THIRD WAY

MEMO *Published May 3, 2021 • 13 minute read*

Digital Currencies' Role in Facilitating Ransomware Attacks: A Brief Explainer

Kristine Johnson
Consultant, Patomak Global Partners

Michael Garcia
Senior Policy Advisor
@garrrcya

Takeaways

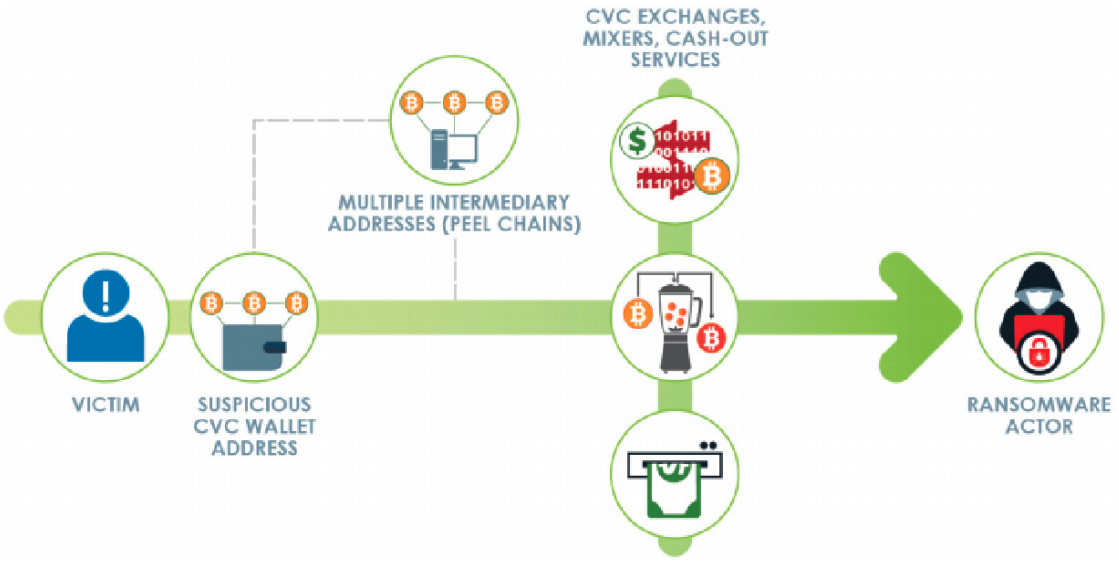
This paper details how Bitcoin—the most popular digital currency—is used to facilitate ransomware attacks and how criminals try—and sometimes fail—to cover their tracks. Understanding how criminals use digital currencies for ransomware attacks can lead policymakers to solutions in thwarting and enforcing cybercrimes.

How does ransomware work?

Ransomware is a favorite tool of cybercriminals to extort money from victims as successful techniques have been perfected over the years. Ransomware is malicious software (malware) that locks or encrypts a victim's computer system or files and demands a ransom payment to unlock the system or retrieve the files. The predominant ransomware tactic involves prompting victims to download a malicious PDF or word document from an email or visit a malicious site, at which point the malware is downloaded onto their computer. The malware encrypts everything on the computer, and a pop-up instructs the user to follow certain steps to access their files. [1]

Following the infiltration, victims are often instructed to pay the ransom demand by transmitting funds via wire transfer, automated clearinghouse, or credit card payment to a digital currency exchange where they can obtain a type and amount of digital currency to send to the attacker's designated digital currency address. The perpetrator then launders the money using various means including traditional money laundering techniques, which may be combined with digital currency-specific techniques and venues as discussed below. The graphic below depicts a typical movement of funds in a ransomware attack using digital currency.

Movement of Digital Currency in Ransomware Attacks



Source: Financial Crimes Enforcement Network, US Treasury. "Advisory on Ransomware and the Use of the Financial." 1 Oct. 2020 https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf. Accessed 06 Apr. 2021.

The harmful impact of ransomware cannot be understated. Homeland Secretary Alejandro Mayorkas referred to it as an "epidemic that is spreading through cyberspace." [2] Global estimates

show that ransomware attacks have increased by 148% since February 2020. [3] Ransom amounts and total costs of attacks also have grown, with U.S. hospitals, schools, and city governments' services often being the focal points of disruption. [4] In fact, in 2020 ransomware was the type of digital currency-based crime that saw the most dramatic increase from the previous year. [5] With the recent rise in ransomware attacks, digital currencies have faced increased scrutiny for their role in facilitating ransom payments. [6]

Why is digital currency, like Bitcoin, used to facilitate ransomware payments?

Digital currencies, especially Bitcoin, have become the preferred payment method for conducting these operations due to their assumed anonymity characteristics. When the Bitcoin blockchain first originated in 2009, it represented a revolutionary invention that solved the "double spending" problem of sending payments virtually. Bitcoin enabled people to send "money" and complete transactions electronically in a peer-to-peer manner, without the use of a third-party intermediary. [7] Bitcoin and other digital currencies are largely anonymous since each participant that sends a transaction is only associated with a public address consisting of a random string of numbers and letters, so it is not known who is conducting a transaction at the time it occurs. Yet, every transaction is recorded and broadcasted on an immutable, distributed public ledger (a blockchain)—in Bitcoin's case, the Bitcoin blockchain—and the trail remains available indefinitely. In this sense, digital currencies like Bitcoin are pseudonymous, but not private. [8]

Differentiating blockchain and Bitcoin: Since Bitcoin was the first application of blockchain technology, people have at times conflated the two. While Bitcoin transactions are stored and transferred on a public, distributed ledger, blockchain is the technology that underpins and maintains such a transaction ledger. Digital currencies are a widespread use case for blockchain technology, but the technology itself may be adapted for other use cases, including supply chain management and integrity. However, it is important to distinguish that blockchains adapted for business use cases are different from the Bitcoin blockchain, notably in that they may not always be decentralized in terms of governance, and often require permissions, as opposed to Bitcoin's permissionless blockchain. Nonetheless, blockchain is the technology that underpins the Bitcoin ledger, but itself is independent and should not be confused with Bitcoin. [9]

But as with any technological advancement, bad actors have also taken notice of the benefits of blockchain and digital currencies due to their perceived anonymous nature. While other digital currencies, including privacy coins like Monero, are becoming more popular for illicit activity,

criminals still predominately rely on Bitcoin. [10] Bitcoin, however, is not as anonymous as many people think. In fact, forensic software services have been used on numerous occasions to assist law enforcement in investigating ransomware attacks and identifying bitcoin users, as discussed below.

Why is it difficult to identify the criminal who receives a Bitcoin ransom?

Cybercriminals rely on traditional money laundering tactics to cover their tracks and evade law enforcement. When dealing with digital currencies like Bitcoin, criminals may use mixing services, also known as tumbling services (mixers or tumblers for short), to break the connection between the Bitcoin sender's address and the receiver's address or "wallet." Once a user sends Bitcoin to a mixer, the mixer mixes it with Bitcoins from different sources, or even newly mined ones, and returns Bitcoin (with different addresses and transaction histories) to a different wallet.

While mixers may be attractive for laundering money, they also have downsides, including: (1) they do not always work well for large sums of money, (2) they require high amounts of trust in the mixing service since the user is handing over Bitcoin, and (3) the new Bitcoins received might be tainted from previous illicit activity, increasing the chances that the digital currency would eventually be flagged. [11]

Whether mixers are used or not, laundering also involves breaking up large amounts of currency into smaller transactions, also known as "smurfing." Smurfing could involve converting between different currencies and transferring funds across many accounts and digital currency exchanges, some of which may be located in jurisdictions with weak anti-money laundering and know-your-customer regimes. [12] In fact, Chainalysis, a company that provides investigative tools to track digital currencies (among other things), found that in the fourth quarter of 2020, over 50 percent of funds leaving ransomware wallets were sent to mainstream exchanges, while less than half went to high-risk exchanges with weak or non-existent compliance protocols. A very small percentage went to other illicit addresses or mixing services. [13]

Anti-money laundering protocols and digital currencies: In the US, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) is responsible for administering the legislative framework designed to prevent money laundering and the financing of terrorism, commonly known as the Bank Secrecy Act. Under the Bank Secrecy Act and FinCEN's regulations, entities engaging in "money transmission" must register as a money services business with FinCEN and maintain an anti-money laundering program. At a minimum, an anti-money laundering program must include policies, procedures, and controls designed to ensure compliance, which include: verifying customer identification (also known as know-your-customer regimes), identifying and reporting suspicious activity, creating and retaining records, and responding to law enforcement requests. FinCEN has issued multiple guidances

detailing how entities engaged in convertible virtual currency activity are subject to the Bank Secrecy Act. In particular, money transmission involves the acceptance and transmission of value that substitutes for currency, by any means. As such, entities that receive one form of value from one person (e.g. digital currency) and transmit either the same or a different form of value to another person, by any means, are considered a money transmitter and subject to the Bank Secrecy Act. In 2019, FinCEN consolidated all of its digital currency-related guidance dating back to 2011 and clarified that those who provide anonymizing services (e.g., mixers and tumblers) are considered money transmitters and obligated to register with FinCEN. [14] As a general rule of thumb, some jurisdictions around the world have applied variations of these standards to entities like digital currency exchanges, to varying degrees, while some jurisdictions remain lax in terms of regulations and/or enforcement.

How do criminals convert digital currency into fiat currency?

Digital currency exchanges exist all over the world and allow for the conversion of one type of digital currency to another or digital currency into fiat- government central-bank issued- currency, and vice versa. [15] Perpetrators seeking to convert laundered Bitcoin into fiat currency may do so by sending the Bitcoin to an exchange with weak anti-money laundering protocols and withdrawing fiat currency from that exchange. Before sending the currency to an exchange where it can be converted into fiat, perpetrators may swap Bitcoin into another digital currency (e.g., Monero) and then back to Bitcoin. Even though exchanges with rigorous anti-money laundering and know-your-customer protocols, such as US exchanges, increase the difficulty and risk for criminals, mainstream exchanges are still the number one destination of funds leaving ransomware wallets. Finally, as Bitcoin and other digital currencies are becoming more widely accepted, perpetrators may choose to spend the digital currencies directly.

How can digital currency forensics and analytics help to identify cybercriminals?

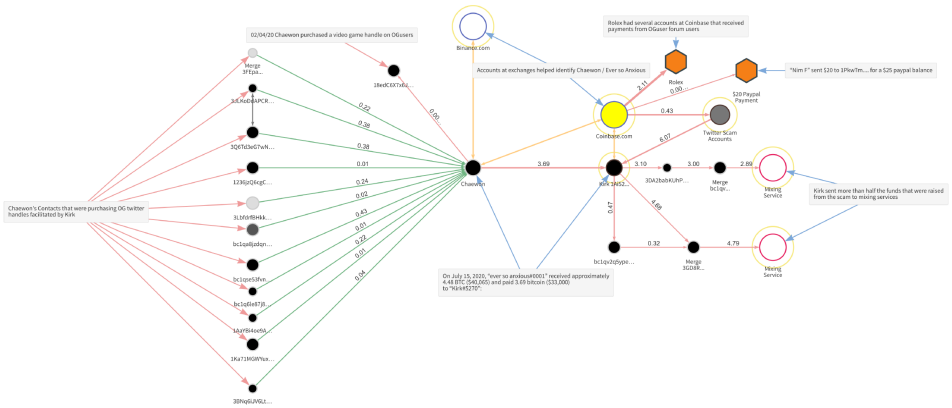
Due to the pseudonymous, but not private, nature of Bitcoin and other digital currencies, it is possible to “follow the money” to see where laundered currencies travel to and from, and in some cases tie the activity to actors holding the wallets. Law enforcement, exchanges, and other institutions use forensic software services that specialize in analyzing transaction data to help monitor and investigate potential illicit activity. When cybercriminals transfer Bitcoins between various accounts, for example, this may indicate a link between the accounts and suggest that the addresses are all linked to the same person. Using advanced analysis of transaction data,

pseudonyms may be "clustered" together, and transaction graph analysis can be conducted to draw certain conclusions. [16]

In addition to forensic tools that employ enhanced clustering techniques and convert blockchain data into clear visualizations, companies also offer transaction monitoring tools that allow users to drill down to the ultimate source and destination of funds. Using these enhanced tools, exchanges and other companies have halted fiat or digital currencies from being taken off the exchange once suspicious activity has been detected.

One recent example demonstrates how these services may be used for investigations. In the July 15, 2020 Twitter hack, where multiple high-profile Twitter accounts were compromised and used to promote Bitcoin scams, three individuals were ultimately arrested and charged with conspiracy to commit money laundering, among other charges. Chainalysis reported that law enforcement used their software to analyze a series of transfers from a Bitcoin wallet address to an address controlled by one of the defendants. [17] By analyzing several other transactions whose timing, amounts, and other details made clear that they were payments for stolen Twitter accounts, another defendant's address was identified. Chainalysis software showed all of Defendant #2's wallet transaction history, including fiat on and off-ramps (exchanges). [18] Law enforcement was then able to reach out to two exchanges, retrieve know-your-customer information, and identify the defendant's true identity. [19]

Chainalysis Twitter Hack Blockchain Analysis



Source: Chainalysis In Action: How Law Enforcement Used Blockchain Analysis to Follow Funds and Identify the Twitter Hackers." Chainalysis Insights, 30 Jul. 2020. https://blog.chainalysis.com/reports/chainalysis-doj-twitter-hack-2020. Accessed 06 Apr. 2021.

However, this forensic analysis has its limitations. In this example, the ability to track down the defendant's true identity was contingent upon the fact that he had accounts with exchanges that maintained adequate know-your-customer measures. Indeed, if the perpetrators would have been more sophisticated in concealing their identities and used exchanges with less robust compliance, analysis by law enforcement would have been much more difficult. While forensic analysis can provide many details, it still only represents part of the picture. [20] As an additional tool, some

exchanges track users' Internet Protocol addresses, which can be particularly useful where know-your-customer information may be incomplete or inaccurate.

What has Congress done to stop ransomware and what could it do?

In the 116 th Congress, in response to continued cyber incidents across the country, multiple bills were introduced and passed that could potentially assist entities in dealing with cyber attacks, including ransomware. Yet, due to the distributed and global nature of blockchain and digital currencies, efforts aimed at banning the use of digital currency to pay ransomware would be highly ineffective and continue to drive activity away from the United States, into unregulated jurisdictions. Further, any attempt at banning digital currency use should not be viewed as a panacea to the ransomware epidemic. For instance, if the victim pays the ransom through traditional money transfers, criminals can still employ common money laundering techniques that continue to be effective in evading law enforcement detection. Third Way recently participated on the Institute for Security + Technology's Ransomware Task Force to develop recommendations on how the government, private sector, and international community can combat ransomware and help victims. Several of those recommendations touch on the use of digital currencies to facilitate ransoms and warrant review by policymakers. [21]

While not aimed at the digital currency challenge directly, Congress has taken action to help victims prepare for and respond to ransomware incidents. For example, the DHS Cyber Hunt and Incident Response Teams Act was signed into law (P.L. 116-94), which creates teams to provide technical assistance to entities to develop mitigation strategies and provide assistance in the event of an attack, such as a ransomware event. [22] Congress also created the Joint Cyber Planning Office in DHS to convene federal, local, and private partners to develop plans that would disrupt the cyberinfrastructure that criminals use to carry out their malicious cyber activities, such as ransomware attacks. [23] Lastly, DHS now has "cybersecurity state coordinators" in each state to, among other things, "support training, exercises, and planning for continuity of operations to expedite recovery from cybersecurity incidents, including ransomware." [24]

In addition to these new authorities, Congress could increase the resources available to state and local law enforcement agencies to improve their digital forensic capabilities to identify the criminals behind these incidents, while supporting US and international efforts to arrest criminals overseas. As mentioned, law enforcement agencies can and do use digital forensic software to track illicit, digital currency payments. Previously introduced bills, such as the Technology in Criminal Justice Act of 2019 (H.R.5227), and reintroduced bills, such as the Violence Against Women Reauthorization Act of 2021 (H.R.1620), would provide grants to local law enforcement agencies to improve their digital forensic capabilities. [25] Congress could also require federal agencies to prioritize digital forensic capabilities in existing grant programs and/or use the appropriations process to provide additional funds for those needs. For example, Congress could increase funds to the Paul Coverdell

Forensic Science Improvement Grants Program—a grant program that supports forensic labs and personnel—and require the Attorney General to prioritize competitive grants that would support digital forensic labs and tools. [26] The Biden Administration appears willing to tap into existing grants to combat ransomware, with DHS Secretary Mayorkas requiring recipients of a large DHS grant program to spend 7.5% of their funds on cybersecurity, up from 5%. [27] Lastly, Congress could prioritize passing the "Cyber Diplomacy Act of 2019" (H.R.739) to elevate a State Department cyber office to a chain-of-command that allows it to have cross-cutting authority. Congress could also focus on evaluating and improving bilateral and multilateral cyber capacity-building efforts around the globe.

Conclusion

The ransomware epidemic continues to affect organizations and individuals at an alarming rate, with tremendous amounts in value being lost either directly or indirectly through the attacks. Understanding how digital currencies operate and the ability to identify criminals who misuse these currencies to facilitate their crimes will enable Congress to develop informed legislation to disrupt the illicit profit gained from ransomware. The Biden Administration and 117 th Congress have a tall task in front of them, but policymakers can begin taking steps that address this cybersecurity threat.

TOPICS

CYBERSECURITY 84 | TECHNOLOGY & SECURITY 8

ENDNOTES

1. A "drive-by" malware attack that hosts malicious code on a legitimate website but prompts the user in the same manner, may also be employed. Financial Crimes Enforcement Network, US Treasury. "Advisory on Ransomware and the Use of the Financial." 1 Oct. 2020 https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf. Accessed 06 Apr. 2021.

2. Miller, Maggie. "DHS Secretary Mayorkas announces new initiative to fight 'epidemic' of cyberattacks." *The Hill*, 25 Feb. 2021. https://thehill.com/policy/cybersecurity/540549-dhs-secretary-mayorkas-announces-new-initiative-to-fight-epidemic-of. Accessed 06 Apr. 2021.

3. Garcia, Michael and Shilo, Pat. "Taking Action on Cyber Enforcement: Assessing US Legislative Progress in the 116th Congress." *Third Way*, Feb 2021. https://www.thirdway.org/memo/taking-action-on-cyber-enforcement-assessing-us-legislative-progress-in-the-116th-congress. Accessed 06 Apr. 2021.

4. Popper, Nathaniel. "Ransomware Attacks Grow, Crippling Cities and Businesses." *New York* Times, 09 Feb. 2020. *available at* https://www.nytimes.com/2020/02/09/technology/ransomware-attacks.html. Accessed 06 Apr. 2021.

5. While representing the largest percentage increase from the previous year, ransomware still makes up a miniscule amount of digital currency-related criminal activity. "The 2021 Crypto Crime Report: Everything you need to know about ransomware, darknet matters, and more." Chainalysis. 16 Feb. 2021, p. 7. https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf. Accessed 06 Apr. 2021.

6. Sobrado, Boaz. "Bitcoin Is Aiding the Ransomware Industry." *Coindesk*, 19 Jan 2021. https://www.coindesk.com/bitcoin-is-aiding-the-ransomware-industry. Accessed 06 Apr. 2021.

7. Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." *Bitcoin.org*, Oct 2008. https://bitcoin.org/bitcoin.pdf. Accessed 06 Apr. 2021.

8. Ludwin, Adam. "How Anonymous is Bitcoin?" *Coin Center*, 22 Jan. 2015. https://www.coincenter.org/education/crypto-regulation-faq/how-anonymous-is-bitcoin/. Accessed 06 Apr. 2021.

9. Lucas, Matt. "The difference between Bitcoin and blockchain for business." 09 May 2017. https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-bitcoin-and-blockchain-for-business/. Accessed 06 Apr. 2021.

10. Silfversten, Erik et.al. "Exploring the Use of Zcash Cryptocurrency for Illicit or Criminal Purposes." *Rand Corporation*, 2020. https://www.rand.org/pubs/research_reports/RR4418.html. Accessed 06 Apr. 2021. Custers, Bart et.al. "Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies." *European Journal of Crime Criminal Law and Criminal Justice*, 28 (2), p. 136, Jul. 2020. https://www.researchgate.net/publication/343009039_Laundering_the_Profits_of_Ransomware_Money_Laundering_Methods_for_Vouchers_and_Cryptocurrencies. Accessed 06 Apr. 2021.

11. Ludwin, Adam. "How Anonymous is Bitcoin?" *Coin Center*, 22 Jan. 2015. https://www.coincenter.org/education/crypto-regulation-faq/how-anonymous-is-bitcoin/. Accessed 06 Apr. 2021.

12. Financial Crimes Enforcement Network, US Treasury. "Advisory on Ransomware and the Use of the Financial." 1 Oct. 2020 https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf. Accessed 06 Apr. 2021.

13. "The 2021 Crypto Crime Report: Everything you need to know about ransomware, darknet matters, and more." Chainalysis. 16 Feb. 2021, p. 28. https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf. Accessed 06 Apr. 2021.

14. Financial Crimes Enforcement Network, US Treasury. "Advisory on Ransomware and the Use of the Financial." 1 Oct. 2020 https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf. Accessed 06 Apr. 2021.

15. While digital currencies may be transacted through Peer-to-Peer (P2P) platforms—marketplaces that allows individuals to trade cryptocurrencies directly with each other without a third-party mediator—centralized digital currency exchanges are a popular way for users to access digital currencies because they are easier to access.

16. Ludwin, Adam. "How Anonymous is Bitcoin?" *Coin Center*, 22 Jan. 2015. https://www.coincenter.org/education/crypto-regulation-faq/how-anonymous-is-bitcoin/. Accessed 06 Apr. 2021.

17. "Chainalysis In Action: How Law Enforcement Used Blockchain Analysis to Follow Funds and Identify the Twitter Hackers." *Chainalysis Insights*, 30 Jul. 2020. https://blog.chainalysis.com/reports/chainalysis-doj-twitter-hack-2020. Accessed 06 Apr. 2021.

18. "Chainalysis In Action: How Law Enforcement Used Blockchain Analysis to Follow Funds and Identify the Twitter Hackers." *Chainalysis Insights*, 30 Jul. 2020. https://blog.chainalysis.com/reports/chainalysis-doj-twitter-hack-2020. Accessed 06 Apr. 2021.

19. Ludwin, Adam. "How Anonymous is Bitcoin?" *Coin Center*, 22 Jan. 2015. https://www.coincenter.org/education/crypto-regulation-faq/how-anonymous-is-bitcoin/. Accessed 06 Apr. 2021.

20. Minsky, Carly. "The Crypto Detectives." *Sifted*, 14 Feb. 2019. https://sifted.eu/articles/crypto-forensics-analytics/. Accessed 06 Apr. 2021.

21. "Combating Ransomware: A Comprehensive Framework for Action: Key Recommendations for the Ransomware Task Force." *Institute for Security Technology*, 29 Apr. 2021. https://securityandtechnology.org/ransomwaretaskforce/report/. Accessed 21 Apr. 2021.

22. United States, Congress, United States Code. P.L. 116-94. 20 Dec. 2019. https://www.congress.gov/116/plaws/publ94/PLAW-116publ94.pdf.

23. United States, Congress, House of Representatives. United States Code. P.L. 116-283. Title XVII, section 1715, US Congress, 1 Jan. 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr. Accessed 12 Mar. 2021.

24. United States, Congress, House of Representatives. United States Code. P.L. 116-283. US Congress, 1 Jan. 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr. Accessed 12 Mar. 2021.

25. United States, Congress, House of Representatives. "H.R.5227 - Technology in Criminal Justice Act of 2019." 21 Nov. 2019. https://www.congress.gov/bill/116th-congress/house-bill/5227/text. Accessed 06 Apr. 2021. United States Congress, House of Representatives. "H.R.1620 - Violence Against Women Act Reauthorization Act of 2021." 08 Mar. 2021. https://www.congress.gov/bill/117th-congress/house-bill/1620/actions. Accessed 06 Apr. 2021.

26. Garcia, Michael. "Follow the Money: Few Federal Grants Are Used to Fight Cybercrime." 16 Feb. 2021. https://www.thirdway.org/report/follow-the-money-few-federal-grants-are-used-to-fight-cybercrime. Accessed 06 Apr. 2021.

27. United States, Department of Homeland Security. "DHS Announces Steps to Advance President's Commitment to Elevate Cybersecurity." 22 Feb. 2021. https://www.dhs.gov/news/2021/02/22/dhs-announces-steps-advance-president-s-commitment-elevate-cybersecurity. Accessed 06 Apr. 2021.