BANK POLICY INSTITUTE

August 25, 2021

Ransomware Issue Summary

Ransomware poses a prolific and grave threat to the U.S. economy, as demonstrated by the 2021 Colonial Pipeline incident, which showed the staggering impacts ransomware attacks can have on both businesses and households. In 2020, adjusted losses from ransomware reached $29.1 million, according to the FBI, up from $8.9 million in 2019. However, since victims rarely report ransomware payments to their financial institution or law enforcement, some estimates indicate that total losses may be closer to $350 million per year.

WHAT IS RANSOMWARE?

Ransomware is a type of malicious software (or malware) that prevents a business or individual from accessing computer files, systems or networks until a ransom is paid to restore normal operations. Ransomware is often delivered through phishing emails that appear to come from legitimate customers or contacts; these emails will contain links or attachments that, when clicked on, may take control of the user's computer and potentially infect other files on the network.

These incidents can severely disrupt business processes and block access to critical data. Criminals use these disruptions and the threat of public disclosure to their advantage to demand payment from their victims, typically in the form of cryptocurrency. Cryptocurrency offers the advantage of anonymity while also making it easy for criminals to verify — using publicly available blockchain data — that a payment has been completed. Victims who decide to pay the demand are usually given instructions on how to restore normal operations; those that don't risk being permanently shut out of their systems or having their data exposed to the public.

While U.S.-based cryptocurrency firms are subject to anti-money laundering (AML) requirements, many ransomware operators are located outside U.S. jurisdiction and solicit payments through foreign firms whose host country does not enforce the same rigorous AML expectations.

WHAT ARE BANKS DOING TO RESPOND TO AND PREVENT RANSOMWARE?

Banks are largely reliant on customers reporting ransomware incidents. When banks are made aware of an incident, they can work with customers, government agencies, law enforcement and national security agencies to identify potentially suspicious activity and report such activity by filing suspicious activity reports (SARs) as appropriate. If the victim determines that circumstances necessitate paying the ransom, some victims will work with third-party intermediaries to assist with remediation and recovery efforts and to negotiate and facilitate payments.

WHAT CAN BE DONE TO ADDRESS THE PROBLEM OF RANSOMWARE?

- **Improve Transparency and Reporting into Ransomware Events:**
    1. The U.S. government should launch a national campaign to encourage ransomware victims to report incidents and information about the criminals *before* paying the demand. A single portal should be created to provide real-time data to law enforcement, including the ransom amount, instructions for how it should be paid and any other patterns or information that could help identify and stop the culprit.
    2. Private industry and government could collaborate to develop real-time, at-scale blockchain analytics capabilities (or, if feasible, leverage existing capabilities) to better understand suspicious activity and enhance transparency into the flow of crypto funds.

► **Encourage Other Countries to Establish Additional Requirements Related to Crypto Transactions and Ransomware Payments:**

3. Concerns around overseas cryptocurrency operators could be addressed by scaling AML requirements through a Financial Action Task Force (FATF) publication on ransomware.

4. Adopt foreign policy postures that encourage other countries to adopt AML regulations for crypto transactions and promote cooperation between law enforcement agencies in different countries.

► **Heighten Regulatory Standards for Crypto Participants:**

5. Increase enforcement of AML regulatory standards for all crypto participants that are subject to crypto regulation but may not currently be complying, and consider whether additional crypto participants should be included in the regulatory framework (e.g., intermediaries who provide ransom-related services and claim they are not required to register as a money service business with FinCEN under its “integral exemption”). Make AML program requirements consistent for all crypto participants who engage in the same activity with the same risk characteristics, regardless of each participant’s status as a bank, MSB or other type of financial institution.

6. Move forward with FinCEN’s December 2020 proposed rule that would require banks and money service businesses that maintain cryptocurrency wallets to conduct additional reporting and recordkeeping. In particular, it requires additional customer verification on crypto transactions greater than $10,000 that involve a counterparty using an unhosted wallet or otherwise covered wallet (e.g., wallet held at a financial institution not subject to BSA/AML regulation and/or located in a foreign jurisdiction identified by FinCEN).

7. Crypto participants should implement a solution to comply with the “Travel Rule” for crypto transactions. The Travel Rule requires financial institutions, including nonbank financial institutions (NBFIs), engaged in transmittal of funds (fiat or crypto), to transmit transactions and customer details to the next financial institution in the chain of payment in order to aid law enforcement agencies by maintaining an information trail of transaction originators and beneficiaries.

8. Financial institutions and NBFIs that exchange virtual currencies for U.S. dollars or other fiat currencies should continue to follow FinCEN’s October 2020 Advisory (FIN-2020-A006) that clearly, reasonably and effectively assists in the detection and reporting of ransomware payments.

► **Impose Financial Sanctions:**

9. Impose sanctions against crypto exchanges/asset service providers, owners and controllers that help facilitate obfuscation of crypto activity (using, for example, an executive order similar to E.O. 13757 and E.O. 13694). Update sanctions authorities as necessary to reflect unique national risks posed by widespread ransomware attacks.

10. Issue sanctions/advisories on issuers and asset service providers that create or support privacy coins designed to be untraceable on the blockchain and known to facilitate ransomware payments.

For additional information about ransomware, please click here.