FATF

FATF REPORT

Countering Ransomware Financing

POTENTIAL RISK INDICATORS

March 2023

COUNTERING RANSOMWARE FINANCING: POTENTIAL RISK INDICATORS

The following potential risk indicators draw from the experience and data received from jurisdictions across the Global Network. These indicators aim to enhance the detection of suspicious transactions relating to ransomware. The list is further differentiated into various perspectives across the process of making a ransomware payment.

Before using the risk indicators, readers are encouraged to read the handling notes below and the 2023 FATF report on countering ransomware financing.

Countering Ransomware Financing

This report analyses the methods that criminals use to carry out their ransomware attacks and how they launder ransom payments.

The report highlights that authorities need to build on and leverage existing international cooperation mechanisms to successfully tackle the laundering of ransomware payments. They also need to develop the necessary skills and tools to quickly collect key information, trace the nearly instantaneous virtual transactions and recover virtual assets before they dissipate.

https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/countering-ransomware-financing.html

The existence of a single indicator in relation to a customer or transaction may not alone warrant suspicion of a ransomware offence, nor will a single indicator necessarily provide a clear indication of such an activity. However, it could prompt further monitoring and examination as appropriate.

The list of indicators complements those provided in FATF's Virtual Assets Red Flag Indicators,[1] and is relevant to both the public and private sectors. On the latter, the indicators can be relevant to VASPs, banks and other financial and payment institutions.

[1] See FATF Virtual Assets Red Flag Indicators of Money Laundering and Terrorism Financing (September 2020), available at: www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf

Banks/Other financial and payment institutions identifying ransomware victim payment

- Outgoing wire transfers to cybersecurity consulting or incident response firms that specialize in ransomware remediation
- Unusual incoming wire transfers from insurance companies that specialize in ransomware remediation
- Client self-reporting of a ransomware attack or payment
- Open-source information on ransomware attacks on clients
- High volume of transactions from same bank account to multiple accounts at a VASP
- Payment description contains words such as "ransom" or names of ransomware groups
- Payments made to VASPs in high-risk jurisdictions (see Box)

VASPs identifying ransomware victim payment

- Request to buy virtual assets by an incident response firm or insurance company on behalf of a third party.
- Customer states to the VASP that they are purchasing virtual assets due to ransomware payment.
- User with no history of virtual asset transactions sending funds outside of standard business practice
- A customer increases limit on an account and sends to a third party
- A customer seems anxious or impatient with the amount of time taking for a payment
- Purchases of or transfers involving anonymity-enhancing cryptocurrencies
- Payments made to VASPs in high-risk jurisdictions
- A new customer purchases virtual assets and transmit the entire balance of their account to a single address

VASPs identifying ransomware payment receipt/ransomware criminal account

- Following an initial large virtual asset transfer, a customer has little or no digital currency activity
- Blockchain analysis on wallet addresses reveals ties to ransomware
- Immediate withdrawal after converting funds to virtual assets
- Sending of virtual assets to wallets linked to ransomware
- Use of a VASP in a high-risk jurisdiction
- Transferring virtual assets to mixing service
- Use of encrypted network
- Verification information is a photograph of data on a computer screen or has a file name containing “WhatsApp image” or similar
- Customer’s syntax does not match the customer’s demographic
- Customer information shows customer holds an email account known for high privacy such as proton mail or Tutanota
- Inconsistent identification details or an attempt to create an account with a false identity
- Multiple accounts linked to same contact details; addresses shared under different names
- Customer appears to use a VPN
- Transactions involving anonymity-enhancing cryptocurrencies

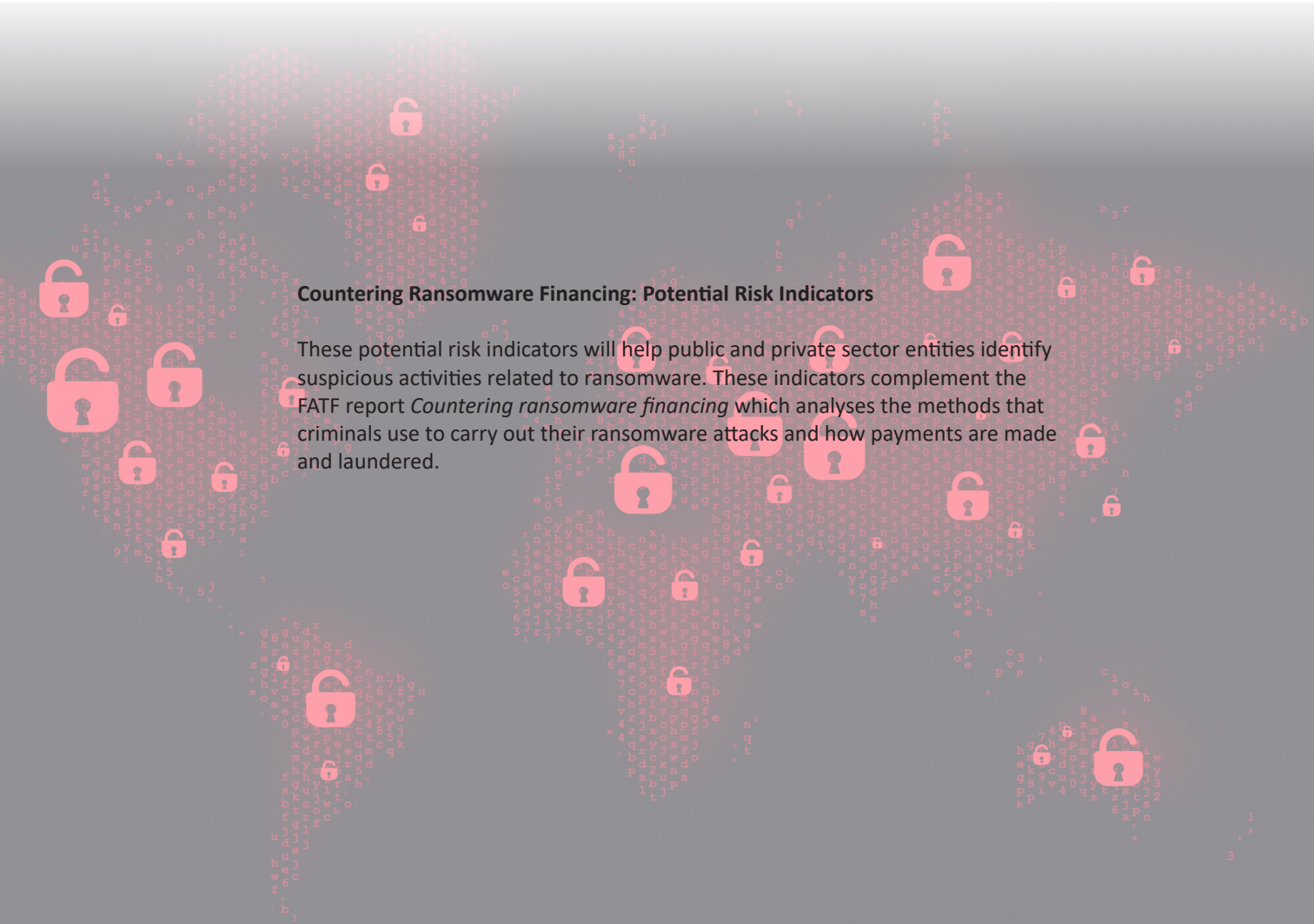
Box: Jurisdictions with higher money laundering risks

While there is no universally agreed upon definition or methodology for determining whether a jurisdiction represents a higher risk for ML/TF, the consideration of country-specific risks, in conjunction with other risk factors, provides useful information for further determining potential ML/TF risks. Indicators of higher risk include: (a) Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them; (b) Countries identified by credible sources as having significant levels of organized crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking, smuggling, and illegal gambling; (c) Countries that are subject to sanctions, embargoes, or similar measures issued by international organisations such as the United Nations; and (d) Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by the FATF statements as having weak AML/CFT regimes, especially for VASPs, and for which VASPs and other obliged entities should give special attention to business relationships and transactions.

Source: FATF (2021) Updated Guidance for a Risk-Based Approach: Virtual Assets and VASPs, para.154

www.fatf-gafi.org

March 2023



Countering Ransomware Financing: Potential Risk Indicators

These potential risk indicators will help public and private sector entities identify suspicious activities related to ransomware. These indicators complement the FATF report *Countering ransomware financing* which analyses the methods that criminals use to carry out their ransomware attacks and how payments are made and laundered.