ICBA
One Mission. Community Banks.®

A Guide to Ransomware Reporting

For Community Banks

866-843-4222
icba.org

1100 New York Avenue NW
Suite 500 East
Washington, DC 20005

518 Lincoln Road
P.O. Box 267
Sauk Centre, MN 56378

Ransomware

Ransomware has quickly become one of the most prevalent threats to businesses and consumers across the globe. The U.S. Financial Crimes Enforcement Network ("FinCEN") reports that in the first half of 2021 there were more than 600 suspicious activity reports ("SARs") filed for ransomware events totaling $590 million, and this only represents the events that were reported to FinCEN. In 2020, there was a total of $416 million of ransomware SARs filed for the entire year.[1]

Not only is ransomware becoming more prevalent, but cyber criminals are looking for ways to disguise their payments and evade law enforcement. This guide will examine three recent government advisories that look at the role that community banks play in preventing ransomware payments, red flags that may tip off criminal activity, and potential penalties community banks may face for facilitating ransomware payments.

CISA - Responding to Ransomware

The United States Cybersecurity and Infrastructure Security Agency ("CISA") released a stop ransomware guide outlining proper ransomware preparedness and responses. To assist community banks in their own preparedness and response, this guide aims to summarize the key points. Community banks are highly encouraged to read the entire document for more detailed information.

What is ransomware?

Ransomware is a type of malware threat actors use to infect computers and encrypt computer files until a ransom is paid. After the initial infection, ransomware will attempt to spread to connected systems, including shared storage drives and other accessible computers.

How does ransomware work?

Ransomware identifies the drives on an infected system and begins to encrypt the files within each drive. Once the ransomware has completed file encryption, it creates and displays a file or files containing instructions on how the victim can pay the ransom. If the victim pays the ransom, the threat actor may provide a cryptographic key that the victim can use to unlock the files, making them accessible.

How is ransomware delivered?

Ransomware is commonly delivered through phishing emails or via "drive-by downloads." Phishing emails often appear as though they have been sent from a legitimate organization or someone known to the victim and entice the user to click on a malicious link or open a malicious attachment. A "drive-by download" is a program that is automatically downloaded from the internet without the user's consent or often without their knowledge.

[1] https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf

What can you do to protect your data and networks?

Backup your computer and systems. Perform frequent backups of your system and other important files and verify your backups regularly. If possible, scan your backup data with an antivirus program to check that it is free of malware.

Store your backups separately. Best practice is to store your backups on a separate device that cannot be accessed from a network.

Train your organization. Organizations should ensure that they provide cybersecurity awareness training to their personnel. To improve workforce awareness, organizations can test their personnel with phishing assessments that simulate real-world phishing emails.

What can you do to prevent ransomware infections?

Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites.

Be careful when clicking directly on links in emails, even if the sender appears to be someone you know.

Open email attachments with caution. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

Keep staff informed about recent cybersecurity threats and up to date on ransomware techniques.

Use and maintain preventative software programs. Install antivirus software, firewalls, and email filters to reduce malicious network traffic. Regularly patch and update systems and software. Conduct internal vulnerability and external penetration scans. Utilize multifactor authentication and encryption to protect internal user accounts and systems. Conduct regular training and tests of your incident response plans. (See more tips in the CISA ransomware guide and the CISA stop ransomware web pages.)

FinCEN Ransomware Advisory

In November 2021, FinCEN released and updated advisory on *Ransomware and the Uses of the Financial System to Facilitate Ransom Payments*.[2] This advisory provided updates in response to the increase in ransomware attacks against critical infrastructure in the U.S.

In addition to outlining recent ransomware activities, the advisory reminds financial institutions ("FIs") of their reporting obligations for suspicious activity regarding ransomware. A Suspicious Activity Report ("SAR") should be

[2] https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf

filed if a FI determines that an incident of ransomware was conducted by, at, or through the FI and "involves aggregates of $5,000 or more in funds or other assets and involves funds derived from illegal activity, or attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of financial institutions to facilitate criminal activity."[3]

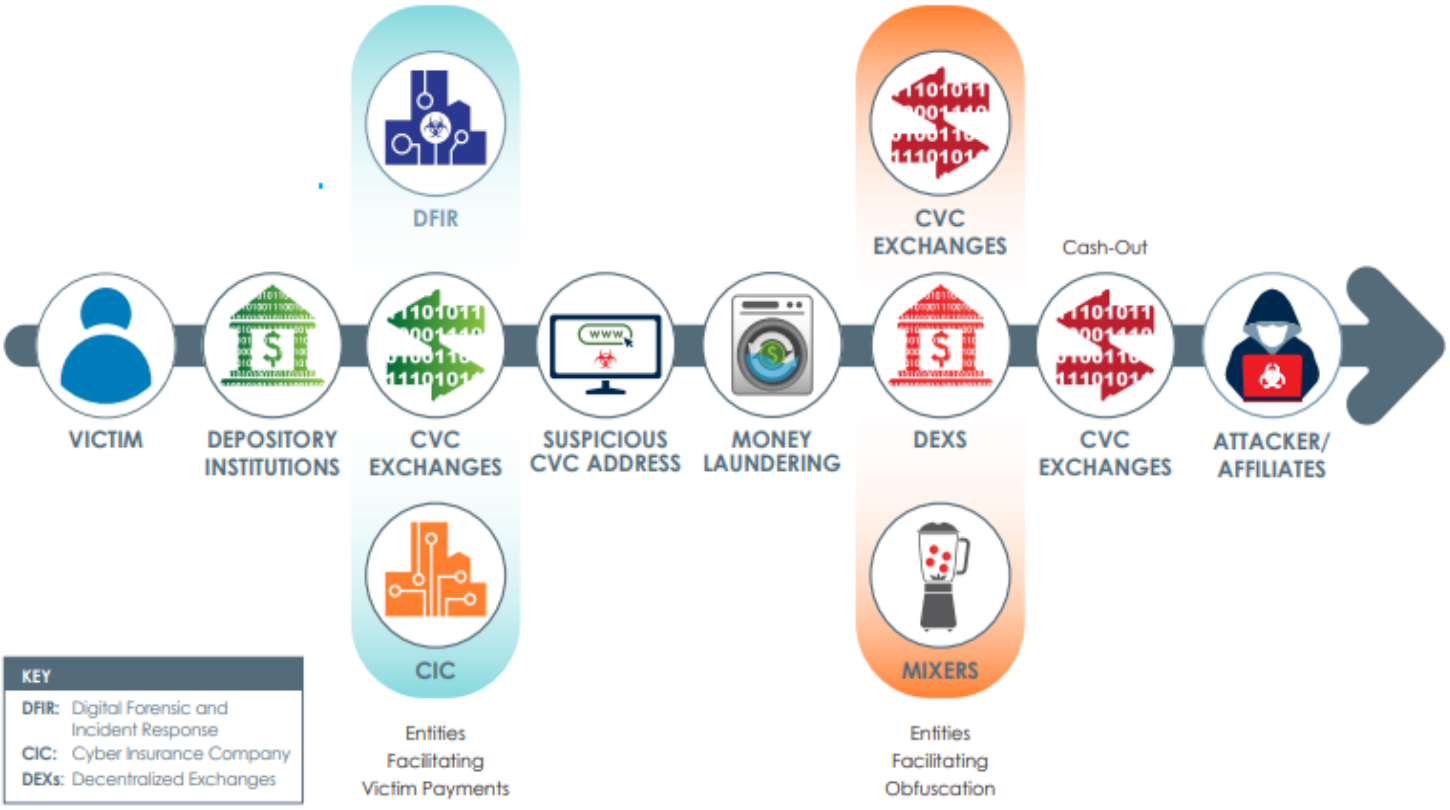
To assist with the identification of ransomware and illegal cyber activity, the advisory lists several red flags of which FIs should be aware:[4]

1. IT enterprise activity that is connected to ransomware cyber indicators or known cyber threat actors.
2. A customer informing the bank that opening a new account is in response to a ransomware incident.
3. A customer's convertible virtual currency ("CVC") address is connected to ransomware variants – may appear in open sources, commercial, or government sources.
4. An irregular transaction occurs between an organization and a digital forensic and an incident response ("DFIR") or cyber insurance company ("CIC") – especially an organization from a high-risk sector.
5. A DFIR or CIC customer receives funds from a counter party and shortly after receipt of funds sends equivalent amounts to a CVC exchange.
6. A customer shows limited knowledge of CVC during onboarding or other interactions but inquires about or purchases CVC – particularly large or rush requests.
7. A customer with no or limited history with CVC transactions sends a large CVC transaction.
8. A customer not registered with FinCEN as a money transmitter, appears to be using the liquidity provided by the exchange to execute many offsetting transactions between various CVCs.
9. A customer uses a foreign-located CVC exchanger in a high-risk jurisdiction.
10. A customer receives CVC from an external wallet and immediately initiates multiple, rapid trades among multiple CVCs.
11. A customer initiates a transfer of funds involving a mixing service.
12. A customer uses an encrypted network (e.g., the onion router) or an unidentified web portal to communicate with the recipient of the CVC transaction.

[3] Ibid.
[4] Ibid.

Figure 1[5] below details the movement of CVC in a Ransomware Incident. Criminals will go to great lengths to disguise ransomware payments. Community banks should be aware of the various steps of the exchange, so they may identify potential ransomware payments being conducted through their institution.

Figure 1. Movement of CVC in Ransomware Incidents



[5] https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf

OFAC Ransomware Advisory

In September 2021, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") issued an update to a previous advisory on the potential risks for facilitating ransomware payments.[6]

OFAC views ransomware payments as enabling "criminals and adversaries with a sanctions nexus to profit and advance their illicit aims."[7] Such payments, in the views of OFAC, both encourage and incentivize malicious actors to conduct further attacks while undermining the effects of U.S. sanctions against such actors. What's more, OFAC views a ransomware payment to a "designated malicious cyber actor" as a sanctions violation under its cyber-related sanctions program and other sanctions programs.

OFAC's advisory notes that they may impose civil penalties for sanctions violations regardless of whether a payment was made that knowingly or unknowingly violated sanctions laws and regulations. To better comply with sanctions-related issues, OFAC encourages FIs to review OFAC's sanctions compliance guide, virtual currency guidance, and implement a risk-based approach to mitigate exposure to sanctions-related violations.[8, 9]

Finally, all victims and those involved with addressing ransomware attacks should report incidents to Cybersecurity and Infrastructure Security Agency ("CISA"), local Federal Bureau of Investigation ("FBI") field office, the FBI Internet Crime Complaint Center ("IC3"), or local United States Secret Service ("USSS") field office as soon as possible. If there is ***any reason*** to suspect a potential sanctions nexus, report the event to Treasury's Office of Cybersecurity and Critical Infrastructure Protection ("OCCIP") and OFAC.

This advisory also provides contact information for those with questions regarding the scope of sanctions requirements described in this advisory. Bankers may contact OFAC's Sanctions Compliance and Evaluation Division at (1-800) 540- 6322 or (202) 622-2490.

[6] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf
[7] Ibid.
[8] https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf
[9] https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf

Where to Report Ransomware – Contact information

- Federal Bureau of Investigation Cyber Task Force
  - https://www.ic3.gov/default.aspx; www.fbi.gov/contact-us/field
- U.S. Secret Service Cyber Fraud Task Force
  - https://secretservice.gov/contact/field-offices
- Cybersecurity and Infrastructure Security Agency
  - https://us-cert.cisa.gov/forms/report
- U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection
  - OCCIP-Coord@treasury.gov; (202) 622-3000
- U.S. Department of the Treasury's Financial Crimes Enforcement Network
  - FinCEN Regulatory Support Section: frc@fincen.gov
- U.S. Department of the Treasury's Office of Foreign Assets Control
  - Sanctions Compliance and Evaluation Division: OFAC_Feedback@treasury.gov; (202) 622-2490 / (800) 540-6322
  - Licensing Division: https://licensing.ofac.treas.gov/; (202) 622-2480
- Placeholder for Regulator Incident Response Contact Information

Referenced Guides and Materials

- CISA - Stop Ransomware Website
- CISA and MS-ISAC - Ransomware Guide
- IC3 - Ransomware Factsheet
- FinCEN - FinCEN Advisory on Ransomware Payments
- FinCEN - FinCEN Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021
- NIST - Cybersecurity Framework Profile for Ransomware Risk Management
- OFAC - Sanctions Compliance Guide
- OFAC - Sanctions Compliance Guidance for the Virtual Currency Industry
- OFAC - Updated Ransomware Advisory
- USSS - A Guide to Ransomware