Executive Summary

The global scale of financial flows related to ransomware attacks has grown dramatically in recent years. Industry estimates report up to a fourfold increase in ransomware payments in 2020 and 2021, compared to 2019. New techniques have increased the profitability of attacks and the likelihood of success. These include the targeting of large, high-value entities as well as ransomware as a service, where ransomware criminals sell user-friendly software kits to affiliates. The consequences from ransomware attacks can be dire and pose national security threats, including damaging and disrupting critical infrastructure and services.

Through this study, the FATF aims to improve global understanding of the financial flows linked to ransomware and highlight good practices to address this threat. The report also provides a list of potential risk indicators that will help authorities and the private sector detect such financial flows. The findings of this report draw upon experience and expertise from across the public and private sectors, including inputs and case studies from more than 40 delegations across the FATF Global Network.

A ransomware attack is a form of extortion and the FATF Standards require that it be criminalised as a predicate offence for money laundering. This report finds that payments and subsequent laundering of ransomware proceeds are almost exclusively conducted through virtual assets. Ransomware criminals exploit the international nature of virtual assets to facilitate large-scale, nearly instantaneous cross-border transactions, sometimes without the involvement of traditional financial institutions that have anti-money laundering and counter terrorist financing (AML/CFT) programs. Criminals further complicate their transactions by using anonymity-enhancing technologies, techniques, and tokens in the laundering process, such as anonymity enhanced cryptocurrencies and mixers.

The near-exclusive use of virtual assets in ransomware-related laundering further reinforces the importance of accelerating the implementation of FATF Recommendation 15, which requires jurisdictions to put in place measures to mitigate risks linked to virtual assets and to regulate the virtual asset service provider (VASP) sector. These efforts are critical to prevent criminals from easily accessing VASPs located in jurisdictions with weak or non-existent AML/CFT controls to launder the profit from their crimes.

This report also finds that ransomware attacks are generally underreported, whether due to challenges in detection by the private sector, negative impacts to the victim's business or a fear of retaliation from criminals if a victim reports an attack. This partly explains the lack of experience in investigating money laundering related to ransomware. Jurisdictions need to carry out further work to increase and enhance sources of detection and reporting. Authorities need to move quickly to collect key information and should have the necessary tools and skills to effectively trace and recover virtual assets.

Ransomware cuts across a wide range of areas and investigations may involve actors outside the traditional AML/CFT authorities, including cybersecurity and data protection agencies. As such, a multi-disciplinary approach is required to effectively tackle ransomware and associated money laundering. Due to the inherently decentralised and transnational nature of virtual assets, building and leveraging existing international co-operation mechanisms is imperative to successfully tackling ransomware-related laundering.

To strengthen the global response against ransomware and related laundering, the FATF proposes that jurisdictions take the following actions.

Proposed Actions

The information gathered for this study provided some practical examples of actions that countries can take to improve their ability to counter illicit financial flows related to ransomware. This section summarises these good practices and makes suggestions for how jurisdictions could more effectively disrupt ransomware-related money laundering.

Implement relevant FATF Standards, including on VASPs, and enhance detection

- Jurisdictions should accelerate compliance with the relevant FATF Standards on the VASP sector by implementing Recommendation 15 (including the Travel Rule[1]) as soon as possible. This ensures that VASPs are complying with the necessary AML/CFT obligations to capture critical financial information and report suspicious transactions.
- Jurisdictions should ensure that ransomware is criminalised as a predicate money laundering offence in line with FATF Recommendation 3 (e.g., as a type of extortion).
- Jurisdictions should enhance detection of ransomware by:
  - Supporting regulated entities to detect ransomware and related money laundering and report suspicious transactions, including by sharing trends, detection guides, and red flag indicators (like those contained in *Countering Ransomware Financing: Potential Risk Indicators*[2]) with the relevant reporting entities.
  - Encouraging victims to voluntarily report incidents, such as by raising awareness of available support and resources or creating safe channels for reporting.
- Jurisdictions should also consider establishing channels of communications with non-traditional actors that may not be subject to AML/CFT requirements (such as cyber insurance and incident response companies) to increase sources of detection.

Promote financial investigations and asset recovery efforts

- Competent authorities should use and adapt, as necessary, traditional law enforcement techniques as well as virtual asset-

1 The 'Travel Rule' is a key AML/CFT measure, which mandates that VASPs obtain, hold, and exchange information about the originators and beneficiaries of virtual asset transfers. This enables financial institutions and VASPs to conduct sanctions screening and to detect suspicious transactions.

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

specific techniques, to conduct ransomware-related money laundering investigations. Competent authorities should have the necessary specialised skills and expertise for successful financial investigations relating to ransomware. This includes development, access and training relating to blockchain analytics and monitoring tools.

- Jurisdictions should ensure that law enforcement has, and maintains, the necessary abilities and powers to swiftly and effectively seize and confiscate assets, particularly for virtual assets. Jurisdictions should ensure that specialised mechanisms are in place to properly manage seized virtual assets.

Adopt a multi-disciplinary approach to tackle ransomware

- Jurisdictions should ensure that they identify and assess the money laundering risks posed by ransomware in their national risk assessments. Given the decentralised nature of virtual assets and ransomware criminal groups, this includes jurisdictions with virtual asset sectors where ransomware is not currently a domestic threat. Such findings can further help support national cyber strategies by achieving a holistic national overview of ransomware risks.
- Jurisdictions should develop co-ordination mechanisms across relevant competent authorities, ranging from law enforcement, AML/CFT and cyber-crime authorities, to non-traditional partners such as cyber-security or data protection agencies. This promotes information and intelligence sharing and provides a useful platform for cross-sharing of various technical expertise.

Support partnerships with the private sector

- Jurisdictions should identify and establish mechanisms that support public-private co-operation. Jurisdictions should consider the inclusion of VASPs and other non-traditional partners in such co-operation mechanisms. This creates useful platforms to raise awareness, exchange expertise and insights, as well as support law enforcement objectives.

Improve international co-operation

- Jurisdictions should establish and actively participate in bilateral, regional, and multilateral mechanisms, such as by using liaison offices and establishing clear 24/7 contact points, to facilitate rapid international co-operation and information exchange. This helps effectively support rapid cross-border funds tracing and effective asset recovery and helps authorities to successfully dismantle transnational networks engaging in ransomware and associated money laundering.