Issue 28

Financial Intelligence Office Newsletter

Inside This Issue

Suspicious Transaction Reports Statistics (2022 Jan to Jun)

Number of STRs	2022 (Jan-Jun)	2021 (Jan-Jun)
From Financial Institutions and Insurance Companies	429 (36.0%)	415 (32.2%)
From Games of Fortune Operators	618 (51.9%)	693 (53.8%)
From Other Institutions	144 (12.1%)	180 (14.0%)
Total	1,191	1,288

- The total number of STRs received by GIF during the first half of 2022 was 1,191, which has decreased by 7.5% as compared with the same period in 2021. The change was mainly due to the decrease in the number of STRs reported by the gaming sector.
- STRs received from financial sector and gaming sector constituted 36.0% and 51.9% of total respectively.
- A total of 119 STRs were sent to the Public Prosecutions Office during Jan to Jun 2022.

International Trend - Targeted Update on Implementation of FATF's Standards on VAs and VASPs

Introduction

In June 2022, the Financial Action Task Force (FATF) has produced a targeted update[1] on implementation of its Standards on virtual assets (VAs) and virtual asset service providers (VASPs). This is the third update after FATF extended its anti-money laundering and counter-terrorist financing (AML/CFT) Standards to financial activities involving VAs and VASPs, with an aim to prevent criminal and terrorist abuse of the sector.

[1] FATF (June 2022), *Targeted Update on Implementation of the FATF Standards on Virtual Assets / Virtual Assets Service Providers.*
http://www.fatf-gafi.org/publications/fatfrecommendations/documents/targeted-update-virtual-assets-vasps.html

This report is a third targeted review of implementation, with a focus on FATF's Travel Rule on VAs and VASPs, which requires the private sector to obtain, hold and exchange beneficiary and originator information with VA transfers. The report also provides a brief update on emerging risks and market developments that FATF continues to monitor, such as Decentralized Finance (DeFi), Non-Fungible Tokens (NFTs), and unhosted wallets.

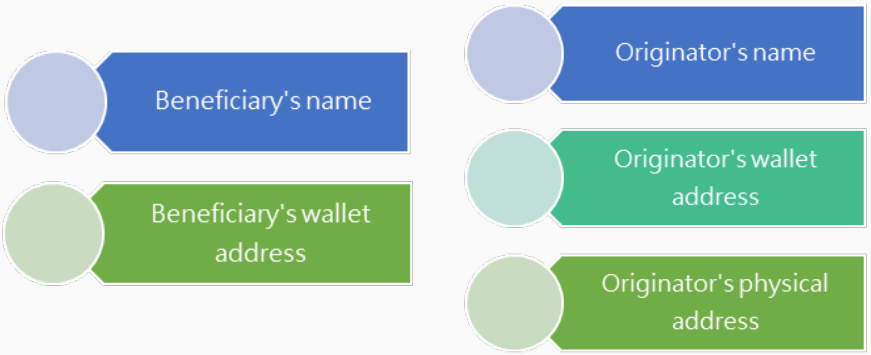
FATF's Travel Rule

◆ Travel Rule

The "Travel Rule" (developed in accordance with FATF Recommendation 16[2]) is a key AML/CFT measure, which requires VASPs to obtain, hold and exchange information about the originators and beneficiaries of VA transfers. This applies to financial institutions when dealing with financial activities involving VAs or VASPs on behalf of a customer. This also enables financial institutions and VASPs to conduct sanctions screening and to detect suspicious transactions.

◆ Required Travel Rule Information

The FATF's Updated Guidance[3] clarifies the types of information that VASPs and financial institutions are required to send/receive for the Travel Rule.



In addition to the above, some jurisdictions may require additional information to assist VASPs detecting relevant money laundering/terrorist financing (ML/TF) risks, and to meet broader AML/CFT requirements such as targeted financial sanctions. The information may include: the purpose of the VA transfer, source of VA funds, and residential addresses of the beneficiary.

[2] FATF Recommendation 16 is "Wire Transfer". According to new revision in Recommendation 15 "New Technologies" in relation to VA and VASPs, FATF requires VASPs to implement preventive measures under Recommendations 10 to 21. As such, Travel Rule for VASPs was developed under the requirement of Recommendation 16.

[3] FATF (October 2021), *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Assets Service Providers*.
https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html

◆ Progress Made by Private Sector in Implementing Travel Rule

Until now, the private sector has generally made progress in facilitating Travel Rule implementation. Technological solutions are currently available to support compliance, albeit with some limitations, and Travel Rule providers have started taking early steps to ensure interoperability with other solutions. Nevertheless, the private sector needs to further strengthen interoperability between solutions, and to ensure full compliance with the FATF Standards, to enable global implementation.

As jurisdictions and the private sector have implemented the Travel Rule, they have found challenges to implementation, especially between jurisdictions that regulate VAs and VASPs, and those that do not (the delay in implementing the rule is known as the "sunrise issue"[4]). This highlights the need for jurisdictions to continue to coordinate on common issues, and for the private sector to advance global technological tools that can accommodate for nuances across jurisdictions.

◆ Data Protection and Privacy (DPP) Issues Relevant to Travel Rule

Based on the consultations made by FATF, industry highlighted DPP issues as key considerations for Travel Rule implementation. The third targeted review of implementation report as mentioned above finds that most jurisdictions require licensed/registered VASPs to meet local DPP regulations when processing any personal data in accordance with their domestic AML/CFT requirements.

FATF recognizes the importance of DPP issues, and the Updated Guidance (October 2021)[5] clarifies that VASPs and financial institutions should take into account the robustness of the counterparty's data security controls when deciding whether to send Travel Rule and other similar data. The above Updated Guidance stated that VASPs and financial institutions need to assess the counterparty's AML/CFT controls to avoid submitting their customer information to illicit actors or sanctioned entities and should also consider whether there is a reasonable basis to believe the VASP can adequately protect sensitive information.

[4] The "sunrise issue" has resulted in situations where Travel Rule requirements enter force at different speeds across jurisdictions. To respond to this, FATF's March 2022 survey highlights that some jurisdictions are: (i) introducing temporary flexibility for domestic requirements to address delays in global implementation, and (ii) providing guidance to the domestic VASPs on how to deal with situations where counterparties are unlicensed/unregistered, or unable to share Travel Rule data.

[5] FATF (October 2021), *Updated Guidance for a Risk-Based Approach to Assets and Virtual Assets Service Providers.* https://www.fatf-gafi.org/publications/atfrecommendations/documents/guidance-rba-virtual-assets-2021.html

Market Developments and Emerging Risks

Since FATF published its Updated Guidance for a risk-based approach VAs and VASPs, which was the second 12-month review in July 2021, FATF has continued to monitor and discuss emerging VA developments, such as DeFi and NFTs. DeFi and NFTs markets have continued to grow, both FATF members and the private sector identify DeFi and NFTs as a challenging area for implementation of the FATF Standards.

The private sector should understand risks, mitigation measures, and approaches to the issues of applying the FATF Standards to DeFi and NFTs. In addition, raising public awareness of common trends in ransomware payments and related money laundering through VAs and VASPs is important to detect illicit fund flows and suspicious transactions.

Below are the definition of DeFi and NFTs as well as their potential illicit financial risks:

Decentralized Finance (DeFi)

Defi is the "decentralized or distributed application (DApp)" which offers financial services, such as those offered by VASPs. It is distinct to decentralized VAs such as Bitcoin, Ethereum, and Tezos. As clarified in FATF's Updated Guidance (October 2021), the FATF Standards do not apply to software. Nonetheless, the FATF Standards can apply to persons who maintain control or sufficient influence over a DeFi arrangement or protocol providing VASP services.

Examples of DeFi

SYNTHETIX AAVE VCDA Cardano DeFi Alliance

Potential illicit finance risks related to DeFi

⇒ DeFi protocols designed without appropriate customer due diligence (CDD) verification, or other AML controls, can be used to perform "chain-hopping" which can make the transactions more difficult to trace.

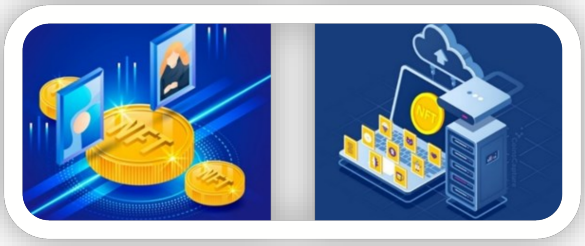
⇒ There is an increased availability and use of privacy-enhancing technologies such as mixers that can make it challenging to trace the origin and destination of funds.

◆ Non-Fungible Tokens (NFTs)

NFTs are digital assets that are unique, rather than interchangeable, and that are in practice used as collectibles rather than as payment or investment instruments. They are not VAs generally speaking for the purpose of the FATF Standards. Nevertheless, jurisdictions should apply the FATF Standards on VAs to NFTs in cases they perform the same function as VAs (used for payment or investment purpose).

◆ Examples of NFTs

⇒ Unique digital artworks
⇒ Digital sport cards
⇒ In game items
⇒ Digital collectibles and rarities
⇒ Domain names
⇒ Music royalties via NFTs



◆ Potential illicit finance risks related to NFTs

⇒ NFTs take different forms and applications ranging from art work to representations of ownership of physical assets. Also, NFTs can be used as collateral for further VA borrowing and lending. Such diversity of NFTs may make it challenging to identify high risk NFTs.

⇒ Regulation and supervision of NFTs is nascent or non-existent in many jurisdictions, and it can be difficult to ascertain activities conducted using the NFTs.

Case Study

Bank A found that 4 customers whose background and financial status were highly incommensurate with the large amount of suspicious transactions recorded in their personal bank accounts. Between February 2020 and March 2022, they received large amount of unidentified funds from third parties, including 440 individuals and 40 companies, as well as carried out more than 4,000 times cash deposits through CDM, involving a total of HKD550 million. After receiving the funds, the 4 customers transferred to other different personal and corporate accounts, involving 200 third-party accounts and 15 shell company accounts. Bank A also found that one of its customers had remitted to an overseas cryptocurrency exchange trading platform. In the account opening forms of the 4 customers, they declared that their occupations were clerk, hotel employee, company manager and housewife, and the accounts were used as savings purposes. Thus, Bank A reported the case to law enforcement agency and financial intelligence unit.

After analysis, the financial intelligence unit found that one of the customers had conducted a large number of cryptocurrencies transactions through the same overseas cryptocurrency exchange trading platform, and converted the cryptocurrencies into fiat currencies, mainly in US dollars, and then deposited the funds, with an equivalent amount of HKD20 million, into local bank accounts or electronic wallets. Law enforcement agency found that 4 suspects were members of a ML group, they traded at an overseas cryptocurrency exchange trading platform with cryptocurrencies from unknown sources, and then deposited the funds into local bank accounts or electronic wallets. On the other hand, the 4 suspects received a large amount of funds through their bank accounts and transferred to other third-party personal and shell company accounts. Some of the funds were also remitted to other jurisdictions through money remittance company. With the use of unrelated third-party accounts to process funds from unknown sources increased difficulty of the investigation.

※ Red flags:

⇒ Background and occupation are highly incommensurate with the account transaction pattern and scale. For example, a suspect with low taxable income and does not have any property under his name, however there are more than 1,000 transaction records are found in his account.

⇒ Involve overseas cryptocurrency exchange trading platform and make use of the characteristic of high degree of anonymity of cryptocurrencies.

⇒ Frequent and rapid funds flows, the account may be used as temporary repository of funds.

⇒ The transaction volume is far beyond the normal range of an individual's account. Involvement of many third-party or shell company accounts and the use of unrelated third-party accounts to process funds from unknown sources increase difficulty of the investigation.

⇒ Use of numerous shell companies with the address provided by company service provider, and no transaction occurs after account opening.

※ Recommendations:

⇒ Should carry out adequate level of CDD, including checking the background and transaction pattern of any suspicious account holders. If it is a company account, it has to be alert whether there are normal operating expenses, such as salaries and rents, etc.

⇒ As cryptocurrency transactions are popular in recent years, criminals may take the opportunity to use the characteristic of high degree of anonymity of cryptocurrencies to conduct illegal activities. If the transaction involves cryptocurrencies or cryptocurrency exchange trading platform, and the transaction amount is large and cannot be justified by the suspect's financial capability, a suspicious transaction report should be reported to GIF.

⇒ Pay more attention to news/media reports and the latest international trends of ML/TF so as to assist in detecting any suspicious transactions in relation to cryptocurrencies.

CONTACT US

Published in November 2022
Published by: Financial Intelligence Office, Macao Special Administrative Region Government

Address : Avenida Dr. Mário Soares, Nos. 307-323, Edifício "Banco da China", 22º andar, Macau

Tel : (853) 2852 3666
Fax: (853) 2852 3777
E-mail : info@gif.gov.mo
Website : http://www.gif.gov.mo

If you have any suggestions and enquiries on this newsletter, please feel free to contact *GIF*.