FATF

FATF Report

Understanding and Mitigating the Risks of Off-shore Virtual Asset Service Providers

March 2026

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2026), *Understanding and Mitigating the Risks of Offshore Virtual Asset Service Providers (oVASPs)*, FATF, Paris, France,
https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/understanding-mitigating-risks-offshore-vasps-2026.html

Table of Contents

1. Understanding the landscape

1.1. Background

1. In 2019, the FATF agreed to extend the application of the FATF Standards to Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs). In summary, through amendments to Recommendation 15 (R.15) and its Interpretative Note (R.15/INR.15), this required jurisdictions to:
    - Identify, assess, and understand the money laundering and terrorism financing (ML/TF) risks emerging from VA activities and the activities or operations of VASPs.
    - License or register VASPs[1] to prevent them from being misused by criminals or their associates.
    - Subject VASPs to supervision or monitoring by competent authorities by applying a risk-based approach to ensure that measures to prevent or mitigate ML and TF are commensurate with the risks identified.
    - Require VASPs to identify, assess, take effective action, and implement preventive measures, such as conducting customer due diligence and monitoring for suspicious activity.
    - Mandate an authority to apply risk-based supervision to VASPs to ensure they meet their obligations.
2. The aim of these changes was to protect the financial system from ML/TF/PF risks by clarifying that VASPs should implement preventive measures comparable to those required of financial institutions (FIs) as well as by ensuring that the sector is subject to effective, risk-based supervision. However, implementation of R.15 across the FATF Global Network has lagged since 2019, and many jurisdictions still face challenges in establishing VASP regimes and in identifying natural or legal persons conducting VASP activities.[2]

[1] The FATF standards require jurisdictions to develop and implement jurisdictional approaches to VASPs either to permit the use of VA and VASPs or to partially or explicitly prohibit their use.

[2] 2025 Targeted Update Report on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers

Table 1. Overview of FATF work on VAs and VASPs

2018	• Recommendation 15 amended including addition of new definitions "virtual asset" and "virtual asset service provider".
2019	• Adoption of Interpretive Note to R.15 • Creation of the FATF Virtual Assets Contact Group (VACG) • Initial guidance for regulators: A risk-based approach to VAs and VASPs (updated in 2021)
2020	• 12 month review of the new FATF Standards: 1st12-month review • Report to the G20: FATF Report to the G20 on So-called Stablecoins • Risk indicators: List of Red Flag Indicators of ML/TF through VAs
2021	• Updated guidance[3]: Updated Guidance for a Risk-Based Approach to VA and VASPs • 24 month review of the FATF Standards: 2nd12-month review
2022	• Report on R.15 compliance, with a particular focus on the Travel Rule, and emerging VA risks: Targeted Update on Implementation of the FATF Standards on VA and VASPs
2023	• Report on ransomware, with focus on VA risks and trends: Countering Ransomware Financing • Report on R.15 compliance, with a particular focus on the Travel Rule, and emerging VA risks: Targeted Update on Implementation of the FATF Standards on VA and VASPs
2024	• Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity
2025	• Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity • Best Practices in Travel Rule Supervision • Quick guide on assessing the Money Laundering risks of virtual assets (VA) and virtual asset service providers (VASP)

3. These challenges are particularly acute for offshore VASPs (oVASPs). For this paper, oVASPs refer to VASPS created under the laws of one jurisdiction ("home jurisdiction") with or without a physical presence and who provide services to clients domiciled or residing in jurisdictions outside of its jurisdiction of incorporation or physical location ("host jurisdiction").[4] The paper focuses on these situations, particularly where the oVASP actively provides such services without being licensed or registered in the relevant jurisdictions, which can increase jurisdictions' exposure to ML/TF risks, distort competition, and undermine the effectiveness of domestic regulatory frameworks.

4. A growing number of jurisdictions require VASPs to be registered or licensed where they provide services, regardless of physical presence. However, many of these jurisdictions continue to report difficulties in detecting offshore providers, effectively supervising their regulated VASPs, and securing timely international co-operation. Several other jurisdictions only place licensing or registration obligations on VASPs located or incorporated in their jurisdiction, which can present vulnerabilities exploited for ML/TF/PF purposes. These vulnerabilities can be compounded if oVASPs are based or incorporated in jurisdictions without Anti-Money Laundering,

[3] The 2021 updated Guidance included updates focusing on the following six key areas: clarification of the definitions of VAs and VASPs; guidance on how the FATF Standards apply to stablecoins; additional guidance on the risks and the tools available to jurisdictions to address the ML/TF risks for peer-to-peer transactions; updated guidance on the licensing and registration of VASPs; additional guidance for the public and private sectors on the implementation of the Travel Rule; and principles of information-sharing and co-operation amongst VASP supervisors.

[4] *Home jurisdiction* refers to the country where an offshore VASP is created and/or located. *Host jurisdiction* refers to a country into which an offshore VASP actively provides services, including without physical presence. For the purposes of this paper, references to a "host VASP" describe an offshore VASP in its role of providing services in a host jurisdiction.

Countering the Financing of Terrorism, and Countering Proliferation Financing (AML/CFT/CPF) frameworks for virtual assets and VASPs. While host jurisdictions may adopt measures to mitigate risks from such activity, home jurisdictions retain primary responsibility for the effective licensing, supervision and enforcement of AML/CFT/CPF obligations for VASPs created or located in their jurisdiction, including on a group-wide basis.[5] Recognising this growing phenomenon, the FATF's Virtual Assets Contact Group (VACG) launched dedicated work on oVASPs in October 2025.

1.2. Scope of the report

5. The objective of this report is to better understand the risks of oVASPs with a view to identifying good practices in mitigating these risks. Specifically, the report analyses how oVASPs structure their activities to avoid or evade regulatory obligations and how illicit actors exploit the vulnerabilities. The report also presents good practices to detect, license or register oVASPs, as well as to enforce sanctions for non-compliance with AML/CFT/CPF obligations and roll-out mitigating measures (e.g., reducing unregistered or unlicensed oVASPs' ability to actively provide services in a market where they are not regulated). It concludes with possible recommendations for stakeholders.

6. As more jurisdictions implement R.15, opportunities narrow for VASP to operate in jurisdictions with weak or non-existent AML/CFT/CPF frameworks. In the interim, jurisdictions must find ways to mitigate risks from offshore business models based or incorporated in jurisdictions without AML/CFT/CPF frameworks for VAs and VASPS. In this short guide, any reference to practices applied in a particular jurisdiction are provided by way of example only and should not be considered FATF-approved or an endorsement of the effectiveness of any jurisdiction's system. FATF guidance products are not binding.

7. This **targeted** report should be read alongside the FATF's broader guidance and work on VAs available on the FATF Website: the 2021 Updated Guidance for a Risk-Based Approach to VA and VASPs and past Targeted Update reports issued since 2022. These annual updates have sought to monitor progress in areas key to this report topic and have also included dedicated mentions to oVASPs since 2024.

1.3. Status of implementation of the FATF Standards

The applicable framework

8. The FATF Standards state that jurisdictions should license or register VASPs that are incorporated or located in their jurisdiction. The Standards also allow – but do not mandate – jurisdictions to extend licensing or registration requirements to VASPs that offer services to customers in, or conduct operations from, their jurisdiction, regardless of where the VASP is created or located. This activity-based approach is discretionary but is intended to enable jurisdictions to bring offshore entities within the scope of AML/CFT/CPF supervision based on risks.

[5] The 2021 Updated FATF Guidance recalls that VASPs should be subject to risk-based AML/CFT/CPF supervision in the jurisdiction where they are created or where their place of business is located and that supervisors should be able to obtain and share relevant information to support effective international co-operation (inter alia, paragraphs 5, 6, and 143).

Box 1. OVASPs in the FATF Standards (INR.15.3)

INR 15.3 VASPs should be required to be licensed or registered. At a minimum, VASPs should be required to be licensed or registered in the jurisdiction(s) where they are created.[6] In cases where the VASP is a natural person, they should be required to be licensed or registered in the jurisdiction where their place of business is located. **Jurisdictions may also require VASPs that offer products and/or services to customers in, or conduct operations from, their jurisdiction to be licensed or registered in this jurisdiction**. Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a VASP. **Jurisdictions should take action to identify natural or legal persons that carry out VASP activities without the requisite license or registration, and apply appropriate sanctions.**

9. The Standards' flexibility with regards to licensing or registration of oVASPs allows jurisdictions to take risk-based action, including the possibility of prohibiting the activities of VASPs. While there is no mandatory requirement to license or register oVASPs, the Standards still require jurisdictions to identify unlicensed activity and apply appropriate sanctions. Other parts of the Standards should also inform how jurisdictions approach oVASPs (e.g., R.13 vis-à-vis nesting activity or R.18 for global VASP groups). The Standards also require jurisdictions to identify, assess and understand the ML/TF/PF risks emerging from VA activities and the activities or operations of VASPs – including those activities carried out by oVASPs - to build mitigating measures. Moreover, jurisdictions should subject VASPs to adequate regulation and risk-based supervision or monitoring by a competent authority.

10. In practice, this flexibility has resulted in a wide range of national approaches, which can also allow for regulatory arbitrage. As shown below, oVASPs have been observed exploiting differences in registration/licensing thresholds, territorial scope, and supervisory capacity to reject oversight and offer services across borders without effective oversight for AML/CFT/CPF. This fragmentation can increase illicit finance risks.

11. Given the cross-border nature of oVASP activity, international co-operation is critical to both understand and mitigate these risks. According to INR.15.8, jurisdictions should provide for the widest possible range of international co-operation in this space. In particular, supervisors of VASPs should exchange information promptly and constructively with their foreign counterparts, regardless of the supervisors' nature and differences in the nomenclature or status of VASPs. The 2021 Updated Guidance expands on this, noting:

    a) The importance of FIU-to-FIU co-operation in relation to cross-border VASP operations; and

    b) The need for sufficient oversight and regulatory control for VASPs operating in-jurisdiction.

[6] References to creating a legal person include incorporation of companies or any other mechanism that is used.

Box 2. INR 15.8 International co-operation on VASPs

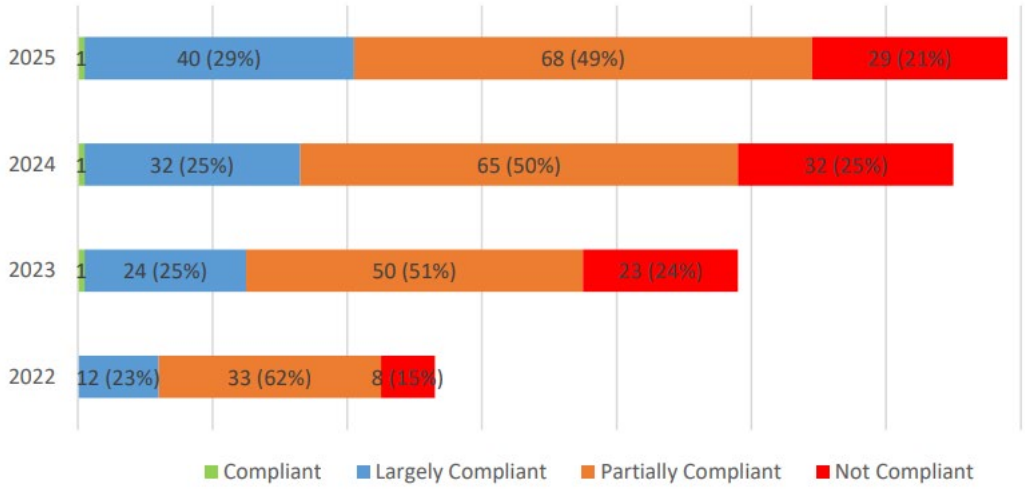
Jurisdictions should rapidly, constructively, and effectively provide the widest possible range of international co-operation in relation to money laundering, predicate offences, and terrorist financing relating to virtual assets, on the basis set out in Recommendations 37 to 40. In particular, supervisors of VASPs should exchange information promptly and constructively with their foreign counterparts, regardless of the supervisors' nature or status and differences in the nomenclature or status of VASPs.

12. Weak AML/CFT/CPF regulation for VAs and VASPs and investigation capacity in many jurisdictions reduce jurisdictions' ability to provide meaningful international co-operation.

State of play

13. As of April 2025, 138 jurisdictions have been assessed for compliance with the FATF standards for VAs and VASPs. While the proportion of jurisdictions partially compliant (PC) with the revised R.15 remains similar (49%; 68 of 138 jurisdictions) to the results in 2024 (50%; 65 of 130 jurisdictions). 29% of jurisdictions (40 of 138 jurisdictions) are now largely compliant (LC) with the FATF's requirements for VA/VASPs (25%; 32 of 130 jurisdictions in 2024). The proportion of jurisdictions not compliant (NC) with the requirements has also decreased from 25% to 21%.[7]

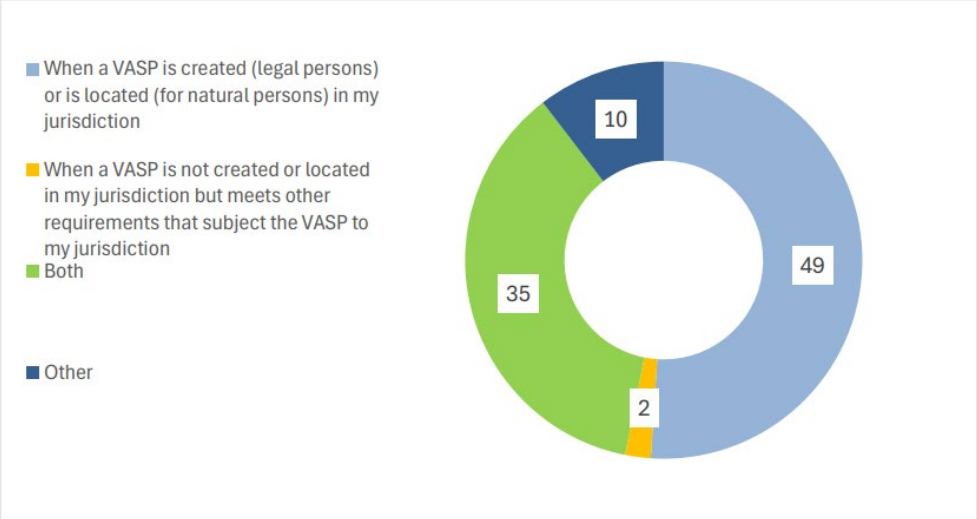
Figure 1 – 2025 survey results: Compliance with R.15 (as of April 2025)



14. FATF survey results from 2025 indicate that the vast majority of jurisdictions with VASP regimes (83%; 80 of 96) at least require VASPs that are created (legal persons) or located (natural persons) within their jurisdiction to license or register.

[7] These results refer to the 2025 survey. For more detail, please see the 2025 Targeted Update.

Figure 2 – 2025 survey results: Does your jurisdictions require VASPs to be registered/licensed?



15. Since 2024, the FATF has specifically collected information on jurisdictions' approaches to oVASPs. Based on the 2025 survey, just under half of jurisdictions that have introduced a registration or licensing requirement (46%; 37 of 80) have adopted an activity-based approach, requiring oVASPs to be licensed or registered where they engage in defined activities such as advertising, onboarding local users, or offering services into the market. These approaches aim to mitigate ML/TF/PF risks posed by offshore business models. The remaining jurisdictions apply the core FATF standard, requiring licensing or registration only for VASPs that are created or physically located in their jurisdiction.

16. Despite the finding that some jurisdictions regulate oVASPs in certain circumstances, most jurisdictions report persistent challenges in identifying oVASPs, particularly determining when licensable activity is taking place and enforcing requirements against entities without a physical presence. In addition, jurisdictions also report challenges in domestic coordination and the persistence of international co-operation related to oVASPs. These challenges are most acute in jurisdictions with broader AML/CFT/CPF supervisory weaknesses.

17. In practice, the optional nature of activity-based licensing under INR.15.3 means that while some jurisdictions regulate oVASP activities, others do not, resulting in diverging regulatory regimes across jurisdictions. These differences reflect variations in how jurisdictions have implemented activity-based licensing (e.g., different definitions and regulatory anchors), creating gaps where R.15 is implemented unevenly. As a result, effective international co-operation may not be possible, including with the relevant oVASP supervisor, thereby limiting the effectiveness of domestic risk-mitigation measures. Varying regulatory approaches have also been raised as a concern by industry stakeholders attending meetings of the Virtual Asset Contact Group. These gaps underpin the characteristics, risks and supervisory challenges associated with oVASPs described in Part I of this report.

2. Characteristics, risks and supervisory challenges linked to oVASPs

2.1. Characteristics of oVASPs

18. As described above, an oVASP is a VASP that provides services to clients in jurisdictions outside its jurisdiction of incorporation or physical location. OVASPs can be incorporated in any jurisdiction and may decide to operate across multiple markets. Where oVASPs are incorporated or physically located in jurisdictions with weak or underdeveloped AML/CFT/CPF regulatory and supervisory frameworks, for VAs and VASPs, it can increase the risk of ML/TF/PF abuse not only in the home jurisdiction but also the host jurisdictions in which the oVASP offers products and services. This risk can be compounded if the latter jurisdictions do not require licensing or registration of oVASPs because they often lack a physical or legal presence in the jurisdictions where their customers reside and may provide VA related services.
19. Without licensing or registration requirements, oVASPs can offer services in host jurisdictions without being licensed or registered locally. Moreover, the structure and operations of some oVASPs can complicate identification of oVASPs or enforcement of applicable requirements even in jurisdictions that require licensing or registration of oVASPs. In some cases, oVASPs also serve users in jurisdictions where VA activity or VASP services are restricted or prohibited.
20. Typically, oVASPs actively solicit customers through online platforms, promotional campaigns, affiliate schemes, or sponsored events. Core corporate functions, including senior management, compliance operations, and data infrastructure, are frequently located outside the jurisdictions where services are offered, limiting the ability of domestic authorities to engage with the entity and access KYC/CDD data. In some cases, these VASPs may actively lower KYC requirements, offering advantageous pricing enabled by lower compliance costs and undermining a level playing field for regulated VASPs.

Case study – oVASPs in India

Under India's AML/CFT/CPF framework, oVASPs are required to register in India where they provide services or products to persons in India, regardless of physical presence.

OVASPs operating in India commonly onboard Indian customers with little or no KYC, accept deposits through domestic payment channels such as Unified Payments Interface (UPI) or card networks, and enable withdrawals to Indian bank accounts or wallets by routing payouts through locally-registered VASPs or compliant intermediaries.

These models showcase how oVASPs are actively providing services in India despite de-facto circumventing India's regulatory perimeter. In addition, these also highlight the importance of the wider financial sector (domestic FIs, payment institutions, and local VASPs) in enabling, or not, oVASP's access to the Indian market.

Source: FIU India

21. Industry representatives[8] have sought to categorise oVASPs. Based on this work and jurisdictions experiences, this report identifies two main categories:
    a) Unintentional – oVASPs may be unaware of, misunderstand, or misinterpret the regulatory framework applicable to the activities they are undertaking.
    b) Intentional – oVASPs willfully circumvent registration/licensing requirements as part of their business model. This wilful circumvention may happen after unsuccessful licensing or registration processes or revocation of license or registration.

22. In practice, intentional oVASPs may design their operating models to minimise regulatory touchpoints. This may include limiting formal presence in jurisdictions in which they offer products and services, fragmenting group structures, or routing customer activity through affiliates or intermediaries in other jurisdictions. These features contribute to the difficulty of attributing responsibility for AML/CFT/CPF obligations and identifying the entity responsible for servicing domestic users even for jurisdictions that require licensing or registration of oVASPs.[9] OVASPs may also be exposed to off-chain activity that is not visible through on-chain analytics (e.g., off-chain internal record-keeping system and the VA remains in the same on-chain omnibus wallet or account), which may further affect risk identification and pose increasing challenges for authorities trying to obtain information.

23. Drawing on their blockchain analytics data, TRM representatives[10] have observed preliminary indications that oVASPs may have significantly higher exposure to on-chain illicit activity compared to regulated onshore, local, VASPs. In addition, oVASPs may also exhibit activity patterns suggesting that a substantial share of their user

[8] TRM Labs Guide "How Regulators Can Detect and Investigate Unregistered VASPs Using Blockchain Intelligence" (2024).

[9] Especially for those jurisdictions that have not imposed regulatory requirements on offshore VASPs actively providing services to their residents.

[10] A blockchain analytics company.

interactions (e.g., visits by users) originate from jurisdictions other than the one in which they are formally established.

2.2. Vulnerabilities and barriers to effective AML/CFT/CPF measures and supervision

24. Certain characteristics of oVASPs create vulnerabilities and constraints that make it challenging for competent authorities to regulate and supervise them – where a jurisdiction decides to do so – or to contact them when information is required for supervisory, intelligence, or investigative purposes. For example, oVASPs may dismiss or fail to respond to direct requests from foreign competent authorities citing (i) the lack of a legal obligation to respond to such authorities; and (ii) requests being insufficiently specific.[11]

Lack or inadequate physical presence

25. OVASPs frequently maintain their compliance functions, key personnel, and data infrastructure outside the jurisdictions where their customers are located. This creates vulnerabilities, as supervisors report that it significantly constrains their ability to engage with the entity, conduct effective oversight, or request information for AML/CFT/CPF purposes. In some cases, the oVASP may have a distributed presence, so they are not concentrated in any one jurisdiction, or may purposefully obfuscate their location.

26. In some cases, oVASPs appoint nominal or ineffective compliance representatives in the servicing, or host, jurisdiction, including so-called "dummy" principal or compliance officers. If a jurisdiction allows oVASPs to operate under such governance arrangements, supervisors can face delays or non-responsiveness to information requests, undermining oversight of core AML/CFT/CPF obligations, including suspicious transaction reporting. Common indicators include:

    a) limited access by the principal officer to customer information (CDD/KYC);

    b) insufficient seniority; and

    c) lack of access by the principal officer to key senior management officials.

Global pooling of customers

27. Regardless of whether a VASP maintains some onshore presence, supervisors have observed that some VASPs with global operations deliberately structure customer onboarding and account management in ways that obscure jurisdictional attribution. Customers may onboard through mobile applications or platforms with limited geo-location controls beyond self-declared information or basic IP address checks. In practice, customer accounts may be serviced through pooled or group-level arrangements rather than clear assignments to a locally supervised entity, which can create vulnerabilities in accountability and oversight. Such structuring can obscure which entity bears responsibility for AML/CFT/CPF obligations and hinder competent authorities' ability to obtain timely and reliable information from VASPs servicing local customers. FIUs have reported that such customer-pooling and routing practices are recurrent across multiple global VASP groups. In some cases, such pooling may

[11] Evidence from a Eurasian Group (EAG) survey conducted between 2023 and 2025, drawing on responses from seven of the nine EAG member jurisdictions.

seek to obscure the active provision of products and services in specific jurisdictions, including to avoid triggering AML/CFT/CPF obligations.

Box 3. Pooling of customers in offshore branches

France

France's FIU has observed cases in which a France-based VASP, when responding to requests for information, stated that the customers under inquiry were not serviced by its French entity but by another branch within the same global VASP group. In several instances, these related entities were established in jurisdictions with weak or no VASP regulation, limiting the ability of competent authorities to obtain timely and reliable information.

Spain

The Spanish FIU has identified cases in which Spain-based VASPs have responded to requests for information by arguing that the customers under investigation were not serviced by the Spain-based VASP itself, but by a branch located in a third country within the same global VASP group. In these cases, the supposed branch turned out to be an independent external company that performs data-processing functions only and is not licensed as a VASP in its jurisdiction. As a result, and in the absence of AML/CFT/CPF obligations, the external company disputes the authority of a foreign FIU to request customer information from it.

To overcome this situation, SEPBLAC has sought the relevant information through the FIUs of the third countries involved. This approach has not always been successful, in particular where the VASP group operates through small intermediary VASPs across multiple jurisdictions.

28. Supervisors have also noted that an increasing number of oVASPs operate through decentralised delivery models, including services provided exclusively through mobile applications or web-based interfaces. These models can limit visibility and reduce the effectiveness of traditional supervisory tools. In some cases, these VASPs also facilitate access to obfuscation services, including mixers or chain-hopping mechanisms.

2.3. Typologies and risks

29. This section provides an overview of key typologies associated with oVASPs, as well as the risk impacts these typologies can generate or amplify. These typologies reflect the methods through which oVASPs provide services across borders, evade applicable regulatory requirements, or obscure customer activity, resulting in heightened exposure to illicit finance risks compared to domestically supervised entities.

Active targeting and circumvention

30. Offshore VASPs may actively solicit or serve customers in jurisdictions where they are not licensed or where VA activity is restricted or prohibited, including by advising users on how to bypass regulatory requirements (e.g. through the use of VPNs or the provision of false information). Affiliate schemes and online promotion are commonly used to reach customers, including through social media, encrypted messaging

applications, or decentralised communication channels. These practices resemble those observed in online fraud schemes and are facilitated by limited consumer awareness of licensing and regulatory status, which may reinforce the appeal of offshore platforms.

Case study - targeting of US residents

In February 2025, Aux Cayes Fintech Co. Ltd. (OKX), a Seychelles-based entity and one of the world's largest exchanges, pled guilty to operating an unlicensed money-transmitting business in the United States.[12]

Although OKX had an official policy purporting to block U.S. users, it actively targeted and served retail and institutional customers in the United States. OKX knew that providing such services required registration as a money services business with FinCEN, but chose not to register.

From 2017 to November 2022, OKX allowed customers to open accounts, receive and transfer funds, and trade without completing a KYC process, thereby executing transactions for users it could not identify. Until early 2024, OKX also permitted trading through "non-disclosure brokers," who provided no identifying information on the underlying customer on whose behalf they were acting. Even after OKX started to progressively roll-out KYC controls, OKX staff continued to advise U.S customers on ways to provide false information to bypass its own prohibition to service U.S. persons.

OKX agreed to pay monetary penalties totalling more than $504 million.

Source: United States

Nested exchanges

31. OVASPs are frequently observed relying on nested or intermediated arrangements to access trading, liquidity, and fiat currency on- and off-ramps,[13] perhaps in efforts to avoid direct supervision in the jurisdictions in which they offer products and services. In these arrangements, oVASPs may have accounts at VASPs that are licensed or registered in such jurisdictions.[14] While nested activity can be legitimate, as VASPs may nest with a larger provider to benefit from their liquidity, they can also pose illicit finance risks.

32. Supervisors and industry sources[15] report that some oVASPs deliberately misrepresent themselves as retail users when opening and accessing nested accounts

12. https://www.justice.gov/usao-sdny/pr/okx-pleads-guilty-violating-us-anti-money-laundering-laws-and-agrees-pay-penalties

13 On and off ramps provide gateways to and from the traditional regulated financial system, in particular those converting from fiat money to VAs and vice versa.

14 As described in the 2021 FATF VA Guidance, nested VASP relationships can be analogous to correspondent relationships, where one VASP provides accounts, sub-accounts, or platform access to another. By operating through accounts opened at regulated onshore VASPs, oVASPs can remain partially or fully obscured from the host supervisor. These arrangements weaken visibility over the identity, risk profile, and transaction activity of the underlying customers and can delay detection of illicit activity. Regulated onshore VASPs may face challenges in meeting their AML/CFT/CPF obligations where nested arrangements limit their visibility over the oVASP's underlying customers and transactions.

15 TRM Labs "Understanding Parasite Exchanges: Backdoors of Illicit Finance in Crypto" August 2023.

or services at onshore VASP. In other cases, onshore VASPs report difficulties obtaining sufficient transaction-level information, testing results, or audit trails from oVASPs, limiting the onshore VASP's ability to monitor transactions. In such cases, nested oVASPs may process illicit transactions that are significantly higher than those of a host VASP's typical retail customers, while accounting for only a small share of total transaction volumes. Industry representatives further note that these risks are more likely to arise in nested relationships where the host VASP has weak AML/CFT/CPF controls. Failures by host VASPs to identify and control nested activity constitute a significant vulnerability. Alternatively, as demonstrated by the Binance case below,[16] oVASPs may provide nested services to additional VASPs, amplifying the risks that an oVASP that fails to comply with regulatory obligations can pose to countries in which they provide products and services.

33. Offshore VASPs may provide nested services to additional VASPs, attracting users with instant execution, anonymity, low fees, or broad asset coverage, regulatory and reputational risks are borne by the host VASP. As demonstrated by the Binance case below, risk of failure to comply with regulatory obligations can be amplified for the host VASP, including exposure to sanctioned actors, enforcement action, and supervisory sanctions where nested activity is not adequately identified or controlled. [17]

Box 4. Examples of misuse of nested relationships

Estonia

FIU Estonia identified a case in which an offshore, unlicensed VASP gained access to services from an Estonian-licensed VASP by posing as a private individual customer. The Estonian VASP, which later lost its license, onboarded several clients as natural persons and treated them as retail users.

However, the activity on these accounts indicated automated, commercial trading and did not amount to the behaviour of retail users. Indicators included very high transaction frequency, a mix of small and large trades, repetitive timing patterns, and counterparties consistent with algorithmic trading. The email domains used by the "individuals" also contained the name of an API-based trading platform. FIU Estonia later confirmed that the automated trading provider was not licensed as a VASP in any jurisdiction.

United States – nested exchanges[18]

After launching in 2017, Binance quickly became the largest VASP in the world, with the greatest share of its customers coming from the United States. As a result of operating wholly or in substantial part in the United States, Binance was

[16] OFAC – Binance settlement case.

[17] Jurisdictions should apply Recommendation 13 to VASP–VASP relationships and require host VASPs to identify nested activity, assess the risk of the underlying entity, and conduct risk-based due diligence. Higher-risk scenarios include:

a. nested VASPs operating from jurisdictions with weak or no AML/CFT/CPF regulation;

b. arrangements that obscure underlying customers and the nature of their transactions; and

c. high-volume flows or the processing of third-party payments.

[18] OFAC – Binance settlement case.

required to register with FinCEN as a money services business (MSB) and to establish, implement and maintain an effective AML program.

An important source of Binance's growth has been its recruitment and retention of large trading firms, allowing their clients direct access the Binance.com platform through subaccounts created by the broker under its own Binance.com account. However, Binance initially failed to implement adequate policies, procedures, and internal controls around these customer-opened subaccounts to ensure that the Binance.com platform was not exploited by illicit actors.

These subaccounts contributed to the establishment of so-called "nested exchanges" operating within Binance without sufficient oversight and due diligence. In particular, two exchanges that were designated by OFAC, Suex and Garantex, operated as nested exchanges at Binance. Additionally, BestMixer, a mixer that conducted illicit activity, utilized multiple unique accounts on the Binance platform and conducted thousands of transactions between 1.9 and 2 bitcoin—just below, or at, the limit of Binance's "No-KYC" policy. In connection with its resolution with FinCEN, Binance agreed to cease the practice of opening anonymous sub-accounts and allowing them to transact on or through Binance.com.

Regulatory arbitrage creating AML/CFT/CPF vulnerabilities

34. OVASPs may relocate, incorporate, or route customer activity through jurisdictions with weak regulatory and supervisory controls in attempts to avoid or minimise regulatory requirements, including AML/CFT/CPF obligations. This regulatory arbitrage creates structural vulnerabilities that allow such VASPs to continue servicing users while remaining outside effective supervision.

35. In practice, VASPs engaging in regulatory arbitrage often fail to comply with core AML/CFT/CPF obligations, including customer due diligence and Travel Rule requirements. Some actively market minimal information requirements or encourage the use of VPNs. These practices can increase exposure to risks, distort competition by converting lower compliance costs into pricing advantages, larger profits, and undermine the effectiveness of domestic regulatory frameworks

Case example – regulatory arbitrage

In 2022, India introduced a dedicated VA tax regime on income from VA transfers as well as a 1% tax for VA transfers to be deducted at source. The deducting at source lies with the person making the payment, or typically the crypto exchange in transactions occurring on an Indian platform.

Independent analyses from the obliged entities indicate that after the introduction of direct taxation and withholding tax provisions a significant proportion of trading traffic moved from Indian Onshore VASPs to various offshore unregistered VASPs. As a consequence, a number of Indian clients have moved from a regulated entity to offshore platforms that are not subject to Indian AML/CFT/CPF rules.

By remaining offshore, these offshore entities fail to comply with AML/CFT/CPF and other requirements (including KYC and Travel Rule obligations, and Indian tax laws). These entities aggressively market their minimal customer information requirements and may encourage the use of VPNs or shell companies to circumvent domestic regulations. This deliberate non-compliance enables them to transform lower compliance costs into attractive pricing.

Source: India

Use of oVASPs in complex ML/TF/PF schemes

36. As a result of these characteristics and vulnerabilities, oVASPs can be misused to facilitate large-scale fraud, money laundering, and proliferation-financing schemes. Common typologies include dispersing victim funds across multiple addresses, routing transactions through layered intermediary wallets, and using multiple blockchains or bridges to increase obfuscation.

37. Experience shared at the April 2025 VACG highlighted sophisticated exploitation of oVASPs by threat actors, including the Bybit theft. Participants noted the DPRK's use of Bybit as an unregistered oVASPs, as well as OTC traders (also known as cash desks), mixers, bridges, and extensive wallet fragmentation, significantly increasing investigative complexity and time sensitivity.

Box 5. oVASPs in complex ML/TF/PF schemes

India – Offshore VASPs and scam compounds

The Indian FIU analysed illicit activity related to a financial conglomerate in a third country. Illicit actors relied on oVASPs providing services in high-risk jurisdictions with weak or non-existent KYC/AML controls. The typical flow involved: (i) converting illicit proceeds from scam compounds into VAs through unregulated or lightly regulated oVASPs; (ii) transferring these VAs to a registered Indian VASPs; and (iii) off-ramping into fiat through domestic accounts.

Registered Indian VASPs detected unusual deposit patterns from these offshore wallets, exposure to high-risk jurisdictions, and a lack of legitimate economic purpose. Following the identification of these red flags, they filed multiple Suspicious Activity Reports (STRs) with India's FIU.

FIU analysis exposed a parallel underground remittance corridor used to move funds through oVASPs, enabling targeted enforcement action and disruption of the channel.

Nigeria – Facilitation of a large-scale fraud scheme

The Nigerian FIU (NFIU) analysed a high-profile investment fraud Scheme, identifying how oVASPs and opaque corporate structures were used to facilitate large-scale fraud, cross-border movement of illicit proceeds, and financial obfuscation. The scheme generated unique wallet addresses for each victim, preventing competent authorities from clustering transactions or identifying common exposure. Victim funds were channelled through multiple intermediary "funnel addresses," creating a complex transaction network on the TRON blockchain.

The analysis further showed that offshore centralised exchanges were used as final cash-out points, including major global VASPs, all providing services from outside Nigeria. These exchanges provided exit ramps for illicit proceeds, additional layers of anonymity, and entities outside of Nigeria's regulatory reach. One global VASP-linked wallet held approximately USD 600 million at the time of analysis.

The NFIU disseminated its findings to law-enforcement agencies for investigation.

38. OVASPs have also been identified as facilitating TF, particularly through low-value, cross-border virtual asset transactions, online fundraising, and the use of platforms operating outside effective supervision. Unlike some ML typologies, TF-related activity often involves smaller transaction values, rapid movement of funds, and reliance on anonymity or jurisdictional opacity rather than large-scale cash-out. OVASPs operating without effective AML/CFT/CPF controls can therefore provide accessible infrastructure for the collection, movement and storage of funds linked to terrorist actors or networks.

Box 6. Involvement of oVASPs in TF

Canada

A foreign VASP assessed as being at risk of terrorist financing abuse was identified through suspicious transaction reporting in Canada. Domestic STRs submitted to FINTRAC revealed that a Canada-based individual was conducting transactions with the foreign VASP in a manner that raised terrorist activity financing concerns. The VASP was reportedly located in a high-risk jurisdiction, within or in close proximity to an active conflict zone, and the specific city in which it operated was controlled by, or subject to significant influence from, a terrorist entity listed in Canada.

Following a law-enforcement investigation, the Canada-based individual was charged and convicted for fundraising on behalf of a terrorist group. FINTRAC's financial intelligence contributed to law-enforcement action that disrupted the exploitation of the foreign VASP for terrorist financing purposes.

Indonesia

PPATK (Indonesia's FIU) identified VA-based financial support to terrorist groups in Syria involving several foundations and individuals in Indonesia.[19] Following the arrest of two initial suspects, collection continued through a third account, from which funds were sent to nine foreign terrorist fighters (FTFs) in Syria, amounting to around USD 35 500, via Binance. Additionally, funds were transferred from a local-regulated VASP wallet to oVASPs, including KuCoin and CoinEx.

In this case, oVASPs were exploited for:

- anonymity through nominee accounts, falsified credentials and looser KYC processes;
- the ability to convert between different types of VAs, including altcoins and DeFi tokens;
- the ability to conduct rapid layering by converting between different types of Vas, including altcoins and DeFi tokens; and serving as an intermediary step before funds were moved to non-custodial wallets, mixers, or privacy coins.

Jurisdictional obstacles to supervision and enforcement

39. Supervisory and enforcement action against oVASPs can be constrained by jurisdictional and legal limitations. As noted above, oVASPs may structure operations, customer accounts, and record-keeping across multiple jurisdictions, including jurisdictions with weak or non-existent AML/CFT/CPF frameworks. Supervisors have also reported cases where overseas entities enter a market by acquiring a pre-existing, licensed or registered VASP, thereby gaining access without having been subject to the

[19] See public court decisions 1 and 2 (Indonesia).

original registration process.[20] In some cases, these onshore VASPs, operating within global groups, may fail to tailor their AML/CFT/CPF programmes and risk assessments to local requirements. These strategies can limit authorities' ability to, amongst others, assert jurisdiction, ensure compliance with local rules or compel records for rapid co-operation.

40. Cross-border enforcement is further hindered where oVASPs rely on internal group arrangements to determine which entity is responsible for holding customer records or responding to information requests from foreign supervisors or law enforcement agencies. In practice, when competent authorities in a jurisdiction where customers are located request information from an oVASP, the VASP may respond that it is not licensed or registered in that jurisdiction and redirect the authority to another jurisdiction (e.g., the jurisdiction of incorporation or a group-level service entity). This may occur even where the oVASP is actively providing services to customers in the requesting jurisdiction. As a result, authorities may need to pursue multiple, sequential co-operation requests across different jurisdictions, which exacerbates delays inherent in mutual legal assistance and other co-operation mechanisms. Requests for information linked to oVASP activity may therefore take months, or even up to a year in some reported cases, particularly where competent authorities have limited visibility over group structures or cannot easily identify the entity controlling the relevant information. These constraints may be further compounded where offshore VASPs integrate or rely on privacy-enhancing technologies, mixers, bridges, or DeFi protocols as part of their service offering, which can fragment transaction records and obscure where relevant data and operational control are located.

41. Law-enforcement agencies have reported cases where oVASPs rely on formalistic or opaque attribution of customer accounts, or delegation of operational responsibilities to different jurisdictions to limit co-operation, even where there are strong operational links to the requesting jurisdiction. This can result in fragmented information-sharing, delayed access to records, reliance on slow informal co-operation or the need to submit mutual legal assistance requests, significantly undermining timely asset tracing and investigations. Weak or fragmented regulatory and supervisory frameworks may further impede timely informal co-operation. This includes delays or obstacles in information exchange between FIUs, co-operation between supervisors, and diagonal co-operation involving FIUs, supervisors, and law-enforcement authorities, particularly where the competent authority or supervisory responsibility is unclear. As a result, authorities may need to rely more heavily on slower formal co-operation channels.

[20] These risks may be heightened in jurisdictions with significant number of dormant or inactive entities, which can be acquired and reactivated.

Case study - Law-enforcement access challenges in oVASP cases

During an investigation, German law-enforcement agencies determined that a German national had sold narcotics and invested the proceeds in VAs. The VAs were managed by his wife. Initially, the location of the VAs could not be identified.

Analysis of electronic evidence later showed that VAs worth approximately EUR 800,000 had been transferred from an oVASP. The oVASP informed German authorities that the account was attributed to a jurisdiction in South-Eastern Europe and that obtaining further information would require legal assistance via a foreign jurisdiction. In a related request concerning an account held by the defendant's brother, the VASP stated that legal assistance from another European jurisdiction was required.

Only after a subsequent request by the German FIU, it was clarified that the assets originated from an account held by the defendant's mother, opened using identity documents from a neighbouring European jurisdiction but accessed exclusively from German IP addresses. The assets were then transferred to an account held by the defendant's brother, which was registered and predominantly accessed from Germany.

A German court issued a seizure order that was sent to the oVASP for execution. Only after extensive correspondence and several follow-up inquiries were the VA assets transferred to the authorities' own addresses about 4 months later.

Source: Germany

The Sunrise issue

42. Supervisory challenges are further compounded by systemic vulnerabilities arising from uneven and delayed implementation of cross-border transparency measures, most notably the Travel Rule. As of 2025, while a growing number of jurisdictions have enacted Travel Rule legislation, implementation timelines and operational practices remain fragmented across jurisdictions, a phenomenon commonly referred to as the "Sunrise Issue."

43. Where oVASPs operate from jurisdictions that have not yet implemented the Travel Rule, competent authorities may lack a legal basis to request or exchange originator and beneficiary information for cross-border VA transfers. This implementation gap creates monitoring blind spots and increases ML/TF/PF risk by constraining the ability of both VASPs and authorities to apply effective, risk-based mitigation measures.

Case study – Impact of the Sunrise issue on cross-border investigations

During a law enforcement-led investigation of a large fraud case, the Nigerian FIU and partner agencies faced significant issues with illicit funds moving into oVASPS located in jurisdictions that have not fully applied FATF's Travel Rule (R.16) yet.

After identifying the movement of proceeds into deposit wallet addresses at several global VASPs, investigators could not obtain originator and beneficiary information due to its absence from the relevant transaction data and the lack of responses to information requests submitted to the relevant foreign VASPs and FIUs.

Source: Nigeria

3. Good Practices

44. This section explores good practices to mitigate the main risks identified in the previous sections. It covers detection and identification of oVASPs, licensing/registration and supervision/oversight, enforcement of measures supported by domestic and international co-operation.

3.1. Identifying oVASPs

45. Jurisdictions should take steps to identify natural or legal persons carrying out covered VA activities or operations without the required licence or registration, including oVASPs providing services into their jurisdiction. This obligation applies regardless of whether a jurisdiction permits, regulates, or prohibits VA activities, in line with Recommendation 15.

46. In practice, identifying oVASPs can be challenging due to the lack of physical presence, reliance on digital delivery channels, and business models designed to obscure jurisdictional attribution. As a result, jurisdictions have reported relying on a combination of indicators, information from obliged entities (e.g., domestic VASPs and FIs), and investigative tools to identify oVASPs providing services in their market.

Potential red flags

47. VASPs may claim they are not incorporated or physically present in the relevant jurisdiction; even if they actively promote their platforms, onboard residents and enable transactions leveraging domestic payment rails When seeking to identify offshore VASP activity, including in situations relevant to paragraph 48, competent authorities have noted a range of indicators suggesting intentional targeting of a jurisdiction, as well as the following red flags:

a) The absence of geo-blocking in the VASP's platform;

b) Platform content encouraging participating in a jurisdiction (e.g., using local language or currencies);

c) Application availability in app stores popular in a market, including reviews from users in said jurisdiction evidencing an active user base;

d) Offering the possibility of on-ramp or off-ramp through domestic methods of payment;

e) Provision of video tutorials on how to trade VAs in a market;

f) Marketing tactics leveraging local influencers and/or opinion leaders through social media platforms;

g) Sponsoring of local events; and

h) Surrogate marketing for expanded reach.

Potential detection tools

48. In order to identify persons operating without a license and/or registration, jurisdictions can leverage these red flags alongside a range of complementary tools and information sources. Depending on domestic frameworks and capacity, these may include:

a) Distributed ledger or blockchain analytics tools, as well as other investigative tools or capabilities;

b) web-scraping and open-source information to identify any advertising, promotional communications (including sponsorship of local events) or affiliation programs or other possible solicitations for business by an unregistered or unlicensed entity;

c) information from the general public, obliged entities (e.g., onshore VASPs) and industry circles (including by establishing channels for receiving public feedback) regarding the presence of certain businesses that may be unlicensed or unregistered;

d) FIU or other information from reporting institutions, such as STRs, investigative leads, or data from central bank account registers, that may reveal the presence of an unlicensed or unregistered natural or legal person VASP;

e) non-publicly available information, such as whether the entity previously applied for a license or registration or had its license or registration withdrawn; and

f) law enforcement and intelligence reports, including information from international co-operation (e.g., tips from international counterparts).

49. Jurisdictions have noted that blockchain analytics tools can be useful for tracing specific transaction flows and supporting law enforcement investigations but are generally insufficient on a standalone basis to identify oVASP activity. Supervisors reported that such tools are most effective when used in combination with open-source intelligence, STRs, and structured engagement with local obliged entities.

Box 7. Building a diverse detection toolkit

India – leveraging STRs from onshore VASPs

FIU India conducted an Operational Analysis following an STR from an onshore Indian VASP's identification of an offshore, unregistered VASP. Said entity appeared to be operating under the guise of an online gambling platform. The platform, based in the Caribbean, was offering unlicensed on-ramp and off-ramp services (VA–fiat and fiat–VA) to Indian residents.

Indian users received VA transfers from the platform and off ramped the proceeds into domestic bank accounts. The pattern of demographically and geographically anomalous transactions indicated the oVASPs was deliberate masking of its activity and leveraging AML/CFT/CPF blind spots to move value across borders.

Access to the platform was blocked in India.

Australia[21] - diverse detection toolkit

Australia's AUSTRAC conducts environmental scanning and monitors for media and social media posts to detect presence of oVASPs offering services locally. Where concerns arise about an oVASP, AUSTRAC uses blockchain analytics, company registers and open-source tools.

Nigeria

Use of blockchain analytics

In a recent market manipulation case linked to a Pyramid Scheme, on-chain analysis enabled the NFIU to trace funds from Nigerian victims through several exchanges before landing at an oVASP. Blockchain analytics allowed the clustering of multiple wallets used by the same operator. Identified patterns also highlighted the use of "peel chains" and micro-transactions, signaling cash-out activity in foreign jurisdictions. This became the basis for a cross-border request for information. The Case/Investigation is ongoing.

Online marketing monitoring

The Nigerian SEC Monitoring is carried out through a structured sweep of online channels, including influencers' pages, sponsored social-media content, Telegram/WhatsApp broadcast groups, and digital-investment forums.

Singapore

For VASPs that are incorporated in Singapore but provide VA services outside of Singapore, the Monetary Authority of Singapore (MAS) has worked with a blockchain analytics service provider to conduct a surveillance scan to detect any entities which could potentially fall within scope of the VASP licensing regime to proactively engage them.

50. Given the resource demands of identifying and supervising offshore VASPs, supervisors should aim to ensure relevant teams have sufficient capacity and expertise

to perform their duties. This could include investing in analytical tools or leveraging existing ones.

Nested and intermediary relationships

51. Nested and intermediary VASP relationships can be an enabler of oVASP activity, allowing unlicensed or unregistered entities to access trading, liquidity, custody, or fiat on- and off-ramps through regulated VASPs or FIs. VASPs providing such services therefore play a key gatekeeping role in mitigating the ML/TF risks. For AML/CFT/CPF purposes, these nested arrangements may give rise to risks similar to those associated with cross-border correspondent relationships. Recommendation 13 provides a relevant framework for applying risk-based controls to these relationships.

Box 8. Application of Recommendation 13 to nested VASP relationships[22]

Jurisdictions should require VASPs providing services to another VASP or FI as part of a nested relationship to:

gather sufficient information about the other VASP or FI with which it proposes to establish a nested relationship, to understand fully the nature of the other VASP or FI's business and its AML/CFT/CPF risk control framework, including: what types of customers the other VASP or FI intends to provide services to through the cross-border correspondent relationship;

a) gather sufficient information and determine from publicly available sources the reputation of the other VASP or FI, the quality of supervision it is subject to and whether it has been subject to an ML/TF investigation or regulatory action;
b) assess the other VASP's or FI's AML/CFT/CPF controls;
c) obtain approval from senior management before establishing new cross-border correspondent relationships; and
d) with respect to accounts or custodial wallets able to be used directly by customers of the other VASP or FI to transact business on the customer's own behalf, be satisfied that the other VASP or FI has conducted CDD on such customers and is able to provide relevant CDD information on request, to the extent permitted privacy and data protection regulations in both jurisdictions.

Risk understanding - Use of thematic reviews

52. Supervisors may use thematic reviews to develop a jurisdiction-wide understanding of exposure to oVASPs and to assess how effectively identified risks are being mitigated by domestic VASPs and other FIs. This can support jurisdictions' broader obligation to identify, assess and understand ML/TF risks, including cross-border VA activity and risks arising from oVASP business models.

[21] Australian law does not prohibit foreign VASPs from providing services to Australians. However, any VASP that seeks registration with AUSTRAC must have a geographic link to Australia, i.e. it must have permanent establishment in Australia (Australian residents and subsidiaries of Australian VASPs operating offshore also meet the geographic link test and must also register).

[22] Please see the 2021 updated VASP guidance for further detail (paragraphs 164 to 169).

53. In practice, thematic reviews can draw on a combination of supervisory data, STRs, market intelligence, blockchain analytics, and information obtained through engagement with domestic VASPs, and FIs. These reviews can be used to:

    a) estimate oVASP exposure;

    b) identify common access points used by oVASPs (e.g. nested accounts, payment rails, intermediaries); and

    c) assess whether domestic VASPs and FIs apply adequate AML/CFT/CPF controls measures.

54. Thematic reviews may be conducted on a desk-based basis or may include direct outreach to identified oVASPs, where feasible, to clarify the nature and extent of their activities in the jurisdiction. Such outreach may include communicating the supervisor's view of potentially applicable obligations under the domestic framework and requesting information needed to assess nexus and risk (e.g., place of management, customer base, marketing/solicitation, and use of domestic intermediaries). This process can also assist supervisors in identifying relevant foreign counterparts and establishing or strengthening international co-operation channels.

55. Where risk assessments identify risks affecting other jurisdictions (e.g., a local VASP providing unregistered/unlicensed VASP services in a third country), home supervisors should consider proactively reaching out to the relevant foreign counterparts. Such information-sharing can support host jurisdictions' risk assessments and supervisory frameworks.

Case study – use of thematic reviews

In 2025, New Zealand carried out a thematic review of the jurisdiction's exposure to oVASPs. The exercise leveraged intelligence to identify 20 oVASPs providing services to New Zealand residents, including through suspicious transaction reports submitted by NZ FIs.

The NZ supervisor, DIA, reached out to all 20 oVASPs to seek clarification from them of their potential AML/CFT/CPF obligations under New Zealand's framework. The request sought to seek clarification from the entities on:

- whether they physically operate in NZ;
- where their center of management is located;
- if they provide any other captured services to NZ customers;
- whether they have any NZ based staff or infrastructure (e.g., a local bank account);
- whether they carried out any active or direct advertising or soliciting of business from persons in NZ.

Of the VASPs that responded, 12 out of 20 disputed that New Zealand's AML/CFT/CPF rules applied, citing the absence of any physical presence or place of business in the jurisdiction.

Source: New Zealand

56. As part of their risk-based supervision, home supervisors can conduct thematic or horizontal reviews to assess the extent to which VASPs under their supervision provide services cross-border, including into jurisdictions where the VASP has no physical presence, and to identify whether group structures, customer allocation models or outsourcing arrangements create AML/CFT/CPF vulnerabilities.

3.2. Imposing licensing and/or registration requirements on oVASPs

57. Jurisdictions may use the flexibility under INR.15.3 to require oVASPs that actively provide services into their market to be licensed or registered domestically, regardless of where the VASP is incorporated or physically located. This activity-based approach can mitigate against oVASPs accessing users in a jurisdiction without AML/CFT/CPF controls.

58. Where jurisdictions apply such requirements, clarity on territorial scope is important. Authorities should aim to clearly articulate what constitutes the active provision of VASP services into the jurisdiction, in order to support enforceability and provide legal certainty. Relevant indicators may include, inter alia:

    a) targeted or localised marketing or promotion;

    b) use of local language

    c) conducting substantial business in the jurisdiction;

    d) onboarding or servicing of residents;

    e) use of domestic payment rails; and

    f) maintenance of local infrastructure (e.g., bank accounts).

59. Respondents to the 2025 annual survey, shared that jurisdictions operationalise "active provision of VASPs services" in different ways. These included:

    a) some apply a conduct-based test linked to "doing business" or "directing services" into the market (e.g., requirements triggered by targeted marketing, solicitation, or provision of services to residents);

    b) some specify concrete nexus indicators such as maintaining local infrastructure or distribution networks (e.g., local bank accounts, offices/servers, or in-jurisdiction arrangements that enable local services); and

    c) some incorporate quantitative or client-based thresholds (e.g., business-volume thresholds, or requirements linked to whether services are offered to retail investors).

Box 9. National approaches to defining 'active provision of VASP services'

Hong Kong, China

In Hong Kong, China (HKC), a person is regarded as carrying out a business of providing a VA service if such person actively markets to the public any services or a function that he provides or purports to provide, if done in HKC, would constitute providing a VA service or performing a regulated function in relation to the

provision of a VA service as defined under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) (AMLO); and no person may actively market, whether in HKC or from a place outside HKC, to the public of HKC any services which would constitute a VA service if provided in HKC, unless that person is licensed by HKC's Securities and Futures Commission (SFC).

The SFC further clarifies in its Frequently Asked Questions (FAQ) by giving examples that 'actively markets' may include those who frequently call on HKC investors and market their services, run mass media programmes targeting at the investing public in HKC, or conduct Internet activities that target HKC investors. The FAQ has also set out factors that the SFC would consider to determine whether or not a person is actively marketing its services to the public. Examples of such factors include the marketing means adopted by the person, the language and the currency used in the marketing materials.

European Commission

For the purposes of determining what constitutes the active provision of VASP services into the European Union, the EU's Markets in Crypto-Assets Regulation (MiCA) provides relevant reference points. Under MiCA:

- applies to any natural or legal persons that are engaged in the issuance, offer to the public, or admission to trading of crypto-assets (VAs), or that provide crypto-asset services in the Union (Article 2 (1)); and
- Offer to the public is defined as "a communication to persons in any form, and by any means, presenting sufficient information on the terms of the offer and the crypto-assets to be offered so as to enable prospective holders to decide whether to purchase those crypto-assets" (Article 3(1)(12)).[23]

Under MiCA, CASPs/VASPs may not provide crypto-asset services within the Union unless they are established and authorised in a Member State (Article 59 for CASPs/VASPs or Article 60 for credit institutions). An exemption applies in cases of reverse solicitation, where "a client established or situated in the Union initiates, at its own exclusive initiative, the provision of a crypto-asset service or activity by a third-country firm" (Article 61), provided that the service is not preceded by an offer to the public or other forms of solicitation in the Union.

Argentina

Argentina's framework establishes explicit criteria to determine when a foreign VASP is considered to be actively providing services in the Argentine market and therefore subject to registration requirements. Under CNV General Resolution No. 1058/2025, this includes cases where a foreign VASP:

- uses an ".ar" domain to provide services;
- has commercial arrangements (including with affiliates or third parties) that enable the receipt of funds from Argentine residents, including through on- or off-ramp services;

[23] Additional background on means of solicitation under MiCA can be found in section 5 the ESMA guidelines solicitation under the MiCA (2025).

- clearly targets or directs services to residents of Argentina, including through advertising;
- derives more than 20% of its global turnover from activities involving Argentine residents.

Any one of these criteria is sufficient to consider a foreign VASP as actively providing services into the Argentine market and to trigger applicable registration obligations. The framework explicitly excludes cases of reverse solicitation, where the client initiates the relationship without targeted outreach by the foreign provider.

Singapore

Singapore imposes licensing requirements on (i) VASPs that carry on a business of providing VA services in Singapore and (ii) VASPs that are incorporated in Singapore but provide VASP services outside of Singapore.

On (i), VASPs that carry on a business of providing VA services in Singapore are required to obtain a licence to operate. When determining licensing applicability, Singapore considers whether the services are provided with system, continuity, and repetition, and the points of nexus to Singapore. VASPs soliciting for VA business from the Singapore public, regardless of whether the solicitation is done from Singapore or elsewhere, would also be caught for licensing.

On the latter, Singapore is of the view that such VASPs have limited nexus to Singapore (as they provide VA services solely outside Singapore) and carry higher risks of being engaged in or be misused for illicit purposes.

In light of these risks, MAS adopts a prudent licensing approach and there would be extremely limited circumstances under which MAS will grant a license under the Financial Services and Markets Act. In assessing applications, MAS considers factors such as:

a) whether the business model is economically sound and justifies incorporation in Singapore without serving the domestic market;
b) whether the VASP is already subject to effective regulation and supervision in its overseas operating jurisdictions in line with international standards (including those of the FATF, FSB, and IOSCO); and
c) any other criteria that may be relevant to the application (or VASP) as determined by MAS.

South Africa

Financial Intelligence Centre (FIC) Act (Act 38 of 2001)

All VASPs (CASPs in South Africa) undertaking operations in South Africa or providing services into South Africa, in one or more of the five (5) business activities or operations listed in the FATF Glossary:

- must register with the FIC as designated accountable institutions under item 22 of Schedule 1 to the FIC Act; and
- as accountable institutions, registered VASPs are under FIC supervision and must comply with all AML/CFT/CPF obligations set out in the FIC Act.

Financial Advisory and Intermediary Services (FAIS) Act

In addition, the FAIS Act (Act 37 of 2002), administered by the Financial Sector Conduct Authority (FSCA), requires VASPs to be licensed with the FSCA where they undertake financial advisory or financial intermediary services in respect of crypto assets. As a financial services provider, VASPs are also supervised by the FSCA for AML/CTF/CPF compliance.

The FAIS Act licensing and FIC Act Registration requirements applies to both domestic and foreign-established VASPs providing such services into South Africa, including where:

- VASPs are not domiciled in South Africa but wish to do business in the country;
- VASPs must demonstrate compliance with applicable FSCA fit and proper requirements;
- VASPs may not market or promote financial advisory or intermediary services in South Africa without a FAIS Act licence; and
- the FSCA publishes and maintains a public list of licensed VASPs on its website.

VASPs that are created in South Africa but do not operate in South Africa do not fall under the FAIS Act but remain designated as accountable institutions under the FIC Act and under FIC supervision. This ensures there is no gap in South Africa's AML/CFT/CPF oversight of VASPS.

Ensuring sufficient physical presence in-jurisdiction

60. Jurisdictions requiring registration/licensing of oVASPs providing services in their jurisdictions have considered how to ensure a sufficiently material presence. To do so, competent authorities may set clear expectations on the type of presence required in jurisdiction, such as for VASPs to:

    a) establish legal entity in the jurisdiction and designate an AML/CFT/CPF compliance officer (or equivalent senior function) who is based in-jurisdiction, has unrestricted access to customer information and internal systems, and holds sufficient authority to act independently. These requirements help ensure that the compliance function is not nominal in nature and that authorities can engage meaningfully.

    b) maintain adequate resourcing for monitoring and reporting, and regular reporting on AML/CFT/CPF matters to the VASP's senior management. The Board should support oversight, including through the appointment of a dedicated director, particularly where ownership structures are complex or span multiple jurisdictions.

61. Authorities may verify compliance with these requirements prior to registration or licensing, including interviews with designated individuals and assessments of their effective authority, access, and independence.

Box 10. Reinforcing physical presence requirements

India

FIU India reinforced its requirements for Principal Officers (POs) to improve enforceability and accountability. The guidelines require the PO to be based in India, have unrestricted access to CDD/KYC information, internal systems and personnel, hold sufficient seniority to take independent decisions, and work exclusively for the VASP in a full-time AML/CFT/CPF capacity, with separate individuals serving as PO and Designated Director.

FIU India verifies these conditions through interview-based due diligence of both the PO and Designated Director before granting registration.

Japan

Japan does not have a concept of "regulated OVASP." As per Japan's Payment Services Act, all VASPs providing VA services to Japanese residents are required to register with Japanese Financial Services Agency.

When applying for registration, applicants are legally required to provide the address of a business office in Japan responsible for handling user complaints and inquiries, and VASPs must maintain a physical presence in Japan as a substantive licensing requirement.

Singapore

Singapore imposes the following requirements, both at the licencing stage and on an ongoing basis, to ensure that licensed VASPs have a minimum level of physical presence in Singapore:

a) Entity type: The VASP entity must either be a Singapore-incorporated company or a Singapore-registered branch of a foreign company.

b) Director requirements: The VASP's executive director (ED)[24] must be resident in Singapore as either a citizen, permanent resident, or employment pass holder. Where the ED is an employment pass holder, the applicant must have at least one other director who is a citizen or permanent resident.

c) Compliance arrangement: The VASP must have a Singapore-based compliance officer.

d) Physical office: Licensees must maintain a physical place of business in Singapore that is accessible by the public.

[24] The ED is defined as a person who is responsible for the day-to-day management of the VASP.

Supervisory engagement

62. Once oVASPs are identified as potentially providing services into the jurisdiction, supervisors may adopt a graduated, risk-based approach to engagement. Early supervisory engagement can help clarify territorial scope, assess the nature and scale of activities, and promote voluntary compliance. Such engagement may include:

    a) formally communicating applicable registration or licensing obligations and territorial-scope rules;

    b) requesting information to understand business models, customer exposure and use of domestic infrastructure;

    c) where appropriate, directing entities to comply with domestic requirements or to cease servicing customers in the jurisdiction; and

    d) liaising with the foreign supervisor in the jurisdiction where the oVASP is incorporated and/or located; and, where relevant, extending such engagement to supervisors in other jurisdictions where the oVASP is actively providing services.

Box 11. Approaches to imposing supervision

New Zealand – engaging identified oVASPs

Following the initial engagement with the identified oVASP population, New Zealand's supervisor (DIA) is structuring a risk-based engagement:

- Lower-risk tranche – A one-to-many approach is being considered. This would involve formal communication to oVASPs, referencing New Zealand's published territorial-scope requirements, to clarify that any entity meeting these criteria will be captured under the NZ AML/CFT/CPF regime.
- Higher-risk tranche – Targeted one-to-one supervisory engagement is being considered for entities where intelligence contradicts the views or responses provided by the oVASPs, indicating that their activities may fall within NZ's regulatory scope.

India

Engaging identified oVASPs

When a VASP raises multiple red flags FIU-India initiates supervisory actions and directs the entities to comply or cease operations. Notices are issued to these entities under the relevant AML/CFT/CPF regulations (MLA, 2002) directing the entity to explain its failure to register and discharge reporting obligations.

Developing indigenous detection capabilities

Efforts are underway to create an indigenous Virtual Asset Lab to enable continuous detection of unregistered, high-risk platforms using analytics, OSINT and automated web surveillance tools.

Gatekeeping access to the market

63. While supervisory engagement can improve transparency and support voluntary compliance, experience shows that some offshore VASPs remain unresponsive, dispute territorial scope, or continue operating without authorisation. In such cases, jurisdictions have complemented engagement with gatekeeping measures that restrict access to the domestic market by targeting key intermediaries and access points on which offshore VASPs rely to promote services, onboard customers, or operate. These measures typically involve obligations or expectations placed on domestic FIs, internet service providers, app stores, or advertising platforms to identify and restrict relationships with unlicensed offshore VASPs.

Box 12. Approaches to imposing supervision

United Kingdom – Preventing unregistered OVASPs from Servicing UK Consumers

The 2020 UK's AML regime for VASPs requires any firm providing crypto asset services by way of business in the UK to be registered with the Financial Conduct Authority (FCA). In October 2023, the UK extended existing financial promotion rules to qualifying crypto assets. As a result, no oVASP may promote services to UK consumers unless registered with the FCA or having their promotion approved by an authorised approver. The FCA has clarified that the rules apply even where a promotion originates outside the UK but is capable of having an effect in the UK.[25]

Failure to comply is an offence under section 21 of the Financial Services and Markets Act 2000.

To support effective implementation, the FCA:[26]

- warned firms promoting crypto assets to UK consumers that they must prepare for the regime, using website statements, letters to firms and industry engagements;
- assessed readiness, noting poor engagement from many unregistered oVASPs with UK customers (only 24 of 150 firms responded to an FCA survey);
- communicated expectations to VASPs and FIs (banks, payment institutions), including:
  - carefully considering the risks they could be exposed to as a result of partnering with unregistered firms illegally promoting to UK consumers; and
  - implementing controls to stop UK consumers accessing unlawful promotions, including proactive due diligence on partners and steps

[25] As per the November 2024 FCA guidance, *"Financial promotions do not need to be expressly targeted towards UK consumers to be capable of having an effect in the UK and subject to the financial promotion regime. For example, if UK consumers can view the promotion and potentially engage in the investment activity that is being promoted, the communication is likely to be capable of having an effect in the UK."*

[26] FCA, "Final warning for cryptoasset firms marketing to UK consumers and those supporting them to get ready for the financial promotion regime" September 2023.

to prevent UK customers from engaging with services promoted from unregistered oVASPs.

- reminded firms that benefits obtained from illegal financial promotions may constitute criminal property, exposing intermediaries to ML offences.

Nigeria - Transition from prohibition to regulation, regulating oVASPs

Between 2021 and 2023, Nigeria operated under a de facto prohibition model for banking interactions with VASPs. While this suppressed regulated activity, it inadvertently pushed users toward offshore platforms. With the introduction of the Investment and Securities Act (ISA) in 2025, the Nigeria Securities Exchange Commission (SEC) was granted clear authority to:

- license VASPs
- enforce AML/CFT/CPF controls
- supervise promotions and marketing by oVASPs
- apply sanctions for non-compliance

In addition, the Nigerian SEC also clarified its approach to marketing and promotion rules, clarifying that any entities, local or offshore, marketing virtual assets to Nigerian residents would be required to obtain a license in the jurisdiction.[27]

Anticipating these reforms, many oVASPs intensified their marketing efforts, exploiting earlier regulatory gaps. The new ISA framework, combined with guidelines from the Central Bank of Nigeria on VASP-related bank accounts has allowed Nigeria to:

- verify any VASPs licensing status as part of their onboarding checks
- explicitly prevent local FIs from servicing unlicensed oVASPs
- generate data (e.g., STRs) to enrich the national VASP risk assessment

Global pooling of customers

64. In addressing risks associated with global pooling of customers (see paragraphs 27 to 28) some jurisdictions have used registration and licensing requirements to require that resident customers are serviced through a locally authorised entity aiming to ensure these activities remain within the national regulatory framework. In practice, this has involved requesting the end of servicing residents through global platforms, migrating resident accounts and wallets to a locally licensed entity, and setting clear conditions for the migration process, including renewed customer identification before access to the new local entity.

[27] The SEC's rulemaking detailed:

(i) the need for prior approval before any VA advertisement or endorsement; and

(ii) liability for promoters who market unregistered platforms.

Case study - managing Risks from Global Customer Pooling

The Japanese Financial Services Agency (JFSA) introduced targeted supervisory and enforcement measures to address customer protection concerns, alongside ML/TF risks arising from global customer pooling by an oVASP. These measures were taken in response to the unregistered provision of VASP services in Japan by a global VASP (Binance) and included:

- Mandatory local registration – Following JFSA a warning letter requesting to cease the unregistered provision of VASP services to Japanese residents, Binance acquired a locally registered VASP, rebranded it as Binance Japan, and provided services to Japanese customers exclusively through that entity.
- Segregation of Japanese customers – Binance was required to migrate all Japanese resident accounts and related personal data from its global platform to Binance Japan, ending the pooling of Japanese customers with global users outside Japanese regulatory oversight.
- Renewed KYC and compliance – Japanese residents were required to complete fresh identity verification to access services on Binance Japan.

Restrictions on the global platform – By 30 November 2023, Binance ceased offering trading services to Japanese residents on its global platform. Non-migrated users were restricted to withdrawals only.

Source: Japanese Financial Services Agency[28]

3.3. Enforcement and other actions to mitigate risks associated with oVASPs

65. Effective enforcement against oVASPs relies on actions taken by home jurisdictions. While host jurisdictions may apply market-access restrictions or disruption measures, effective risk mitigation requires that home jurisdictions use their supervisory and enforcement powers to address non-compliance by VASPs created or located in their jurisdiction, including where misconduct primarily affects foreign markets. Home jurisdictions therefore play a key role in enabling enforcement in oVASP cases.

66. Where gatekeeping and supervisory measures are insufficient, host jurisdictions may apply enforcement actions to address persistent or serious non-compliance by oVASPs. The FATF Recommendations require competent authorities to have access to a sufficient range of proportionate and dissuasive measures, from remedial actions to formal sanctions. Several jurisdictions sought to overcome enforcement challenges with market-access restrictions (e.g., denial of access to apps or URLs) with supervisory and LEA action.

67. In practice, effective responses to oVASPs often involve a combination of supervisory, administrative and enforcement tools applied in a graduated manner, including:

[28] For further detail, please see public statements 1, 2, 3 and 4.

a) public warnings or market alerts;
b) website, app-store or domain takedowns;
c) restrictions on access to domestic intermediaries;
d) remedial action plans with follow-up monitoring;
e) restricting access to the domestic market where deficiencies persist; and
f) financial penalties, civil action or criminal prosecution.

Box 13. Building an enforcement toolkit

Use of public lists

France

France's financial market supervisor (Autorité des marchés financiers, AMF) maintains a publicly available blacklist of entities and websites illegally offering services in France. This list is incorporated into IOSCO's i-scan tool and is used to warn customers, support reporting, and assist authorities in identifying potentially unauthorised activity.

The AMF also publishes a whitelist of VASPs authorised to offer services in France, including VASPs registered in France and those registered elsewhere in the EU that are permitted to passport their services. Supervisors and other stakeholders can cross-check this whitelist to detect VASPs operating in France without the required authorisation.

Singapore

MAS maintains two public lists:

a) VASPs that are licensed to provide VA services in Singapore; and
b) unlicensed local and foreign VASPs who, based on information received, may have been wrongly perceived as being licensed or authorised by MAS.

Members of the public are reminded to check these lists before engaging with a VASPs.

Japan – Addressing Risks from Unregistered VASPs – registration requirements and response measures

Any VASP providing services in Japan must be registered with the Japanese Financial Services Agency (JFSA), regardless of where it is located. The JFSA issues warning letters to unregistered OVASPs, directing them to cease providing services in Japan and to take any necessary corrective actions.

In cases where no corrective action is taken despite the issuance of warning letters, JFSA will file an accusation with the investigative authorities as necessary.

When measures such as warnings or accusations are taken, the JFSA will publish on its website the trade name, corporate or individual name, address or location of

the business operator, along with details of any VASPs conducted without registration.

Despite repeated warnings from the JFSA, some OVASPs continued their business or failed to submit corrective actions. The JFSA requested Apple Japan and Google Play Japan to remove those OVASPs' apps from their sites in early 2025.

United Kingdom – Disruption and access-restriction measures

Following the introduction of clear rules for oVASPs promoting services to UK residents and to address persistent non-compliance by oVASPs, the FCA has undertaken a series of enforcement and disruption measures, including:

- issuing 2,300+ alerts on illegal promotions;
- driving the takedown of 1,000+ scam websites;
- issuing 60+ app-removal requests to the Google and Apple app stores where illegal promotions were identified;
- commencing civil litigation against one oVASP for unlawfully promoting crypto asset services to UK consumers.

United States – sanctions and criminal enforcement

In November 2023, Binance Holdings Limited and its affiliates, which operate the world's largest VASP, Binance.com, entered into the largest resolution in the Treasury's history with FinCEN (including a penalty of $3.4 billion) and OFAC (including a penalty of nearly $1 billion), as well as resolutions of parallel investigations by the DOJ and the CFTC. As part of these resolutions, Binance pleaded guilty and paid penalties totalling over $4.3 billion, to resolve the Justice Department's investigation into violations related the BSA, failure to register as a money transmitting business, and the International Emergency Economic Powers Act.[29]

Ireland

The Central Bank of Ireland's Unauthorised Providers Unit (UPU) investigates entities that may be providing financial services in Ireland without the appropriate authorisation. The UPU receives reports of suspect unauthorised activity from a number of different sources including:

- complaints from members of the public;
- reports from internal supervisors;
- proactive searching;
- reports from regulators in other jurisdictions; and
- from Law Enforcement Agencies.

The UPU investigates those reports to assess whether an entity, include an oVASP/CASPs, is in fact providing services into the jurisdiction without a required authorisation and therefore is operating outside the regulatory perimeter. In appropriate cases, enforcement action will be taken and this most frequently involves the issuance of a warning notice to the public, warning about the unauthorised entity.

[29] Binance Holdings Limited

Separately, if the unauthorised entities have an online presence, the UPU will report any websites and associated advertisements to the relevant online platforms. Where possible, UPU relies on an accreditation as a Trusted Flagger under the EU Digital Services Act to ensure Online Platforms prioritise these requests.

68. Some jurisdictions have also established structured co-operation with internet service providers, app-store operators and online platforms to support rapid disruption of unauthorised oVASP activity.

Case study – channels for co-operation with social media and internet service providers

India's Ministry of Home Affairs has launched a dedicated portal (Sahyog portal) to foster co-operation between social media intermediaries and competent authorities. The portal automates and streamline sending takedown notices to IT intermediaries (i.e., social media platforms, web hosts, internal service providers) when content is deemed unlawful or being used to commit illegal acts. FIU India has leveraged this platform to direct intermediaries to take down website content. So far 85 URLs pertaining to unregistered non-compliant oVASPs have been taken down.

Source: India

3.4. Domestic coordination mechanisms

69. In line with Recommendation 2, jurisdictions should ensure effective national co-operation and co-ordination in the regulation, supervision and enforcement of AML/CFT/CPF obligations relating to VASPs, including oVASPs. Given the cross-border, digital and multi-sectoral nature of VA activity, no single authority is typically able to identify, assess and mitigate oVASP risks in isolation.

70. Domestic coordination is particularly important where oVASP activity cuts across multiple remits, including AML/CFT/CPF supervision, securities regulation, payments, tax, consumer protection, cybercrime and online content regulation. Fragmented mandates or unclear allocation of responsibilities can create supervisory blind spots that oVASPs actively exploit.

71. Jurisdictions may therefore consider establishing formal domestic coordination mechanisms, such as inter-agency working groups or task forces, to support a shared understanding of oVASP risks and enable coordinated action. At a minimum, such mechanisms can support:

    a) information-sharing on identified or suspected oVASPs;

    b) coordination between licensing, supervisory, FIU and law-enforcement functions;

    c) alignment on enforcement and disruption priorities; and

    d) joint use of available tools (e.g., STRs, market monitoring, website or app-store actions).

Box 14. Approaches to multi-agency coordination

New Zealand

New Zealand has established a formal mechanism for system-wide coordination through the Virtual Assets Investigation Resource Group (VAIRG). VAIRG brings together all key agencies, including, amongst others, the AML/CFT/CPF supervisors, the FIU, law-enforcement agencies (NZ Police), the Serious Fraud Office, Inland Revenue.

This platform enables operational knowledge-sharing across competent authorities and supports coordinated supervision, regulation and enforcement relating to VASPs. It also facilitates the identification of oVASPs that may be operating in New Zealand.

India

The Department of Revenue established a Virtual Assets Contact Sub-Group in July 2023 as a multi-agency platform to coordinate India's approach to VASP-related risks. The platform, comprising law-enforcement agencies, intelligence agencies and regulators, meets regularly to identify emerging risks, and formulate strategies. It also supports the sharing of trends, typologies and case studies, and promote synergies across agencies. It also supports the identification of oVASPs, strengthening inter-agency data-sharing, and contributes to India's national VA risk-assessment work.

Nigeria

To ensure clear roles and responsibilities, Nigeria has set up a multi-agency VASP coordination committee comprising all key supervisory, law-enforcement and intelligence bodies. This structure has reduced duplication and strengthened both market monitoring and case prioritisation. It has also enabled:

- a coherent supervisory strategy for onshore and oVASPs,
- alignment on enforcement priorities,
- formal protocols for data exchange between regulators, tax authorities, the FIU and national-security bodies,
- coordinated responses to high-risk entities operating through Nigeria-based promoters marketing, facilitating or onboarding customers for oVASPs.

Ireland

Ireland relies on structured domestic coordination mechanisms to support awareness and understanding of oVASP risks. In particular, FIU Ireland leads public–private partnership arrangements, including:

- the Joint Intelligence Group (JIG); and
- the Fintech Intelligence Taskforce (FIT).

These bring together FIU, Law Enforcement, FIs, Fintech firms, and CASPS/VASPs. These fora support regular information and intelligence sharing on emerging risks, typologies and trends, contributing to shared risk awareness across participants.

In practice, this has included consideration of oVASP-related risks, such as cross-border fund flows, typologies involving unregistered and/or offshore platforms, and indicators of potential misuse. These arrangements support early risk awareness and help inform broader FIU and law-enforcement considerations.

72. In addition to public-sector coordination, some jurisdictions have complemented inter-agency mechanisms with structured public–private engagement involving VASPs, and FIs. Such arrangements can enhance early detection of oVASP activity and improve the quality and timeliness of reporting to competent authorities.

Public-Private co-operation

73. In addition to public-sector coordination, some jurisdictions have established structured public–private working arrangements involving VASPs, banks and payment intermediaries, internet service providers, and social media companies. These arrangements can support the development of red-flag indicators, early detection of oVASP activity, and reporting to competent authorities.

Box 15. Co-operation with private sector - India

FIU India has set up a dedicated Working Group with the local VASP and other obliged entities (e.g., banks, payment aggregators and gateways) to formulate Red Flag Indicators (RFIs) for the Indian financial sector. One of the group's key goals is to jointly develop strategies to detect and address operations of oVASPs serving Indian users.

3.5. International co-operation

74. Given the inherently cross-border nature of oVASP activity, effective international co-operation is critical to identifying, supervising and, where necessary, sanctioning oVASPs that provide services into multiple jurisdictions. Weak or delayed co-operation creates regulatory blind spots that oVASPs can exploit to avoid oversight.

75. In line with the 2021 Update Guidance,[30] supervisors are encouraged to establish practical communication channels with foreign counterparts in jurisdictions where VASPs are legally established but provide services into other markets. For such co-operation to be effective, home jurisdictions should be able to respond promptly and substantively to requests from foreign counterparts, including by compelling information from VASPs under their supervision and, where appropriate, taking supervisory or enforcement action.[31] In practice, international co-operation may be required at different stages of the supervisory lifecycle, including:

[30] Please see part six of the guidance *Principles of Information-Sharing and Co-Operation amongst VASP Supervisors*

[31] Effective international co-operation may depend on home jurisdictions effectively implementing their role as primary supervisors of these oVASPs. Where home jurisdictions do not effectively supervise or enforce compliance by VASPs created or located in their jurisdiction, the ability of host jurisdictions to mitigate risks is inherently limited and reactive.

a) clarifying whether an oVASP is licensed or registered in its home jurisdiction;

b) understanding the scope of activities conducted into the requesting jurisdiction;

c) exchanging supervisory findings, or concerns; and

d) supporting enforcement or disruption measures.

Case study – co-operation in enforcement

In December 2023, the Cayman Islands Monetary Authority (CIMA) identified regulatory concerns relating to a VASP previously registered in the Cayman Islands and operating under an international corporate group. During supervisory engagement, CIMA identified links between the Cayman entity and related entities in the Abu Dhabi Global Market (ADGM) and engaged with the Financial Services Regulatory Authority of ADGM (FSRA).

The group structure involved multiple entities sharing the same ultimate beneficial owner (UBO), including an ADGM-based special purpose vehicle (SPV) that was not licensed by the FSRA to conduct any financial services activity.

Through direct collaboration, CIMA and the FSRA uncovered serious governance failures, including the UBO's misuse of his director position to override AML/CFT/CPF controls. CIMA determined that the Cayman entity was operating fraudulently, with unfit management and an unfit majority shareholder, and cancelled its registration. In parallel, the FSRA found that the Cayman entity and an ADGM-based affiliate had conducted significant unlicensed virtual asset-related payment and arranging services in ADGM by routing fiat–VA conversion transactions through the unlicensed SPV. FSRA enforcement action included financial penalties totalling USD 8.85 million and a ban on the UBO.

76. Where oVASPs operate across multiple jurisdictions, supervisors may consider more structured forms of co-operation, including bilateral or multilateral arrangements, such as joint mappings and supervisory colleges, or regular dialogue fora. These mechanisms can support coordinated supervisory engagement and ensure on supervisory expectations and efforts.

Box 16. Approaches to fostering closer co-operation

Australia

AUSTRAC established the International Crypto AML Supervisors Roundtable in 2024 to bring together 11 AML supervisors from North America, Europe, Asia, Australia/NZ to discuss operational challenges, supervision methods and share key learnings from our collective efforts supervising the sector. Jurisdictions were selected based on their crypto adoption journey and maturity. Meetings are held virtually twice a year.

The benefits for forum participants are: supervisory co-operation, knowledge and capability building, horizon scanning for better visibility of what could be ahead (from more mature jurisdictions), and collaboration/partnerships.

Outcomes to date have included: bilateral information exchanges with jurisdictions supervising similar global entities, technical capacity building by learning and comparing supervisory approaches that have worked / not worked, including how partners are using block chain analytics tools, tackling the travel rule.

Kazakhstan

Use of MoUs with foreign supervisors

Astana Financial Services Authority (AFSA), acting as the supervisory authority of the AIFC (Astana International Financial Centre) has concluded MoUs with other supervisors, such as with the National Commission of Digital Assets of El Salvador (CNAD). These arrangements provide provide predefined contact points, clearer expectations regarding response timelines, and more structured communication channels.

Use of MoUs with global VASPs

Kazakhstan's FIU (the Agency for Financial Monitoring of Kazakhstan) has also concluded a Memorandum of Understanding with a global VASP, focusing on co-operation and information exchange in AML/CFT/CPF matters. These MOUs establish a structured framework for co-operation, enabling information exchange and operational support.[32]

77. In cases where direct supervisor-to-supervisor co-operation is not feasible, excessively slow, or constrained by legal or practical barriers, some jurisdictions have relied on alternative channels, including FIU-to-FIU co-operation, to obtain the necessary information.

[32] Please see 1 and 2 for further detail.

Case study – use of diagonal co-operation

Nigerian supervisors (SEC) have relied on their FIU when co-operation channels with offshore regulators were absent, excessively slow, or when foreign public registries were inaccessible or insufficient. By channelling requests through the Egmont platform, supervisors were able to use diagonal co-operation to obtain critical information that would otherwise have been unobtainable.

This has enabled:

- tracing BO information for VASPs.
- confirming criminal investigations involving suspected oVASP operators
- identifying real-world identities behind wallets flagged through blockchain analytics

78. Regional insights[33] indicate that response times may depend on the channel used. While direct outreach to VASPs remains common, several authorities report faster responses and higher response rates when requests are channelled through supervisors or FIUs (e.g. the Egmont Secure Web) instead of address directly to the oVASP, as these give requests a clearer official standing in the oVASP's home jurisdiction. Mutual legal assistance is used less frequently due to its complexity and longer response timelines.

[33] Survey conducted amongst EAG Members, apart from India and China, on the 2023-2025 period.

4. Conclusions and recommended actions

79. The report identifies the ML/TF/PF risks that oVASPs can present, in particular when oVASPs lack clear AML/CFT/CPF obligations or oversight in the jurisdictions in which they are incorporated or located and/or if jurisdictions in which the oVASPs offer products and services do not place licensing or registration obligations on oVASPs. Differences in how jurisdictions regulate – or not, given, amongst others, diverging approaches in implementing the flexibility in R.15 (INR.15.3) – can present opportunities for jurisdictional arbitrage and challenges for effective international co-operation and enforcement.

80. The following presents a list of recommended actions for jurisdictions and private sector, based on the existing FATF Standards, updated guidance and the good practices identified in this report.

4.1. Recommended actions to mitigate the risk stemming from offshore VASPs

4.2. For all jurisdictions

81. When assessing ML/TF/PF risks related to VAs and VASPs, include oVASP activity that provides services into or from their jurisdiction, including activity conducted without physical presence, and set up a risk-based supervisory approach.

82. Co-operate, to the maximum extent possible, both among domestic relevant authorities, and with foreign competent authorities, including supervisors, in line with the FATF Principles of Information-Sharing and Co-operation among VASP Supervisors.[34] Home and host jurisdictions should consider promoting the set-up of supervisory colleges to identify and mitigate ML-TF-PF risks.

4.3. For home jurisdictions

83. For those jurisdictions where oVASPs have been created and are located:

    a. Ensure comprehensive risk-based supervision of VASPs created or located in the jurisdiction, including compliance with FATF Recommendation 18. This should be based on an assessment of the risks based on the global activities of the VASPs. This should include ensuring that supervisors have the necessary powers to obtain, on a risk basis, relevant information and documentation on the activities carried abroad and to take supervisory or enforcement action where deficiencies are identified in those operations (e.g., including in the context of international co-operation).

    b. Co-operate with foreign competent authorities, including supervisors, to the maximum extent possible. This includes quickly responding to requests for regulatory information and assisting in enforcement and law enforcement measures. It should also include proactively sharing information with foreign counterparts where significant activity affects another jurisdiction, for example, home jurisdictions should consider informing the relevant host authorities.

[34] See part 6 of the 2021 Updated VASP guidance

4.4. For host jurisdictions

84. For those jurisdictions where oVASPs are actively providing their services into:

    a. Building on the outcome of their risk assessment, jurisdictions should decide on the appropriate policy response. Jurisdictions are encouraged to use the flexibility under INR.15.3 to require oVASPs that provide services to customers in their jurisdiction to be licensed or registered domestically.

85. Based on the good practices identified in this report, jurisdictions that regulate oVASPs, authorities should consider clearly defining what constitutes the active provision of VASP services, which may include, inter alia:

    a. targeted or localised marketing,

    b. onboarding of residents,

    c. provision of VA services to domestic users,

    d. use of local payment rails or FIs, and

    e. maintenance of infrastructure, personnel, or agents serving the market.

86. Where jurisdictions restrict or prohibit certain oVASP activities, they should ensure that associated ML/TF/PF risks are identified and mitigated, including through engagement with relevant foreign supervisors, guidance to local FIs, and targeted enforcement against unlicensed activity

87. To the maximum extent possible, share relevant information with the oVASP's home supervisor regarding the VASP's provision of services in the host jurisdiction, to support a comprehensive supervision of the VASP's global activities. Host supervisors should also require home supervisors to implement appropriate measures to reduce risk where necessary.

4.5. For the private sector

88. Financial institutions and VASPs should

    a) Conduct risk assessments on their group-wide activities and apply risk-based controls in line with Recommendations 13 to manage exposure to oVASPs, including identifying such exposure, detecting potential nested activity, and mitigating associated ML/TF/PF risks;

    b) apply group-wide AML/CFT/CPF controls, where relevant, in line with Recommendation 18, to ensure effective oversight of oVASP-related activities within financial groups; and

    c) notify their home regulator or supervisor when they identify an oVASP that appears to be operating without registration or licence. In these cases, FIs and VASPs should refrain from establishing or maintain business relationships with these unregistered or unlicensed VASPs.

March 2026

www.fatf-gafi.org