CHAMBER OF DIGITAL COMMERCE

STATEMENT FOR THE RECORD OF THE
CHAMBER OF DIGITAL COMMERCE
HEARING BEFORE THE SENATE JUDICIARY COMMITTEE
JULY 27, 2021

"America Under Cyber Siege: Preventing and Responding to Ransomware Attacks"

The Chamber of Digital Commerce is the world's leading trade association representing the digital asset and blockchain industry. The Chamber's mission is to promote the acceptance and use of digital assets and blockchain-based technologies. Through education, advocacy, and working closely with policymakers, regulatory agencies, and industry, our goal is to develop an environment that fosters innovation, jobs, and investment. Members of the Chamber provide blockchain analytics and other services to industry and government that have been used to trace the flow of cryptocurrency payments, including those made as a result of ransomware attacks.

The Chamber of Digital Commerce co-founded the Blockchain Alliance, which works closely with key law enforcement agencies around the globe. The Blockchain Alliance is a public-private forum that enables the blockchain community and law enforcement to work together to help combat criminal activity. It is comprised of 20+ state, federal and international law enforcement agencies. This forum serves as a resource for law enforcement and regulatory agencies by providing educational resources, technical assistance, and periodic informational sessions regarding the use of blockchain-based technologies.

Ransomware is not a cryptocurrency and blockchain problem

Ransomware may be defined as a type of malicious software designed to block access to a computer system until a sum of money is paid. Ransomware attacks on information infrastructure date to at least 1989, when attendees to an international AIDS conference were targeted with infected computer disks.[1] Ransomware payments have taken many forms over the past few decades, including through wire transfers, prepaid debit cards, iTunes gift cards, cash payments, and other forms.[2]

In other words, ransomware criminality pre-dates the development of blockchain and cryptocurrencies by many decades. While it is true that ransomware attacks began to increase in frequency starting in 2011, the fundamentals of ransomware criminality were well established before the advent of cryptocurrency. The vulnerability of information infrastructure, combined with a monetary incentive to lock and unlock networks in return for payment, mean that as workspaces

[1] https://www.varonis.com/blog/a-brief-history-of-ransomware/
[2] https://www.aier.org/article/fighting-ransomware-doesnt-require-banning-cryptocurrency/

become increasingly digitized, bad actors will increasingly be incentivized to engage in ransomware attacks – particularly as the cybersecurity defenses of America's small businesses remain dangerously weak.

Indeed, ransomware attacks against small businesses with poor cybersecurity defenses can cost less than $100 to perpetrate.[3] Until carrying out ransomware attacks becomes prohibitively expensive thanks to the proliferation of strong cybersecurity defenses across American small businesses, criminals will be incentivized to continue to carry out these attacks. Payment activities related to or involving cryptocurrencies do not alter that harsh reality that the recent surge in ransomware attacks was primarily enabled by a rapid nationwide embrace of digital workplaces that was not accompanied by sufficient improvements in cybersecurity defenses. To stop ransomware attacks in an increasingly online world, resources are best spent developing programs and initiatives aimed at bolstering the cybersecurity of American small businesses, which are disproportionately victimized by ransomware attacks.[4]

Ransomware criminals using cryptocurrency can be traced on the blockchain

In fact, the attributes of cryptocurrencies actually enable regulators and law enforcement to trace ransomware transactions back to perpetrators. As lawmakers, regulators, and prosecutors gain a better understanding of cryptocurrency, we believe they will understand how it can be leveraged to combat the ongoing surge in ransomware attacks. This is because cryptocurrencies are created on an open blockchain, and as such, there is a public record of each transaction that cannot be altered. This auditability function helps explain why authorities have been able to track down and arrest the criminals behind some of the largest ransomware attacks,[5] and/or recover amounts paid by victims.

Indeed, the recent Colonial Pipeline ransomware attack ultimately resulted in almost all related criminal bitcoin transfers being traced and recovered. In fact, DOJ announced in a press release on June 7, 2021, that "by reviewing the Bitcoin public ledger, law enforcement was able to track multiple transfers of bitcoin and identify that approximately 63.7 bitcoins, representing the proceeds of the victim's ransom payment, had been transferred to a specific address."[6] The FBI obtained the "private key" for the address and recovered the payments. Had the DarkSide hackers in the Colonial Pipeline case instead demanded payment in cash or through another payments channel, recovering the funds could have been much more difficult.

[3] https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report
[4] https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report
[5] https://apnews.com/article/europe-malware-netherlands-coronavirus-pandemic-7de5f74120a968bd0a5bee3c57899fed
[6] https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

As this example shows, cryptocurrency enables law enforcement to utilize technological tools and methods to track criminals that are unavailable for financial crimes that cannot be traced on a blockchain. In order to halt the recent increase in ransomware attacks, law enforcement can embrace new technologies to aggressively track and prosecute criminals.

Blockchain and other distributed ledger technology (DLT) can reduce financial crime

At the same time, it is critical for policymakers to embrace digital assets as well as blockchain and other forms of DLT, which if integrated into the traditional financial system, could lead to a large overall reduction of financial crime. The United Nations estimates that the amount of money laundered globally in one year is 2 to 5% of global GDP, or $800 billion to $2 trillion.[7] Conversely, one study estimates that total ransomware paid via cryptocurrencies in 2020 equaled $350 million[8] – in other words, an amount less than one-tenth of a percent of the value of total money laundered annually.

Most money laundering and financial crime takes place via traditional financial intermediaries. For the same reasons that the blockchains of cryptocurrencies like bitcoin enable authorities to track and trace financial criminals such as ransomware attack perpetrators, the adaptation of DLT and blockchain solutions could help traditional financial institutions combat the massive global problem of financial crime. DLT is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions, and certain applications of blockchain technology—a form of DLT—have characteristics that can help governments and businesses combat financial crime, including the following:

Distributed: Blockchain creates a shared system of record among business network members – eliminating the need to reconcile disparate ledgers.

- Transactions via blockchain networks can be constructed and held throughout the network and ultimately accessible via secured channels for audit and tracking purposes. This can be very helpful with respect to both client and transaction-related data, and the protection and presentment of Know Your Customer (identity) data between corresponding financial intermediaries

Immutability: Consensus is required from all members and all validated transactions are permanently recorded. Even a system administrator cannot delete or alter a transaction.

[7] https://www.unodc.org/unodc/en/money-laundering/overview.html
[8] https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf

- Transactions can be recorded for auditability and transaction monitoring. Transaction history and specifics cannot be altered once inputted, which means the associated identities of senders and receivers of a transaction can be verified as associated with the transaction itself. The immutability of the ledger can therefore benefit ongoing client and transaction monitoring real time – increasing process efficiencies and reducing costs associated with compliance activities.

Permissioned: Each member of the network must have access privileges and information is shared only on a need-to-know basis between network nodes.

- Information regarding the transaction origin (sender) and recipient can be permissioned between nodes for easy and secure access without disclosure to third parties without permission, and be leveraged for verification/validation purposes, managing against fraud, and assisting network participants in a common financial ecosystem.

How the Chamber of Digital Commerce Can Help

The Chamber applauds recent actions taken by the Administration and Congress related to combating ransomware, such as proposals to increase resources to prosecute these criminals,[9] and a willingness to leverage technologies that can trace cryptocurrency transactions.[10] Ransomware is a crime, and we stand ready to work closely with government officials to continue to thwart attacks, raise awareness of cybersecurity initiatives, and help on the back end to trace the cryptocurrencies paid in each attack. We have attached to this document the most up to date report on the state of ransomware.

In conclusion, the Chamber of Digital Commerce hopes to be a valuable resource to the Judiciary Committee and law enforcement as we develop policy solutions to stop ransomware attacks. History demonstrates that criminals will pursue potentially lucrative ransomware attacks when and where they detect security weakness. Recent events, however, also demonstrate that criminals who demand payment in cryptocurrencies open the door to novel investigative and enforcement strategies that permit recovery of ransom funds. By embracing and expanding policy initiatives aimed at improving Main Street's cyber defenses while also increasing capabilities to aggressively track and prosecute cyber-criminals through analyzing cryptocurrency blockchains, we can put an end to ransomware attacks. We are also hopeful that an embrace of blockchain technology will lead to a reduction of illicit financial flows through traditional financial channels as well.

[9] https://www.justice.gov/jmd/page/file/1398826/download
[10] https://www.bloomberg.com/news/articles/2021-07-15/u-s-plans-to-counter-ransomware-attacks-through-crypto-tracing

Thank you for considering our views. We would be interested in meeting with you to provide a demo that illustrates the cryptocurrency traceability and auditability referred to in this letter.