ACAMS

Are you familiar with the sanctions risks of ransomware payments?

Last Updated Monday 4th of September

Ransomware payments have experienced a notable increase in recent years, and while there was a decline in 2022, the trend seems poised to resume its upward trajectory. **Ransomware actors have grown in sophistication, utilizing new attack vectors and a variety of techniques to conceal and attain their illicit gains.** Amid this environment, the United States and other jurisdictions have pursued an aggressive strategy of disrupting the ransomware payment ecosystem.

Ransomware payments pose financial crime risks to both victims and other organizations, especially in the financial sector. These risks have grown in recent years, particularly as the use of the sanctions tool is a key pillar in the U.S. government's counter ransomware strategy. Indicative of this growing prominence and concern, **in March 2023 the Financial Action Task Force (FATF) published its first Report on Countering Ransomware Financing.**

What is Ransomware?

Ransomware is a form of malicious software ("malware") that aims to restrict access to a computer system or data often by encrypting data or programs within information technology (IT) systems. Victims are coerced into paying a ransom fee in return for decrypting the compromised information and restoring access to their system or data.

Ransomware Payments Present Multiple Touchpoints with the Financial Sector[1]

Successful ransomware attack completed with payment demanded in cryptocurrency.

Victim (or third party* working on their behalf) will transmit funds to a VASP, usually via:

- Wire transfer
- Automated clearinghouse
- Credit payment

Victim (or third party) will send the payment (usually from a wallet hosted at a VASP) to the virtual asset address provided by the ransomware attacker.

A variety of techniques (e.g., chain-hopping, use of tumblers and mixers) will potentially be deployed to layer the funds and obfuscate them so that they can be converted into fiat currency and deposited, spent, or reinvested into further attacks. Ultimately, the money is cashed out through unregulated VASPs, darknet marketplaces, etc.

*Third party can often be a cyber incident response firm

[1] Based on information compiled from the Financial Action Task Force's Countering Ransomware Financing Report (2023). For a more detailed analysis of the ransomware payment ecosystem, see the Institute for Security and Technology's 'Mapping the Ransomware Payment Ecosystem' (2022).

Sanctions Risks of Ransomware

Ransomware payments are generally not prohibited by governments per se. **However, ransomware payments that breach financial sanctions can pose significant legal, financial and reputational risks for the victim and actors involved in facilitating the transaction** (banks, virtual asset service providers (VASPs), insurance companies, cyber incident response firms, etc.).

Several ransomware actors have been sanctioned, as the U.S., U.K. and EU have Cyber Sanctions programs. This increases the risk of a sanctions nexus in a ransomware payment. Furthermore, a significant nexus with Russian entities is evident among known ransomware attackers. **According to FinCEN's reporting data, 75% of ransomware-related payments were linked to Russia in the first half of 2021.** Indeed, a number of Russian ransomware groups are closely linked to the Russian regime.

It's important to keep in mind the concept of **'strict liability'** in the U.S. and U.K., which is an enforcement activity that can be taken against organizations, even if facilitating a payment to a sanctioned actor was unknown.

Organizations which may be involved and consequently exposed to potential sanctions risks due to ransomware attacks:

Financial Institutions

Acting as intermediaries that victims or third parties use for transmitting funds to a VASP for purchasing of virtual assets.

VASPs

Used to purchase and transfer the type and denomination of virtual assets demanded by the criminal(s).

Insurance Companies

May cover and pay a ransom as part of cyber insurance cover.

Incident Response Firms

May be involved with negotiating the payment with the ransomware attacker, and may act on the victims behalf in purchasing and transferring virtual assets to the attacker.

Red Flags and Risk Indicators for Identifying Ransomware Victim Payments

For Financial Institutions:

- Words such as ‘ransom’ and names of ransomware groups in the payment description
- Connection between an adress with which a customer conducts transactions and ransomware variants or activity
- Open-source information on ransomware attacks on clients
- Payments made to VASPs in high-risk jurisdictions
- Outgoing payments to cybersecurity or incident response firms which specialize in ransomware remediation
- Incoming (and unusual) payments from insurance companies that specialize in ransomware remediation
- High volume of transactions to multiple accounts at a VASP

*Anonymity-enhanced cryptocurrency is intended to reduce traceability on the blockchain and protects users' privacy.

For Virtual Asset Service Providers (VASPs):

- Purchases or transfers involving anonymity-enhanced cryptocurrencies*
- An individual or organization with no history of virtual asset transactions sends funds outside of standard business practice
- A customer is impatient that a payment is taking too long
- Payments made to VASPS in high-risk jurisdictions
- A new customer purchases virtual assets and transmits the entire balance to a single address, particularly if they have a limited knowledge and/or history of CVC transactions
- A customer increases the limit on an account and sends funds to a third party
- Purchase of virtual assets by an incident response firm or insurance company for a third party
- A customer states that virtual assets are being purchased for a ransomware payment

Based on information compiled from the Financial Action Task Force’s ‘Countering Ransomware Financing: Potential Risk Indicators’ (2023) and FinCEN’s ‘Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments’ (2021)

ACAMS Resources to learn more:

- Global Ransomware Risks Survey Report (2022)
- Sanctions Masterclass: Exploring the Intersection of Ransomware, Crypto and Sanctions Risks (2022)
- Sanctions Masterclass: Nexus of Cyber, Ransomware and Sanctions Compliance (2021)
- Nexus of Cyber, Ransomware and Sanctions Compliance - A Sanctions Masterclass Follow-Up Briefing (2021)
- Stay updated on ransomware developments with the ACAMS Sanctions Monthly Update

---

Regulatory Guidance to be aware of:

- OFAC Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (2021)
- FinCEN Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments (2021)
- OFSI Guidance on Ransomware and Financial Sanctions (2023)

This information has been reviewed and is believed to be accurate as of the time of publication. ACAMS cautions that current events remain fluid and dynamic. Any developments after the time of publication may impact the accuracy of this information. ACAMS is under no obligation to update this information. The content contained herein is for general information purposes only. This information should not be considered as legal, tax, or business advice nor should it be relied upon as such. Please consult your legal, tax and business advisors with any questions regarding the application of this information to your individual circumstances.

V13092023