEX for Laundering Millions in Illicit Funds*, BITCOIN.COM (Sept. 22, 2021), https://news.bitcoin.com/us-sanctions-russian-crypto-broker-suex-for-laundering-millions-in-illicit-funds/ [https://perma.cc/8MQC-BG3P] (explaining the U.S. sanctions for a Czech crypto exchange operated out of Russia); Joseph Marks, *The Cybersecurity 202: The Biden Administration Is Stepping Up the Fight Against Ransomware*, WASH. POST (July 14, 2021), https://www.washingtonpost.com/politics/2021/07/15/cybersecurity-202-biden-administration-is-stepping-up-fight-against-ransomware/ [https://perma.cc/45HW-R4SG] (describing the continued pressure by the Biden Administration on President Putin to "crack down on ransomware attacks from Russian territory").

[120] FIN. CRIMES ENF'T NETWORK, *supra* note 119, at 15–16; *Requirements*, *supra* note 48, at 9–10.

[121] *See supra* note 120.

[122] FIN. CRIMES ENF'T NETWORK, *supra* note 119, at 7–8.

linked to an expansive, but specific, list of SUA makes the MLCA difficult to apply to P2P cryptocurrency ransoms.[123]

First, to sustain a conviction under the MLCA, both sections 1956 and 1957 require the government to prove both underlying SUA, as set out in section 1956, and to tie the transaction—in this case, the cryptocurrency ransom transfer, and the underlying SUA—to an individual, the ransomware attacker.[124] The anonymous and hard-to-trace nature of P2P transactions can make "tying any particular person to a pseudonymous account" very challenging, especially if ransomware attackers scatter the funds "among many [crypto] addresses to hide the dirty money's source," [125] choose types of cryptocurrency that are more privacy focused, and use anonymization services such as Tor Browsers.[126] While the MLCA's list of underlying SUA is expansive, that expansiveness does not matter much if the government is unable to link an anonymous transaction on the public ledger to a specific individual or is unable to show that SUA is the source of the money. If the government was, however, able to trace the transaction to a specific individual and was able to show that the transaction was made in connection with a ransomware payment, it is likely the ransomware extortion could be classified as SUA under a definition like "racketeering activity." Racketeering activity is a broad term that involves "any act or threat involving . . . bribery, [or] extortion . . . ."[127] Exchanges are, once again like with the BSA, easier to apply the MLCA to, since most exchanges impose KYC requirements on users and exchanges must already comply with AML regulation such as the aforementioned BSA reporting and recordkeeping requirements. Such strictures make it easier to tie together SUA, a specific individual, and a cryptocurrency transaction because the government can follow a paper trail.[128]

Next, section 1957 is generally easier to apply than section 1956 because section 1957 does not include specific knowledge or intent requirements "that the launderer had the intent to promote SUA, evade taxation, or knowingly concealed laundering or avoided AML requirements,"[129] which can be, again, difficult to prove given the anonymous nature of cryptocurrency and thus in tracing transactions to specific individuals. Instead, under section 1957 the government must prove: (1) an individual knowingly engaged or attempted to engage in an exchange (2) a transaction exceeding ten thousand dollars, (3) involving property derived from SUA, and (4) involving a financial institution.[130] Although an in-depth analysis of further AML legislation is beyond the scope of this Note, it is worth mentioning that in recognition of the difficulty of proving "actual knowledge of illegal structuring activities," Congress passed the Money Laundering

---

[123] *See* Anna Driggers, *Money Laundering*, 48 AM. CRIM. L. REV. 929, 930–32 (2011).

[124] 18 U.S.C. §§ 1956–57; *see also* 18 U.S.C. § 1961(1) (offenses listed also constitute SUA).

[125] Bryans, *supra* note 65, at 460; INST. FOR SEC. & TECH. & RANSOMWARE TASK FORCE, *supra* note 1, at 14; *see also* Bagby et al., *supra* note 48.

[126] *See* Irwin & Dawson, *supra* note 16, at 122; THE TOR PROJECT, *supra* note 53.

[127] 18 U.S.C. § 1961(1) (offenses listed here also constitute SUA); *see also* Albrecht et al., *supra* note 22, at 213; Turner, *supra* note 5.

[128] Bryans, *supra* note 65, at 460; s*ee also* 31 U.S.C. § 5311; FIN. CRIMES ENF'T NETWORK, *supra* note 119, at 7–8 (describing BSA applicability to cryptocurrency exchanges).

[129] Bryans, *supra* note 65, at 460 n.166.

[130] *Id.* at 460.

Suppression Act of 1994 ("MLSA"), which eliminated the "willfulness requirement relating to civil penalties for structuring transactions."[131] However, while the MLSA omits the MLCA's willfulness, or intent, requirement for laundering or avoiding AML requirements in regards to civil penalties, the aforementioned difficulties remain in connecting a SUA with a specific individual and a specific cryptocurrency payment.

However, the application of section 1957 faces the same shortcoming as the BSA's emphasis on financial institutions because section 1957 requires a transaction exceeding ten thousand dollars to involve a financial institution.[132] The definition of "money transfer" set out in section 1957(f)(1) requires a payment to be "by, through, or to a financial institution."[133] Financial institutions are defined under section 1956, and by extension under 31 U.S.C. § 5312(2).[134] This definition is not readily applicable to individual users of cryptocurrency, as was already laid out earlier in this Note under the 2013 FinCEN guidance for the BSA concerning the difference between users, administrators, and exchangers and other businesses engaged in the exchange of virtual currency.[135] The definition includes a long list of entities, including insured and private banks, currency exchanges, licensed senders of money, and "any person who engages as a business in an informal money transfer system"; but, again, the definition does not apply to single-transaction individuals who are not acting as transmitters but rather are just receiving and using the funds.[136] Thus, like with the BSA, the MLCA remains difficult to apply to individual ransomware attackers who receive cryptocurrency transfers P2P without any exchange or other financial-institution entity acting as an intermediary to the ransomware attackers' transaction.

In sum, issues in applying the MLCA to ransomware attackers stem from the difficulty in identifying the source of cryptocurrency transfers and the specific actor involved, which is difficult due to the anonymous decentralized nature of cryptocurrency and because of the MLCA's focus on financial institutions, not on individuals engaging in P2P transactions.

V. THE BIDEN ADMINISTRATION'S RESPONSE TO THE RANSOMWARE THREAT

When President Biden took office in 2021, he did so on the heels of the December 2020 SolarWinds attack, which was perpetrated by Russian-linked hackers. [137] The SolarWinds attack affected numerous U.S. government entities, including the State Department, the Department of

[131] Straub, *supra* note 74, at 525.
[132] 18 U.S.C. § 1957(f)(1).
[133] *Id.*
[134] 18 U.S.C. § 1956; 31 U.S.C. § 5312(2).
[135] *Id.* (the closest would be (j) "a currency exchange, or a business engaged in the exchange of currency, funds, or value that substitutes for currency or fund" but this is not applicable to individuals); *see also* FIN. CRIMES ENF'T NETWORK, *supra* note 57; FIN. CRIMES ENF'T NETWORK, *supra* note 119.
[136] 31 U.S.C. § 5312(2).
[137] *See e.g.*, Zachary Cohen, Civian Salama & Brian Fung, *US Officials Scramble to Deal with Suspected Russian Hack of Government Agencies*, CNN: POLS. (Dec. 14, 2020), https://www.cnn.com/2020/12/14/politics/us-agencies-hack-solar-wind-russia/index.html [https://perma.cc/3882-PAF6].

Homeland Security, and the Treasury Department, and major private companies, including Microsoft, Intel, and Cisco.[138] Consequently, and unsurprisingly, President Biden pledged to make improving the U.S.'s cybersecurity one of his administration's top priorities.[139] Throughout the beginning of Biden's presidency, cyberattackers have continued to mount attacks against U.S. targets, including the high-profile Colonial Pipeline and JBS USA ransomware attacks in 2021.[140] Because a comprehensive examination of all of the Biden administration's cybersecurity-related actions taken to this point is beyond the scope of this Note, this section will briefly discuss the Biden administration's cybersecurity policies and initiatives as they specifically relate to countering ransomware.[141]

First, this section examines the Ransomware Task Force ("RTF"), which the Biden administration formed in the middle of 2021, in addition to the State Department offering "rewards as high as ten million dollars for helping identify [ransomware] perpetrators."[142] The RTF was made up of private and public sector experts for the purpose of developing a "comprehensive framework for tackling" ransomware.[143] The RTF made forty-eight recommendations, with their main priorities being: (1) the coordination of international efforts to prioritize ransomware attacks and eliminate safe havens; (2) a coordinated whole-of-government response that involves establishing new cybersecurity positions and bodies; (3) establishing funds to support the victims of attacks; (4) establishing an international framework "to help organizations prepare for, and respond to, ransomware attacks;" and (5) the increased regulation of "crypto exchanges, crypto kiosks, and over-the-counter IOTC trading 'desks' to comply with existing laws."[144]

Overall, this whole-of-government approach that seeks to increase private and public sector cooperation, improve international cooperation, and improve cyber hygiene demonstrates a dedication to a multi-pronged approach. However, one of the RTF's big focuses, the disruption of the ransomware business model, contains the same pitfall as the BSA and MLCA

---

[138] *Id.*; *see also* Isabella Jibilian & Katie Canales, *The US Is Readying Sanctions Against Russia Over the SolarWinds Cyber Attack. Here's a Simple Explanation of How the Massive Hack Happened and Why It's Such a Big Deal*, BUS. INSIDER (Apr. 15, 2021), https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12 [https://perma.cc/8PMZ-35YR].

[139] Solender, *supra* note 9; White House, *supra* note 9; Exec. Order No. 14,028, *supra* note 9.

[140] William Turton & Kartikay Mehrotra, *Hackers Breached Colonial Pipeline Using Compromised Password*, BLOOMBERG (June 4, 2021), https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password [https://perma.cc/9539-RAUK]; Lily Hay Newman, *Ransomware Hits a Food Supply Giant—and Underscores a Dire Threat*, WIRED (June 1, 2021), https://www.wired.com/story/jbs-ransomware-attack-underscores-dire-threat/ [https://perma.cc/NT35-RAPM].

[141] *See* Press Release, White House, Fact Sheet: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government networks (May 12, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/ [https://perma.cc/HQV4-YSMH]; Jill McKeon, *Biden Administration Announces National Cybersecurity Initiatives*, HEALTHITSECURITY (Sept. 7, 2021), https://healthitsecurity.com/news/biden-administration-announces-national-cybersecurity-initiatives [https://perma.cc/J2CE-8EEC] (discussing a cybersecurity summit hosting leaders in private industry).

[142] Eric Geller, *White House Announces Ransomware Task Force—and Hacking Back Is One Option*, POLITICO (July 14, 2021), https://www.politico.com/news/2021/07/14/white-house-ransomware-task-force-499723 [https://perma.cc/7GG3-36BE].

[143] INST. FOR SEC. & TECH. & RANSOMWARE TASK FORCE, *supra* note 1, at 3.

[144] *Id.* at 6.

because it focuses on intermediary entities and on continuing to try and apply the, as previously explained, ill-suited existing AML laws to ransomware attackers. Recommendations by the RTF related to this pitfall include improving compliance with existing laws for cryptoexchanges and other cryptocurrency intermediaries, incentivizing voluntary information sharing between crypto intermediaries and law enforcement, and streamlining the seizure process of cryptocurrency from cryptoexchanges.[145] Ultimately, these measures focus on intermediaries, such as cryptocurrency exchanges, but ignore P2P transmitters who operate outside existing AML laws.

It is worth briefly noting that the RTF framework contemplates expanding the Racketeer Influenced and Corrupt Organizations Act's ("RICO") applicability to disrupt the "ransomware criminal enterprise."[146] While RICO may be better suited for targeting individual parties than the institution-focused BSA and MLCA, its application would still face similar hurdles of first having to identify specific individuals and then link them to specific activities tied to anonymous cryptocurrency transactions in order to apply RICO. A RICO case requires individuals to engage in a "pattern of racketeering activity, requiring at least two acts of racketeering activity within a ten-year window," which presents additional problems given the difficulty in connecting individuals to payments on a blockchain ledger. [147] Moreover, just like the BSA and MLCA, RICO was drafted over thirty years ago, likely without any intention of being readily applicable to the then non-existent medium of cryptocurrency.[148] New legislation could better fully address the technological and extraterritorial issues that crimes like ransomware, which are facilitated through cryptocurrency, pose, rather than adapting old laws.

Next, other efforts to combat ransomware by the Biden Administration include, among many other things, the establishment of the National Cyber Investigative Joint Task Force (NCIJTF) to align ransomware enforcement initiatives, the launch of CISA's "Reduce the Risk of Ransomware Campaign to encourage public- and private-sector organizations to implement best practices, tools, and resources" to combat ransomware,[149] the ongoing regulatory battle between the Securities Exchange Commission (SEC) and the largest U.S.-based cryptocurrency exchange Coinbase,[150] the Treasury Department's first-ever sanction of a foreign cryptoexchange, SUEX,[151] the increased dedication of government personnel to combatting ransomware attacks, initiatives to bolster the security of critical infrastructure facilities, creating the National Cryptocurrency Enforcement Team ("NCET") to

[145] *Id.* at 28–34.

[146] *Id.* at 34; *see also* Racketeer Influenced and Corrupt Organization Act, 18 U.S.C. § 1692.

[147] Chelsea Pieroni, *La Crypto Nostra: How Organized Crime Thrives in the Era of Cryptocurrency*, 20 N.C. J.L. & TECH. 111, 138–39 (2018).

[148] *See* 18 U.S.C. § 1692.

[149] INSTIT. FOR SEC. & TECH. & RANSOMWARE TASK FORCE, *supra* note 1, at 18; *see also Stop Ransomware*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/stopransomware [https://perma.cc/7XL7-VJEW].

[150] Todd Ehret, *SEC Spat with Coinbase Previews Complex Legal Battle over Crypto*, REUTERS (Sept. 28, 2021), https://www.reuters.com/legal/transactional/sec-spat-with-coinbase-previews-complex-legal-battle-over-crypto-2021-09-28/ [https://perma.cc/YT32-56VT].

[151] While SUEX is hosted in the Czech Republic, it is operated out of Russia. Tassev, *supra* note 107; *see also Treasury Takes Robust Actions to Counter Ransomware*, U.S. DEP'T TREASURY (Sept. 21, 2021), https://home.treasury.gov/news/press-releases/jy0364 [https://perma.cc/5ES9-SQ9C].

investigate and prosecute "criminal misuses of cryptocurrency, particularly crimes committed by virtual currency exchanges,"[152] creating the Ransomware and Digital Extortion Task Force to respond to and prevent ransomware incidents,[153] and international cooperation efforts such as joint statements by NATO and the Financial Action Task Force (FATF) and pushing for the expansion of the Budapest Convention.[154] However, these initiatives, like the RTF's recommendations, still continue to focus on exchange intermediaries by expanding reporting and AML requirements for exchanges, increasing the government's ability to seize funds that pass through cryptocurrency exchanges, and increasing regulatory actions against exchanges, instead of addressing gaps in applying existing AML laws like the BSA and the MLCA to criminal actors who are not intermediaries, just users of cryptocurrency, and who trade cryptocurrency directly P2P with their victims.

Finally, however, a meaningful change to the BSA is pending at the time of this Note.[155] The government wants to expand the BSA to cover payments made through a bank or MSB if one of the wallets is an unhosted wallet or if one of the wallets is an "otherwise covered wallet . . . hosted in a jurisdiction identified by FinCEN."[156] Unhosted wallets and wallets in foreign jurisdictions that are not cooperating with U.S. AML enforcement efforts were two gaps in the BSA's applicability that this Note identified earlier. This amendment would be a big step towards addressing problematic gaps in existing AML legislation because it recognizes the important role that unhosted wallets play in laundering cryptocurrency and extraterritorial difficulties when wallets are in uncooperative foreign countries. In fact, in this proposed change, FinCEN specifically recognized that there are "illicit finance risks involving CVC [that] are enhanced by the capacity of users to engage with the CVC through unhosted wallets or wallets hosted by a foreign financial institution not subject to effective anti-money-laundering regulation (an "otherwise covered wallet").[157] However, this proposed change still fails to properly target the P2P transactions that this Note has identified as being the most problematic because the proposed rule still requires either a bank or MSB to be involved in the transaction by hosting the unhosted wallet or the "otherwise covered wallet."[158] Thus, true P2P transactions that do not use a centralized exchange or bank remain outside the BSA's jurisdiction.

---

[152] *Deputy Attorney General Lisa O. Monaco Announces National Cryptocurrency Enforcement Team*, U.S. DEP'T JUST. (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team [https://perma.cc/2JHW-UJVA].

[153] *U.S. Government Launches First One-Stop Ransomware Resource at StopRansomware.gov*, U.S. DEP'T JUST. (July 15, 2021), https://www.justice.gov/opa/pr/us-government-launches-first-one-stop-ransomware-resource-stopransomwaregov [https://perma.cc/4AMJ-W7J5].

[154] White House, *supra* note 9. For FinCEN guidance on the difficult application of the BSA to virtual currency, see FIN. CRIMES ENF'T NETWORK, *supra* note 119.

[155] Current as of early November 2021.

[156] *Requirements*, *supra* note 48, at 8–25.

[157] *Id.* at 6.

[158] *Id.*

VI. POLICY RECOMMENDATIONS

The Biden Administration's proposed course of action faces a similar pitfall as the BSA and MLCA by focusing on the regulation of traditional exchanges and, similarly, cryptocurrency equivalents.[159] However, there are limitations to government action if exchanges are not located in the United States, such as in a country unwilling to cooperate with U.S. AML enforcement efforts.[160] To address these limitations, the Biden Administration must continue prioritizing private-public sector collaboration, pursuing increased international cooperation given that ransomware attacks are a global issue and enforcement raises extraterritorial issues, and emphasizing a whole-of-government approach to combatting ransomware.[161] While this Note is not suggesting that the increased regulation of cryptoexchanges is without merit, if attackers opt for P2P transactions, they are outside existing AML regulation like the BSA and MLCA, so the focus of new legislation should be to close that gap.[162]

Thus, in addition to steps the Biden Administration has already taken, this Note proposes prioritizing: (1) new cryptocurrency-specific legislation that can provide a better regulatory framework to address P2P ransomware cryptocurrency payments; (2) improving forensic accounting and other technology solutions for tracing money; and (3) improving cyber hygiene.

First, aside from the current proposal to expand the BSA to cover certain unhosted wallets, the Biden Administration has yet to address gaps in existing AML legislation's applicability to cryptocurrency, and thus one priority going forward should be to draft new AML legislation. [163] Merely extending the BSA and MLCA to cryptocurrency will result in a patchwork approach given the fact that many key aspects of the two pieces of AML legislation, such as the KYC and recordkeeping requirements of the BSA or the SUA requirement underlying the MLCA, remain difficult or impossible to apply due to the anonymous nature of cryptocurrency. Technology changes quickly, and the BSA and MLCA were drafted more than thirty years ago when the technology enabling ransomware attacks and cryptocurrency was likely unforeseeable for Congress. New legislation should focus specifically on cryptocurrency and its underlying technology instead of trying to adapt existing AML laws.

Next, the government should continue to focus on improving its ability to trace payments through a type of forensic accounting of the blockchain

---

[159] INST. FOR SEC. & TECH. & RANSOMWARE TASK FORCE, *supra* note 1, at 28–34.

[160] For example, the SEC's regulatory battle with Coinbase is possible because the cryptoexchange is based in the U.S.. Ehret, *supra* note 150. Similarly, the SUEX exchange which is based in the Czech Republic (but is operated out of Russia) was willing to cooperate with the U.S. Alan Rappeport, Andrew E. Kramer & David E. Sanger, *The Biden Administration Is Combating Ransomware with a Crackdown on Cryptocurrency Payments*, N.Y. TIMES (Sept. 21, 2021), https://www.nytimes.com/2021/09/21/us/politics/treasury-department-combating-ransomware-cryptocurrency.html [https://perma.cc/W86B-BV9N]; *cf.* Russia's resistance to prosecuting ransomware attacks originating in their country. Marks, *supra* note 119.

[161] *See* White House, *supra* note 141; McKeon, *supra* note 141; Jenna McLaughlin, *White House Brings Together 30 Nations to Combat Ransomware*, NPR (Oct. 13, 2021), https://www.npr.org/2021/10/13/1045248842/white-house-brings-together-30-nations-to-combat-ransomware [https://perma.cc/LRU6-TZLC].

[162] INST. FOR SEC. & TECH. & RANSOMWARE TASK FORCE, *supra* note 1, at 29–30.

[163] *Requirements*, *supra* note 48, at 8–25.

given that tracing the proceeds of crime has traditionally been the most effective way to track down criminal actors.[164] There is, however, a lack of a uniform approach by law-enforcement agencies to tracing cryptocurrency payments.[165]

Following the digital money trail has already proven successful, evidenced by the Biden Administration's new Ransomware and Digital Extortion Task Force. The new task force managed to recover two million three hundred thousand dollars of the cryptocurrency ransom paid to ransomware attackers in the Colonial Pipeline attack.[166] While it is not entirely clear how the task force was able to obtain the key linked to the Bitcoin account to which the ransom was delivered, the FBI stated that it will utilize the techniques that proved successful in future cases as well.[167] Since payments are so rarely recovered, learning how to use cryptocurrency-specific features like public key addresses and the public ledger to follow payments is a good step towards continuing to remove the financial motivations underlying ransomware attacks. In addition, there are other blockchain-enabled technology solutions that the government can pursue to assist AML efforts, in cooperation with exchanges and the crypto community. For example, the government can build in "proof of identity features," to help identify holders of wallets; the government can use machine learning technology to scan the public ledger for and report suspicious activity, like traditional banks already do, by focusing on matching transaction *patterns* with suspected addresses instead of focusing on matching or following specific *transactions*.[168]

Finally, perhaps the easiest and most effective fix to prevent ransomware attacks, is to ensure that overall cyber hygiene across the public and private sectors in the U.S. improves. Cyber hygiene is a term that "refers to the steps that users of computers and other devices can take to improve their online security and maintain system health" when they are accessing the internet, which then, in the aggregate, improves the security of entire businesses and institutions.[169] The Biden Administration has already made this a priority, but preventing attacks in the first place would mitigate the complicated identification, recovery, and prosecution process.[170] As the current chief of the Department of Homeland Security's Cyber Crime Unit said: "If you look at the most major ransomware attacks that have occurred, basic cyber hygiene could have prevented the vast majority of them . . . . [including]

---

[164] Irwin & Dawson, *supra* note 16.

[165] *Id.*

[166] *See* Vanessa Romo, *How a New Team of Feds Hacked the Hackers and Got Colonial Pipeline's Ransom Back*, NPR (June 8, 2021), https://www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked-the-hackers-and-got-colonial-pipelines-bitcoin-bac [https://perma.cc/FUW2-46WN]; U.S. DEP'T JUST., *supra* note 137.

[167] *See* Romo, *supra* note 166.

[168] *See* Campbell-Verduyn, *supra* note 91, at 292, 297; Ammar Oad, Abdul Razaque, Askar Tolemyssov, Munif Alotaibi, Bandar Alotaibi & Chenglin Zhao, *Blockchain-Enabled Transaction Scanning Method for Money Laundering Detection*, 10 ELECS. 1766, 1766–67 (2021); Yan Wu, Fang Tao, Jiayan Gu, John Panneerselvam, Rongbo Zhu & Mohammad Nasir Shahzad, *A Bitcoin Transaction Network Analytic Method for Future Blockchain Forensic Investigation,* 8 IEEE TRANSACTIONS ON NETWORK SCI. & ENG'G 1230, 1231–33 (2021).

[169] *Good Cyber Hygiene Habits to Help You Stay Safe Online*, KASPERSKY, https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits [https://perma.cc/LQ27-JEEY].

[170] INST. FOR SEC. & TECH. & RANSOMWARE TASK FORCE, *supra* note 1, at 39–40.

heavy network segmentation, network security monitoring, zero trust models," which requires users to continually verify their credentials while they use a system,[171] and "multi-factor authentication . . . ."[172]

Additional basic cyber hygiene best practices include keeping an organization's software patched and up to date, backing up systems regularly, storing backups separately from the network with separate login information, creating an incident response and business continuity plan, limiting or controlling folder access, training employees to better spot phishing attacks, using good browsing practices, avoiding suspicious emails and downloads, and creating strong passwords for their computers and accounts.[173] While good cyber hygiene habits may be more of a ransomware avoidance or mitigation technique than real prevention, these straightforward steps that individuals can take could make a huge difference in protecting everything from small businesses to large-scale organizations and federal agencies.[174] The Biden administration has already demonstrated its commitment to raising awareness about ransomware, as is evidenced by, among many other initiatives, the RTF Taskforce's proposed course of action and CISA's Reduce the Risk of Ransomware Campaign; going forward, these education and awareness efforts need to continue throughout the private and public sectors.[175]

VII. CONCLUSION

This Note has demonstrated that the BSA and MLCA's focus on intermediaries such as traditional banks and other financial institutions and now, by modern extension, on cryptocurrency exchanges, makes them difficult to effectively apply to P2P transactions such as those underlying cryptocurrency ransom payments to ransomware attackers. While the BSA is applicable to transfers conducted through centralized cryptocurrency exchanges and other similar intermediaries, individual users who do not act as money transmitters fall outside the BSA's scope. Similarly, the MLCA is difficult to apply to cryptocurrency payments to ransomware attackers

---

[171] Aaron Boyd, *Biden Administration Releases Draft Zero-Trust Guidance*, NEXTGOV (Sept. 7, 2021), https://www.nextgov.com/cybersecurity/2021/09/biden-administration-releases-draft-zero-trust-guidance/185166/ [https://perma.cc/767Y-ZD6K].

[172] Grace Dille, *Feds Preach Cyber Hygiene to Prevent Most Ransomware Attacks*, MERITALK (Aug. 29, 2021), https://www.meritalk.com/articles/feds-preach-cyber-hygiene-to-prevent-most-ransomware-attacks/ [https://perma.cc/84JT-PS38] (quoting Matthew Swenson, chief of the DHS's Cyber Crime Unit at Homeland Security Investigations (HSI)).

[173] *See* Adhirath Kapoor, Ankur Gupta, Rajesh Gupta, Sudeep Tanwar, Gulshan Sharma & Innocent E. Davidson, *Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions*, 14 SUSTAINABILITY 1, 13–14 (2021); Ben Rossen, *Ransomware Prevention: An Update for Businesses*, FED. TRADE COMM'N: BUS. BLOG (Dec. 11, 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/12/ransomware-prevention-update-businesses [https://perma.cc/A3CQ-MRWP]; CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, *supra* note 149 (coordinated government response to stopping and reporting ransomware-run by CISA); *Stay Safe from Cybersecurity Threats*, U.S. SMALL BUS. ADMIN., https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats [https://perma.cc/EAW5-G65N].

[174] Kapoor et al., *supra* note 173.

[175] *See* INST. FOR SEC. & TECH. & RANSOMWARE TASK FORCE, *supra* note 1; CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, *supra* note 149; *CISA, FBI, and NSA Release Blackmatter Ransomware Advisory to Help Organizations Reduce Risk of Attack*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Oct. 18, 2021), https://www.cisa.gov/news/2021/10/18/cisa-fbi-and-nsa-release-blackmatter-ransomware-advisory-help-organizations-reduce [https://perma.cc/C7UW-5LLN].

because the anonymous and decentralized nature of cryptocurrency makes it difficult to prove a transaction's underlying SUA and to tie a transaction and SUA to a specific individual.[176] Further, for that reason, proving section 1956's intent and knowledge requirements is difficult, and section 1957 is likely not applicable to ransomware payments because an individual or group does not constitute a "financial institution," as is required to be involved in the transaction by section 1957; again, the MLCA is better applied to a financial institution or other similar intermediary like a cryptocurrency exchange.[177]

As previously discussed in this Note, the whole purpose of passing the BSA and MLCA was to create a paper trail that would allow the government to investigate and follow the money used to facilitate a plethora of crimes and to ultimately allow the government to charge the associated criminal actors with money-related offenses, such as for money laundering or terrorist financing and proliferation.[178] However, given the aforementioned difficulty in tying actors to ransomware payments made using cryptocurrency, in situations when ransomware attackers are convicted, they often noticeably do not face any money-related charges because the government is unable to meet the requirements under either act to properly tie the actors to the cryptocurrency ransoms.[179] This lack of money-related charges against convicted attackers, given that ransomware attacks are financially motivated crimes and given the immense financial costs associated with these attacks, demonstrates the incredible inapplicability of existing anti-*money*-

[176] 18 U.S.C. § 1956–57; Bryans, *supra* note 65, at 460.

[177] *See* 18 U.S.C. § 1957(f)(1); Bryans, *supra* note 65, at 460 n.166.

[178] Federal Deposit Insurance Act Amendments, Pub. L. No. 91-508, 84 St. 1114 (stating that the records "have a high degree of usefulness in criminal, tax, and regulatory investigations and proceedings"); Money Laundering Control Act of 1986, Pub. L. No. 99-570, 100 Stat. 3207-18 (amending 18 U.S.C. ch. 95 to make money laundering a federal offense and creating a broad range of SUAs linked to money that allow individuals to be charged under the Act); *see also* KLEIN, *supra* note 58; 31 U.S.C. § 5311; Turner, *supra* note 5, at 1405; Straub *supra* note 74; 18 U.S.C. §§ 1956–57; Review of Bank Secrecy Act Regulations and Guidance, 86 Fed. Reg. 71201, 71202–03 (proposed Dec. 15, 2021) (accepting public comments until Feb. 14, 2022), https://www.govinfo.gov/content/pkg/FR-2021-12-15/pdf/2021-27081.pdf.

[179] When ransomware attackers are charged, they are primarily charged in connection with their actions related to the actual infiltration of the computer networks and damage to the computers themselves, but not in relation to the ransoms. Money-related charges are noticeably absent, despite the incredible sums of money that are involved in the attacks. *See e.g.*, *Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses*, U.S. DEP'T JUST. (Nov. 28, 2018), https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public [https://perma.cc/5XGJ-EHXW]. Two hackers were both charged with (1) conspiracy to commit fraud and related activity in connection with computers, (2) conspiracy to commit wire fraud, (3) intentional damage to a protected computer, and (4) transmitting a demand in relation to damaging a protected computer. There were, however, no money-related charges, for the $6 million (additional losses from loss cost victims $30 million) SamSam Ransomware attacks on a variety of schools, hospitals, companies, and government agencies. *3 North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe*, U.S. DEP'T JUST. (Feb. 17, 2021), https://www.justice.gov/usao-cdca/pr/3-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyber-attacks-and#:~:text=LOS%20ANGELES%20%E2%80%93%20A%20federal%20indictment,from%20financial%20institutions%20and%20companies%2C [https://perma.cc/9TZP-VU32]. Three hackers were charged with, among other charges, (1) conspiracy to intentionally access computers without authorization and obtain information from protected computers; (2) conspiracy to knowingly and with intent defraud access protected computers without authorization; (3) conspiracy to knowingly cause the transmission of programs, information, codes, and commands, and as a result of such conduct intentionally cause damage without authorization to protected computers; (4) conspiracy to commit wire fraud; and (5) conspiracy to commit bank fraud. The hackers participated in a $1.3 billion scheme also referred to as the "Sony Pictures hack."

laundering laws to combatting this serious problem and the great necessity of legislative action.

In sum, ransomware remains a pressing global threat. If the United States wants to be in a better position to prevent attacks and prosecute attackers, it needs to continue its whole-of-government efforts, private-sector collaboration, and international efforts. The Biden administration should also consider drafting new cryptocurrency-specific legislation, improving its ability to trace cryptocurrency transfer payments, exploring other technology-based solutions to trace transfers, and improving overall cyber hygiene in the United States.