



# TRUST & CORPORATE SERVICE PROVIDERS

## *Suspicious Activity Trends, Typologies & Risk Landscape*

### *Strategic Analysis Report*

Reporting Period:  
**January 2023 - March 2026**

Published By:  
**Financial Investigation Agency (FIA)**

Publication Date:  
**31<sup>st</sup> July, 2026**

*Restricted — For Official Use Only*

# CONTENTS

|   |                                              |    |
|---|----------------------------------------------|----|
| ➤ | TABLE OF FIGURES                             | 03 |
| ➤ | GLOSSARY OF TERMS                            | 04 |
| ➤ | PREFACE                                      | 05 |
| ➤ | EXECUTIVE SUMMARY                            | 06 |
| ➤ | INTRODUCTION                                 | 07 |
| ➤ | SCOPE & METHODOLOGY                          | 08 |
| ➤ | SAR TREND ANALYSIS: VOLUME<br>& DISTRIBUTION | 09 |
| ➤ | OFFENCE CATEGORIES &<br>PREDICATE OFFENCES   | 11 |
| ➤ | TYPES OF COMMON<br>OFFENCES                  | 16 |
| ➤ | GEOGRAPHICAL DISTRIBUTION                    | 19 |
| ➤ | RECOMMENDATIONS                              | 21 |
| ➤ | CONCLUSION                                   | 22 |
| ➤ | REFERENCES                                   | 23 |

# TABLE OF FIGURES

|   |                                                                       |    |
|---|-----------------------------------------------------------------------|----|
| ➤ | FIGURE 1. SNAPSHOT OF REPORTING PERIOD, 2023-2026 Q1                  | 06 |
| ➤ | FIGURE 2. TOTAL TCSP SARs REGARDING LEGAL PERSONS FILED, 2023-2026 Q1 | 09 |
| ➤ | FIGURE 3. NUMBER OF TCSP FILERS, 2023-2026 Q1                         | 10 |
| ➤ | FIGURE 4. TCSP SARs BY OFFENCE TYPE ML/TF/PF/SANCTIONS 2023-2026 Q1   | 10 |
| ➤ | FIGURE 5. MAJOR ML PREDICATE OFFENCES IN TCSP SARs, 2023-2026 Q1      | 11 |
| ➤ | FIGURE 6. HIGH-RISK OFFENCE DISTRIBUTION, 2023-2026 Q1                | 14 |
| ➤ | FIGURE 7. HEAT MAP OF RED FLAGS (LEGAL PERSONS)                       | 16 |
| ➤ | FIGURE 8. GEOGRAPHICAL ANALYSIS OF JURISDICTIONS HEAT MAP             | 19 |

# GLOSSARY OF TERMS

| ABBREVIATION | DEFINITION                                                                                         |
|--------------|----------------------------------------------------------------------------------------------------|
| AML/CFT/CPF  | Anti-Money Laundering / Countering the Financing of Terrorism / Countering Proliferation Financing |
| AI           | Artificial Intelligence                                                                            |
| AIU          | Analysis and Investigation Unit (within the FIA)                                                   |
| BO           | Beneficial Ownership                                                                               |
| BCs          | Business Companies                                                                                 |
| BVI          | Territory of the Virgin Islands                                                                    |
| BVIBCs       | British Virgin Islands Business Companies                                                          |
| CDD          | Customer Due Diligence                                                                             |
| EU           | European Union                                                                                     |
| FATF         | Financial Action Task Force                                                                        |
| FIA          | Financial Investigation Agency (Virgin Islands)                                                    |
| FIs          | Financial Institutions                                                                             |
| FIU          | Financial Intelligence Unit                                                                        |
| FSC          | Financial Services Commission                                                                      |
| KYC          | Know Your Customer/Client                                                                          |
| LEA          | Law Enforcement Agency                                                                             |
| ML           | Money Laundering                                                                                   |
| NRA          | National Risk Assessment                                                                           |
| OFAC         | Office of Foreign Assets Control                                                                   |
| PEP          | Politically Exposed Person                                                                         |
| PF           | Proliferation Financing                                                                            |
| PTC          | Private Trust Company                                                                              |
| RA           | Registered Agent                                                                                   |
| SAR / STR    | Suspicious Activity Report / Suspicious Transaction Report                                         |
| TCSP         | Trust and Corporate Service Provider                                                               |
| TF           | Terrorist Financing                                                                                |
| UBO          | Ultimate Beneficial Owner                                                                          |
| VA           | Virtual Assets                                                                                     |



# PREFACE

The Financial Investigation Agency (“FIA”) is a key component of the AML/CTF/CPF machinery within the Territory of the Virgin Islands (“BVI”). One of the most significant ways in which it fulfils its function is by serving as the *Financial Intelligence Unit (“FIU”)* of the BVI.

The core functions of an FIU are to collect, receive, investigate, analyse, exchange and disseminate financial intelligence. This is clear in accordance with Financial Action Task Force (“FATF”) Recommendation 29 by which the BVI is guided. However, Recommendation 29 also requires FIUs to conduct strategic analysis. The unit within the FIA which conducts these functions is called the *Analysis and Investigation Unit (“AIU”)*.

Pursuant to section 4(2)(f) of the Financial Investigation Agency Act, 2003 (as amended) (the “FIA Act”), the FIA is empowered to conduct strategic analysis *“which uses available and obtainable information, including data that may be provided by domestic competent authorities and foreign investigation agencies, to identify money laundering, terrorist financing and proliferation financing and related trends and patterns.”*<sup>[1]</sup>

Conducting strategic analysis achieves significant objectives. A few of these objectives include:

1. Assisting the FIA to identify money laundering (“ML”), terrorist financing (“TF”) and proliferation financing (“PF”) typologies;
2. Educating relevant stakeholders, and reporting entities, about ML/TF/PF-related trends and patterns, as well as related issues;
3. Recommending amendments to the future work and policy of the FIA;
4. Informing the development of long-term strategies to combat ML/TF/PF-related threats and vulnerabilities within the BVI which sometimes necessitates legislative intervention; and
5. Helping to inform and sensitize financial institutions, designated non-financial businesses and professions, non-profit organisations and the public generally about ML, TF, PF and other related issues.

It is indisputable that strategic analysis is a critical FIU function. This 2026 advanced strategic analysis report with a focus on TCSPs, was rendered possible due to the hard work and effort of the entire analysis team – analysts and administrative staff alike.

The FIA also takes this opportunity to renew its commitment to prepare and disseminate, when necessary, strategic intelligence. Doing so would undoubtedly enhance the ability of the FIA to contribute in a meaningful way to the AML/CFT/CPF machinery of the BVI.

---

[1] Virgin Islands Financial Investigation Agency Act, 2003, s. 4(2)(f), as amended by the Financial Investigation Agency (Amendment) Act, 2021 (No.34 of 2021).



# EXECUTIVE SUMMARY

The Trust and Corporate Service Provider (TCSP) sector remains one of the most strategically significant components of the BVI's financial services industry. As a premier financial centre, the BVI is home to an extensive volume of corporate and fiduciary structures, TCSPs occupy a critical position as institutional gatekeepers. Consequently, the sector faces inherent exposure to potential risks associated with money laundering (ML), terrorist financing (TF), and proliferation financing (PF).

This strategic analysis report examined Suspicious Activity Reports (SARs) filed by TCSP reporting entities during the period of January 2023 to March 2026. It identifies predominant offence categories, emerging typologies, geographic exposure, and risks observed within the TCSP sector.

Specific filing patterns and data distributions were evaluated to provide current risk exposures, typology guidance, and establish actionable steps to enhance compliance and fortify the overall effectiveness of the BVI's AML/CFT/CPF machinery.

KEY FINDING

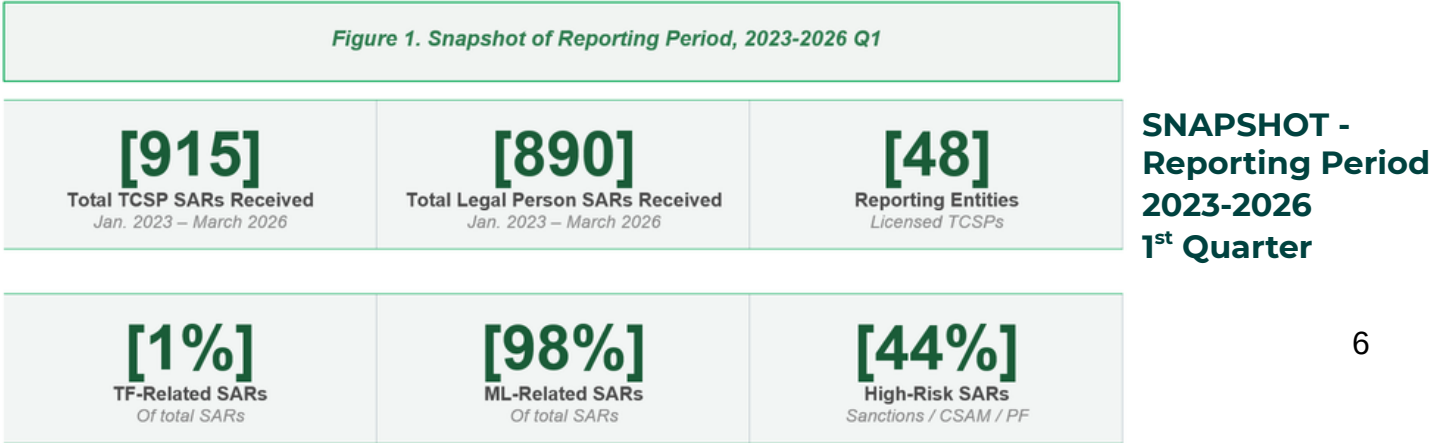
*In SARs related to legal persons, money laundering — predominantly through layering, BO concealment and real estate investment — remains the dominant offence category in TCSP-related SARs. Fraud, corruption, organised crime, and tax evasion facilitation are major risk areas within money laundering. Fraud is most frequently identified in these SARs.*

## Summary of Key Findings

- The highest reported suspected predicate offence is fraud, particularly in cases involving legal persons whose beneficial owners or directors are criminalised in other jurisdictions.
- The United States, United Kingdom, Russia, and Brazil exhibit the strongest links to BVIBCs across multiple indicators, including address, nationality, suspected criminal activity, and ongoing legal proceedings. This indicates significant cross-border use of BVIBCs in connection with major predicate offences, law enforcement activity, and the holding or movement of assets.
- Common typologies identified are layering through company structures, beneficial ownership concealment, real estate investment, professional enablement and unauthorized diversion of trust proceeds.

## Summary of Key Recommendations

- Invest strategically into the digital public infrastructure to keep abreast with advances in artificial intelligence and virtual assets that create opportunities for fraud.
- Enhance private/public sector engagement to share financial intelligence on suspected persons in real time which would support effective preventative measures.
- Strengthen onboarding procedures to identify and assess risk at the outset of the business relationship.





# 01 - INTRODUCTION

## BACKGROUND

Within the BVI's AML/CFT/CPF framework, Trust and Corporate Service Providers (TCSPs) are regulated and supervised by the Financial Services Commission (FSC) and are recognised as a high-risk sector based on the Territory's assessment of ML/TF/PF risks, given the nature of their activities and exposure to such risks. These risks are further amplified in circumstances involving complex ownership chains, nominee shareholders or directors, connections to high-risk jurisdictions, politically exposed persons (PEPs), and reliance on third-party or cross-border introducers of business.

Findings from the 2025 National Risk Assessment emphasise these vulnerabilities, noting that approximately 28% of legal persons were onboarded through third-party introducers, 10% of foreign companies were incorporated in jurisdictions assessed as high risk for ML, and approximately 14,757 PEPs act as ultimate beneficial owners (UBOs) of legal persons within the BVI (BVI, 2025a).

In addition, the 2025 Terrorist Financing Risk Assessment identified a gap between the level of risk associated with the TCSP sector and the volume of SARs submitted, highlighting this imbalance as a significant vulnerability. Between 2020 and 2023, only 448 SARs were filed by TCSP entities. However, reporting activity has shown a marked upward trend, with 223 SARs submitted in 2024, representing nearly half of the total submitted over the preceding three-year period, and a further increase to 442 SARs in 2025 (BVI, 2025b).

This upward trajectory in SAR reporting, alongside legislative amendments implemented in January 2025<sup>[2]</sup> to strengthen transparency and accessibility of beneficial ownership information, indicates that the TCSP sector is taking measurable steps to improve its detection and reporting of suspicious activity. Collectively, these developments suggest a closer alignment between the inherent risk profile of the sector and its mitigation efforts, although continued vigilance and supervisory engagement remain essential.

## REGULATORY CONTEXT

TCSPs operating in or from within the BVI are subject to licensing and ongoing supervision by the FSC under the Banks and Trust Companies Act (as amended) and the Company Management Act (as amended).

To ensure compliance with these statutory obligations, the FSC actively monitors the sector through both desk-based reviews and on-site examinations conducted by its Compliance Inspection Unit. This ongoing supervisory pressure is reflected in the FSC's enforcement and advisory activity. This sector has a massive corporate footprint, including 362,165 total active BVI Business Companies (BCs) on the register as recorded in the FSC's Statistical Bulletin (Q1 2026).

Against this sectoral backdrop, the data analysed by the FIA for this three-year period consists of SARs submitted by 48 individual Reporting Entities (TCSPs). In aggregate, the total volume of SARs examined for this report reflects a focus on approximately 523 underlying entities.

## OBJECTIVES

This report seeks to:

1. Provide a data-driven analysis of TCSP-related SAR activity received by the FIA during the review period.
2. Identify the predominant ML/TF/PF offence categories, predicate offences, red flags, and emerging typologies within the TCSP sector.
3. Highlight jurisdictional and structural patterns in suspicious activity to support targeted risk-based supervision.
4. Evaluate the risks posed by BVI business companies and structures within this sector.
5. Recommend strategic considerations and mitigation measures to enhance compliance and lower key risk areas in the TCSP sector.

---

<sup>2</sup> Reference to Section 96A of the BVI Business Companies (Amendment) Act, 2024 (Act No. 15 of 2024), effective 2 January 2025, which inserted the obligations to keep, collect and maintain BO information. Further, the BVI Business Companies and Limited Partnerships (Beneficial Ownership) Regulations 2024 (No. 59 of 2024) (as amended) which imposed obligations of filing BO information and maintenance and access of the beneficial ownership register.



# 02 - SCOPE & METHODOLOGY

## SCOPE

This report covers SARs filed by registered TCSP entities operating in the BVI during the period of January 2023 to March 2026. The analysis is drawn from the FIA's internal intelligence database and is supplemented by open-source research to identify regional and global trends and typologies that influence suspicious activity and suspicious activity reporting patterns observed within the dataset. While the report principally focuses on risks, trends and typologies involving legal persons, limited reference is also made to legal arrangements where relevant typologies were identified during the review period.

## METHODOLOGY

Intelligence was gathered and collated using the following methodology:

| PHASE                                    | ACTIVITY                                                                                                                                                                                                                                                                                     |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Data Collection                       | Extraction of TCSP-specific SARs from the FIA's internal intelligence database and refined into a sample of 681 unique SARs.                                                                                                                                                                 |
| 2. Classification                        | The employment of Excel tools, Python and Artificial Intelligence for the identification of keywords and phrases and the classification of each SAR by predicate offence, typology, and associated red flags. Findings were subject to manual review to confirm correctness and consistency. |
| 3. Intelligence Development              | Collation of SAR data with open-source intelligence (OSINT), court judgements, FSC supervisory findings, and typologies from domestic and international counterparts.                                                                                                                        |
| 4. Trends and Pattern Analysis           | Identification of recurring typologies, emerging trends, associated red flags, and risks within the TCSP sector.                                                                                                                                                                             |
| 5. Cross Referencing and Recommendations | Findings were cross-referenced against geographical indicators, including high-risk jurisdictions and relevant external developments, such as sanction designations and cross-border criminality.                                                                                            |
| 6. Quality Assurance                     | Review by FIA management and legal counsel to ensure accuracy and proportionality of findings.                                                                                                                                                                                               |
|                                          |                                                                                                                                                                                                                                                                                              |

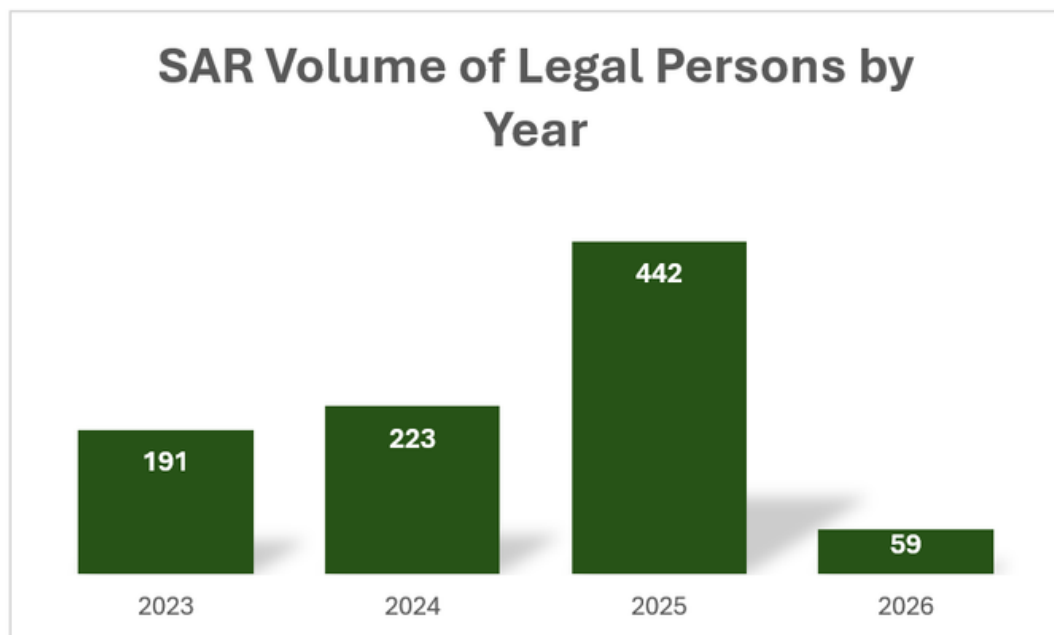


## 03 - SAR TREND ANALYSIS: VOLUME & DISTRIBUTION

### TOTAL TCSP SAR VOLUME (2023–2026)

The following diagram shows the total number of SARs received from TCSP reporting entities between 2023 and March 2026. It demonstrates a positive trend where SAR filings increased steadily over the period, with the sharpest rise recorded in 2025.

*Figure 2. Total TCSP SARs regarding Legal Persons Filed, 2023-2026 Q1*

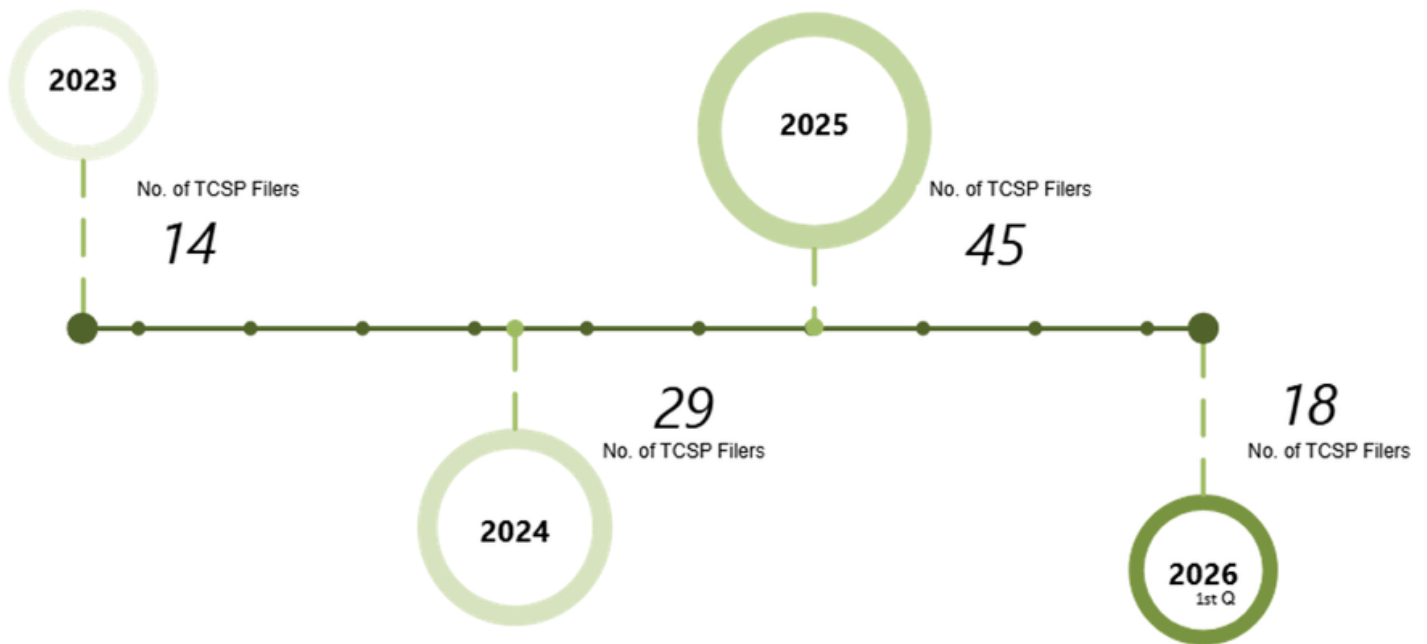


While the steady increase in SAR activity is encouraging, a structural gap remains when comparing the overall scale of the sector with levels of individual corporate engagement. Although the FSC records 296 active reporting entities overseeing a substantial corporate population of 362,165 active business companies, only 48 unique reporting entities submitted SARs during the three-year review period. This indicates that a significant proportion of all licensed TCSPs in the BVI did not submit SARs between 2023 and 2025, with reporting activity concentrated among a relatively small subset of entities. Notably, just four individual TCSPs accounted for over 60% of all submitted SARs, highlighting a degree of concentration in reporting behaviour across the sector, which underscores the importance of continued efforts to broaden participation in suspicious activity reporting.

Notwithstanding this, recent trends point to a marked improvement in engagement at the entity level. Following targeted outreach and supervisory initiatives undertaken in 2024 and 2025, the number of TCSPs submitting SARs increased significantly, rising from 14 unique reporting entities in 2023 to 45 in 2025. These developments reflect growing participation across the sector and suggest that ongoing engagement and supervisory efforts are beginning to address earlier gaps in reporting activity. Figure 3 demonstrates an increase in the number of filers per year.



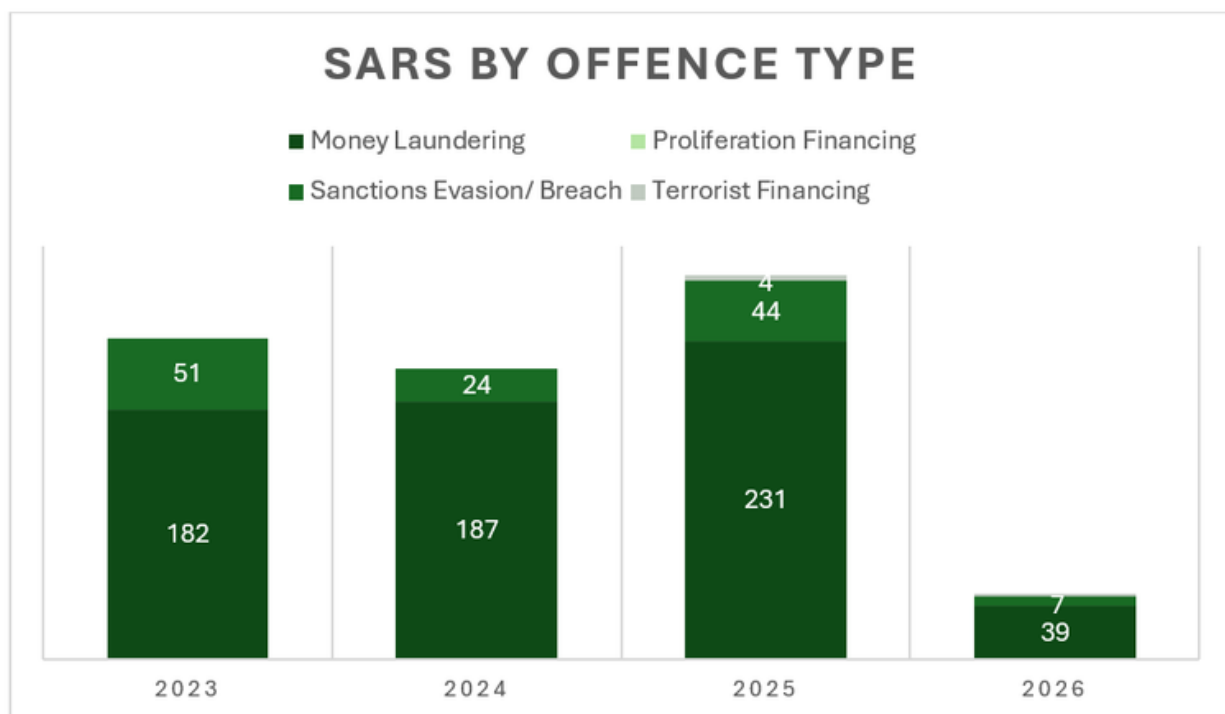
Figure 3. Number of TCSP Filers, 2023-2026 Q1



### SAR CLASSIFICATION BY OFFENCE TYPE

All SARs received are classified according to the primary suspected offence category — money laundering (ML), terrorist financing (TF), or proliferation financing (PF). As with other reporting sectors, money laundering constitutes the dominant category across all reporting years.

Figure 4. SARs by Offence Type ML/TF/PF/Sanctions 2023-2026 Q1





# 04 - OFFENCE CATEGORIES & PREDICATE OFFENCES

Adverse media referencing criminal proceedings or judicial actions in other jurisdictions appears to be a dominant trigger of SAR reporting within the sector. This trend significantly impacts analytical outcomes, as BVI structures are often reported not for confirmed misuse, but due to their association with individuals engaged in illicit activity. Consequently, the figures, trends, and typologies primarily reflect offences occurring in other jurisdictions, with the observed typologies indicating potential channels through which such activity may be facilitated.

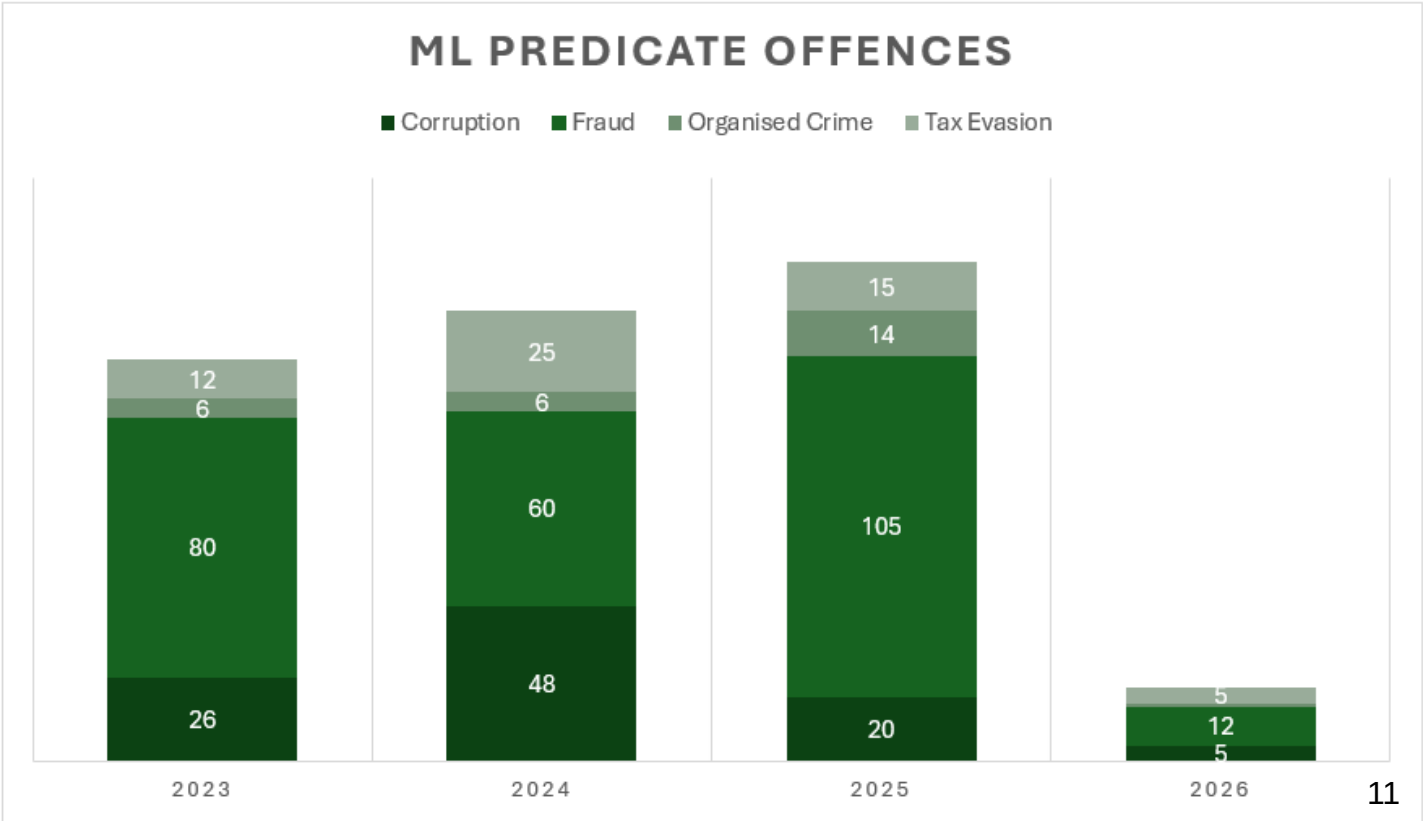
## MONEY LAUNDERING — DOMINANT OFFENCE

Money laundering remains the most prevalent offence category in TCSP SARs. The structural characteristics of TCSP services, which provide access to legal entities, nominee arrangements, and cross-border asset transfer mechanisms, make the sector particularly vulnerable to misuse for the acquisition, transfer, use, concealment, retention, or conversion of criminal proceeds (Proceeds of Criminal Conduct Act 1997, ss 29-30).

Within the ML category 15 predicate offences were identified in varying amounts. The following predicate offences were most frequently observed:

- Fraud
- Tax evasion
- Corruption
- Organised Crime

Figure 5. Major ML Predicate Offences in TCSP SARs, 2023-2026 Q1



## HIGHEST ML PREDICATE — FRAUD

Fraud was the leading offence category in SARs submitted by TCSPs during 2023–2026, accounting for 257 (38%) of the SARs submitted. Reporting peaked in 2025 with 105 cases, compared with 80 in 2023 and 60 in 2024. The 2026 figure currently stands at 12 SARs and reflects only the first quarter of the year.

Across the review period, eleven (11) fraud types were identified: bank fraud, misappropriation (incl. embezzlement), creditors' fraud, identity theft/ID fraud, investment fraud, scams operations, securities fraud, tender fraud, wire fraud, forgery and insider trading.

The most frequently identified fraud types were investment fraud and misappropriation (incl. embezzlement). These categories were relatively evenly represented, accounting for approximately 34.6% and 33.0% of fraud-related SARs, respectively.

## PROMINENT TYPOLOGIES, TRENDS & PATTERNS

Fraud-related SARs evolved over the review period, with recurring links to ongoing foreign investigations and the suspected misuse of BVI business companies, while the underlying typologies shifted over time.

2023: Misappropriation/embezzlement, and investment fraud were the dominant types, with SARs most commonly involving the suspected misuse of BVI business companies in connection with those offences.

2024: Fraud cases declined, but investment fraud and misappropriation/embezzlement remained the most prevalent typologies. Greater emphasis was also observed on real estate-linked activity involving BVI business companies.

2025: Cases increasingly feature complex corporate structures. Securities fraud and forgery rose notably and were nearly as prevalent as investment fraud, while misappropriation/embezzlement remained the most significant typology by a large margin.

Investment Fraud was the only fraud type to demonstrate a consistent decline over the review period, decreasing from 47.5% of fraud-related SARs in 2023 to 16% in 2025. In contrast, securities fraud increased significantly, with filings in 2025 being ten times higher than those recorded in 2023. Misappropriation/embezzlement also rose considerably, with reported cases in 2025 almost doubling those observed in 2023. Most of the remaining fraud types recorded their highest levels in 2025, making it the most significant year for fraud-related reporting within the TCSP sector. Overall, fraud-related SARs increased by 24% when compared with the previous year.

Consistent with these observations, the Interpol's Global Financial Fraud Threat Assessment 2026 reported that fraud had increased by 54% since 2024, with the majority of cases linked to European jurisdictions. The report identified investment fraud as one of the most prevalent fraud types across Europe, Asia and the Pacific, the Americas, the Caribbean, Africa and the Middle East (INTERPOL, 2026).

Similarly, the Chainalysis 2026 Crypto Crime Report found that investment scams remained the dominant scam category by inflow volume. The report reinforced observations made in the 2025 edition regarding the growing role of artificial intelligence in facilitating fraud and scam operations. Notably, the 2026 report identified an expansion in AI-enabled scam types, highlighting the increasing sophistication and scale of fraud-related activity (Chainalysis, 2026).

There is a notable shift towards the fraudulent use of crypto assets as the world of virtual assets becomes increasingly saturated. In the FIA's Virtual Asset Strategic Report: Virtual Assets - Evolution of the Digital Era in the Virgin Islands (2025), fraud was recognised as the leading predicate offence in ML with reference to virtual assets between 2023 and 2025 Q1. Further, the FIA's internal database shows that fraud appeared 916 times in VA SARs in 2025. This rise in VA-related fraud has impacted the way BVIBCs may be fraudulently misused. This trend is illustrated by the Cambodia-based Prince Holding Group network (Prince Group), which was publicly designated by OFAC and the UK. Publicly available information indicates that numerous BVI business companies were associated with the network's alleged use of virtual assets and offshore corporate structures in connection with investment scam activity. A significant number of BVIBCs were linked to the network, with 28 companies designated by OFAC and one company, Prince Global Group Limited, designated by the UK.<sup>3</sup> This case demonstrates how virtual assets and legal persons may be used in complex cross-border arrangements linked to suspected illicit activity.

<sup>3</sup>Internal investigations into The Prince Group is still under way therefore intelligence concerning the total and actual amount of companies linked will be reserved.

In most cases, fraud and the associated predicate offences occurred outside the BVI and were already under investigation by foreign authorities. The association between individuals implicated in criminal activity and the BVIBCs suggests that the BVI business companies may have been used to facilitate the layering and concealment of funds, or to channel proceeds derived from embezzlement and misappropriation. In some cases, those funds were allegedly used to acquire real estate, hold assets or maintain accounts in other jurisdictions, including Switzerland, or were linked to related tax offences. Ukraine, Russia, India and Brazil were the jurisdictions most frequently referenced in fraud-related SARs. This finding is consistent with trends observed in real estate-related SARs, where connections to high-risk jurisdictions, particularly Russia, represented one of the most frequently identified red flags.

## **PROMINENT TYPOLOGIES, TRENDS & PATTERNS**

The most prevalent typology, identified in 28% of SARs, involves multiple BVI business companies linked to a single beneficial owner who is the subject of corruption allegations. The second most common feature, appearing in 21% of SARs, is the holding of real estate assets through BVI entities. Properties were identified across multiple jurisdictions including the United Kingdom, United States, United Arab Emirates, and Macau. In several cases, the BVI served as the registered owner of the property or held interests in a property-holding vehicle, while the alleged proceeds of corruption were generated in the subject's home jurisdiction and subsequently invested into real estate offshore. Nominee arrangements, whereby the declared director or shareholder differs from the underlying beneficial owner, were also identified in a smaller but notable proportion of SARs.

Two recurring sub-patterns emerge from the SAR narratives. First, subjects' declared source of funds are frequently linked to contracts involving state-owned enterprises, including oil companies in Brazil, Venezuela, and Azerbaijan, pension funds in Brazil, and public procurement agencies in Indonesia, Ukraine, and Panama. Second, subjects are connected to government procurement processes where allegations include overbilling, bid-rigging, and irregular contract awards, with cases spanning Brazil, Taiwan, Argentina, and Panama. In both patterns, BVI entities are suspected of serving as the holding vehicles for assets derived from alleged corruption, bribery, or other procurement-related irregularities.

In several 2023 SAR filings, TCSPs noted continued client relationships despite adverse findings. By 2025, resignation or declined business became the dominant recorded outcome, reflecting a measurable shift in how TCSPs responded to elevated ML/TF/PF risks over the review period.

## **Organised Crime**

There were 27 SARs citing organised crime between 2023 and 2026. BVI-registered entities are reported as being connected to individual subjects to organised crime allegations across multiple jurisdictions and criminal networks.

## **Prominent Typologies, Trends & Patterns**

The most significant development in the dataset is the Prince Group, a transnational criminal organisation designated by OFAC under the Transnational Criminal Organisations sanctions programme and by the UK Foreign, Commonwealth and Development Office (FCDO) under the Global Human Rights Sanctions Regulations in October 2025. According to publicly available information, the Prince Group was associated with large-scale online fraud, human trafficking, forced labour, sextortion, illegal gambling, and money laundering activities across Southeast Asia. SARs associated with the network highlight several recurring risk indicators, including the use of aliases and legal name changes to conceal identities during onboarding. In these cases, the true identities of the principal subject and associated individuals only became apparent following the publication of the sanctions designations.

Additional SARs identified BVI entities connected to individuals linked to triad societies and junket operations in Macau and Hong Kong, money laundering investigations in Bangladesh involving alleged cross-border transfers of approximately USD 1 billion, and an illegal gambling and money laundering network associated with an organised crime clan in Italy.

## **Tax Evasion**

Tax Evasion was the third most frequently reported predicate offence during the review period. Tax-related SARs were often associated with broader concerns involving organised crime, corruption, and sanctions evasion/breach. Similar to corruption-related reporting, the highest number of tax-related SARs was received in 2024, largely reflecting the impact of major investigations that emerged in previous years.

PROMINENT TYPOLOGIES, TRENDS & PATTERNS

The most prominent trend identified in the dataset is the use of corporate entities to facilitate broader financial crime linked to tax evasion, accounting for approximately one-third of tax-related SARs. This trend demonstrates that tax evasion is frequently embedded within wider schemes involving money laundering, fraud, corruption, or other criminality, rather than occurring in isolation. It remained the dominant trend observed throughout the review period. A second significant trend is the use of offshore structures, both within and outside the BVI, to evade or obscure tax liabilities. These cases reflect the potential use of BVI and other offshore entities to hold assets, route income, or establish structures that may shield beneficial owners from tax exposure in other jurisdictions. This trend emerged prominently in 2024 and continued to feature in reporting throughout 2025 and 2026. In several cases, subjects openly expressed a desire to evade tax liabilities, prompting Registered Agents to undertake enhanced due diligence measures, which often resulted in the termination of the business relationship.

Another prominent trend is the concealment or non-disclosure of beneficial ownership and assets. Common indicators include undeclared offshore assets, incomplete beneficial ownership information, reluctance to provide due diligence documentation, and apparent attempts to conceal wealth from foreign regulatory or tax authorities. While this trend was more prevalent in earlier reporting periods, its relative frequency has declined in recent years.

An equally prevalent typology is sanctions-linked tax evasion. SAR narratives indicate a notable overlap between tax risk, sanctions exposure, and the suspected use of opaque structures to avoid scrutiny or disclosure obligations, or regulatory attention.

Less frequent but still significant typologies include the use of false documentation / invoicing schemes, nominee arrangements, and layering through complex corporate / trust structures. Although observed less often, these mechanisms can facilitate the concealment of ownership, misrepresentation of economic activity, and cross-border movement of assets.

The reports most frequently involve subjects connected to the United States, reflecting US exposure through assets, investigations, tax liabilities, and real estate holdings. Israel, Russia, and Switzerland also feature prominently, primarily in connection with beneficial ownership concerns, sanctions exposure, criminal allegations, and the holding of assets or banking relationships.

High Risk Offences

Although the following high-risk offence categories account for a comparatively small proportion of SARs, they warrant heightened attention due to their seriousness and potential implications for national security. The diagram below presents the number of SARs associated with these high-risk offences received during the reporting period.

Figure 6. High-Risk Offence Distribution, 2023-2026 Q1



## **PROLIFERATION FINANCING**

No SARs relating to proliferation financing were received during the reporting period. In addition, analysis of the jurisdictions associated with beneficial owners identified in the SARs did not reveal links to jurisdictions assessed as presenting elevated proliferation financing risks. Nevertheless, the potential misuse of BVIBCs for proliferation financing cannot be excluded, particularly where beneficial ownership is concealed or where complex and opaque ownership structures create indirect exposure to higher- risk jurisdictions.

## **SANCTIONS EVASION/BREACH**

The FIA receives SARs linked to a range of international sanctions regimes; however, 88% of sanctions-related reports relate to US and UK designations. The volume of reporting generally corresponds with the introduction of new designations or amendments to existing sanctions regimes, which often prompt reporting entities to identify previously unknown exposure through screening and ongoing customer due diligence measures.

## **PROMINENT TYPOLOGIES, TRENDS & PATTERNS**

Most UK sanctions-related reports concern the Russia (Sanctions) (EU Exit) Regulations 2019, reflecting cases in which BVIBCs and legal arrangements are directly or indirectly owned by designated Russian nationals. Across the review period, 42% of UK sanctions-related reports were triggered by the direct ownership of a designated Russian national.

In 2025 and 2026, reports were received concerning the designation of Chen Zhi of the Prince Group under the Global Human Rights Sanctions Regulations 2020 (UK), involving connected Southeast Asian individuals with ownership interests in BVI business companies. These reports highlight concerns regarding the use of opaque and dormant corporate structures connected to designated persons and their associates. More broadly, the case illustrates the intersection of sanctions exposure, organised crime, and efforts to conceal beneficial ownership and control across multiple jurisdictions.

Less common but emerging typologies associated with this offence include exposure to sanctioned financial institutions, the use of nominee directors or nominee ownership arrangements, indirect exposure to sanctioned associates, and attempted ownership restructuring following designation. Collectively, these typologies are consistent with efforts to conceal the beneficial ownership and control of BVI legal persons.

While sanctions-related reports are often associated with terrorist financing or proliferation financing indicators, the predominant association observed within the TCSP sector is organised crime. Several SARs demonstrate the use of aliases, legal name changes, nominee arrangements, and layered ownership structures to obscure the involvement of designated persons. This intersection between sanctions evasion and organised crime became particularly notable in 2025 following the designation of transnational criminal organisations and their associated networks.

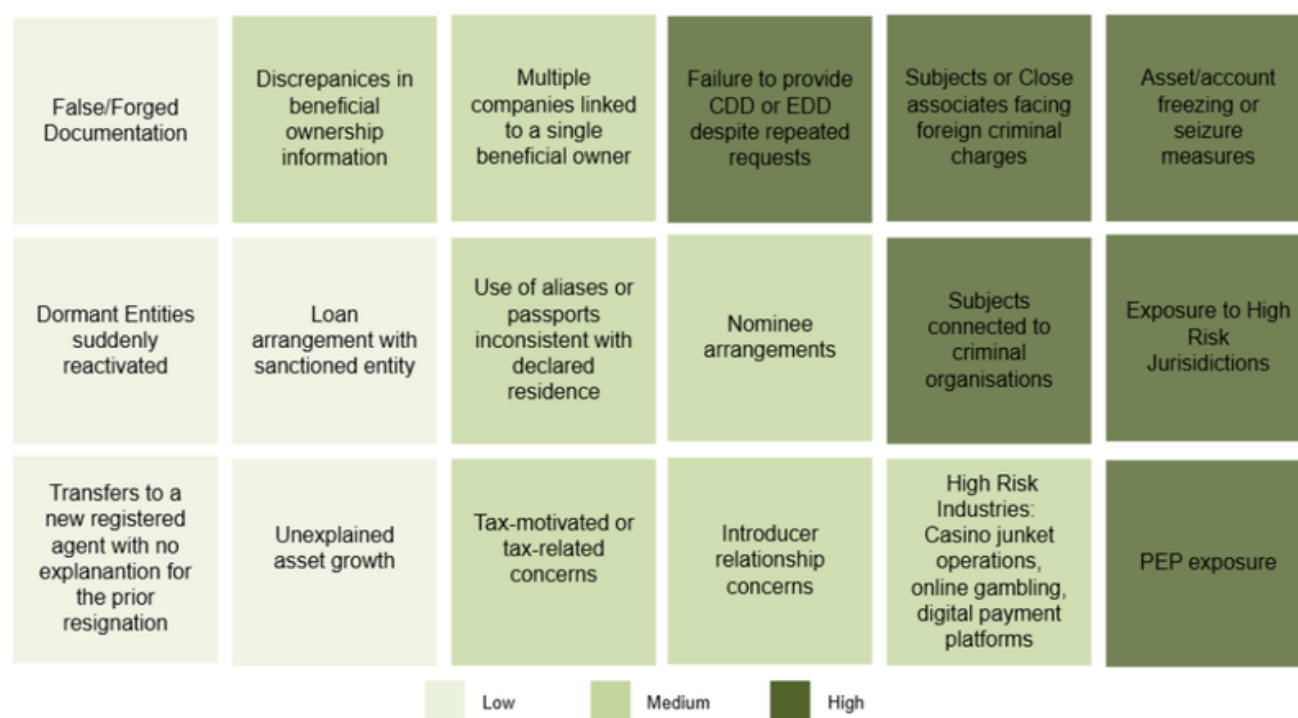
## **HUMAN TRAFFICKING AND SEXUAL EXPLOITATION**

Reports relating to human trafficking and sexual exploitation were limited during the review period. No such reports were received before 2025. In 2025, 15 SARs were submitted in connection with individuals linked to the Prince Group following international sanctions designations. All reports were associated with the same criminal network and raised concerns relating to human trafficking and related exploitation indicators.

## **RED FLAGS**

The red flags identified during the reporting period are relevant across multiple offence types and are commonly associated with behaviours involving legal persons. The following heat map highlights the most frequently observed red flags within the dataset, with high, medium and low indicating their relative frequency of occurrence.

Figure 7. Heat Map of Red Flags



The most frequently observed red flags are consistent with the overarching typology identified throughout the dataset, whereby the natural person associated with a BVIBC is the subject of criminal proceedings or judicial measures in another jurisdiction. This finding reinforces the significance of adverse media, foreign enforcement actions, and other external risk indicators in driving SAR reporting within the TCSP sector. It also highlights the exposure of legal persons to misuse by individuals implicated in criminal activity and the importance of ongoing monitoring to identify and mitigate such risks.

## 05 - TYPOLOGIES OF COMMON OFFENCES

Analysis of TCSP SARs revealed a number of recurring typologies involving legal persons and legal arrangements. These typologies reflect both global patterns documented by the FATF and Egmont Group, and BVI-specific patterns identified through domestic SAR analysis.

### LEGAL PERSONS

#### TYPOLGY 1 — LAYERING THROUGH NOMINEE ARRANGEMENTS

##### HOW IT WORKS

Individuals employ nominee shareholders, proxy directors, or associates, as well as the use of professional intermediaries to create complex ownership chains. The objective is often to obscure ownership and control, impede transparency, and reduce the visibility of links to sanctioned individuals, PEPs, or other high-risk subjects. This typology was identified across a number of major offence categories, including several of the highest-risk offences observed during the review period, demonstrating its role as a recurring mechanism for concealing beneficial ownership and controlling assets.

## TYPOLOGY 2 — COMPANY STRUCTURES FOR LAYERING

### HOW IT WORKS

The use of BVIBCs for layering emerged as a recurring ML typology within the dataset. The typology involves the suspected use of multiple BVI business companies to obscure the ownership, movement, and control of assets or funds, particularly in cases involving corruption-related offences. The pattern typically involves unnecessarily complex cross-border corporate structures, frequent changes to ownership or control, and the use of intermediary entities with limited or unclear economic purpose. In several SARs, BVI entities appeared to function as holding or intermediary layers for assets linked to foreign predicate offences, including organised crime, fraud, sanctions-related activity, and suspected corruption. The dataset also indicates that this typology intersects with nominee arrangements, particularly where the beneficial owner is concealed through family members, associates or professional intermediaries. Common indicators included an inability to verify the UBO, concerns regarding introducer relationships, and the use of multiple jurisdictions to obscure the source of funds, ownership, or control.

## TYPOLOGY 3 — COMPANY STRUCTURES FOR LAYERING

### HOW IT WORKS

The analysis identified a typology involving the concealment of beneficial ownership through the use of nominee shareholders, frequent changes in corporate control, and the strategic use of offshore entities. In several cases, declared beneficial owners were inconsistent with information obtained through court proceedings, adverse media, or institutional records, suggesting potential misrepresentation of ownership and control. Patterns of ownership restructuring and non-responsiveness to due diligence requests further indicated efforts to obscure the identity of the true beneficial owner. These mechanisms were frequently observed in SARs involving sanctions exposure, fraud, organised crime, and corruption, highlighting the role that beneficial ownership concealment may play in facilitating the misuse of legal persons.

## TYPOLOGY 4 — REAL ESTATE INVESTMENT

### HOW IT WORKS

The acquisition and holding of real estate through BVIBCs emerged as one of the most prominent typologies identified during the review period. It was the most frequently observed typology in 2023, 2024 and the first quarter of 2026, and ranked second only in 2025. Overall, it represented the most prevalent typology observed during the review period, accounting for approximately 17% of identified cases. Analysis of the underlying SARs indicates that corruption and fraud were the predicate offences most commonly associated with this typology. BVIBCs were reported as using holding real estate assets in jurisdictions including the UK, US, UAE, Cyprus, and Russia. Sanctioned individuals as well as individuals closely associated with designated individuals, frequently appeared as beneficial owners, particularly in matters involving Russian-linked exposure. In some cases, complex ownership structures were used to obscure beneficial ownership, potentially facilitating the circumvention of sanctions or concealing the source of wealth used to acquire real estate. The risks associated with the use of real estate as a vehicle for ML are consistent with findings in the European Commission's 2022 Supranatural Risk Assessment<sup>4</sup> which identified the real estate sector and real estate transactions as presenting a very significant ML/TF risk, assigning the highest risk and vulnerability rating at level 4 (European Commission, 2022).

## TYPOLOGY 5 — OBFUSCATED OWNERSHIP CHAINS AND SERVICE PROVIDER TRANSFERS

### HOW IT WORKS

Sanctions exposure is obscured through the layering of ownership across multiple corporate entities and jurisdictions, making it difficult to establish a clear picture of ownership and control. The typology is frequently accompanied by attempts to transfer structures to a new corporate service provider without full disclosure of underlying sanctions exposure or high-risk connections. In such cases, transfer may reduce the visibility of information previously known to the existing service provider and create challenges in establishing a complete understanding of the ownership structure during onboarding. The use of complex ownership chains, multiple jurisdictions, and changes in service providers may collectively serve to obscure beneficial ownership and limit transparency regarding the true source of control.

<sup>4</sup>European Commission, Commission Staff Working Document Accompanying the Document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, SWD(2022) 344 final (Brussels: European Commission, 2022), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022SC0344>

## LEGAL ARRANGEMENTS

### TYPOLGY 1 — ASSET PRESERVATION BY DESIGNATED PERSONS

#### HOW IT WORKS

*Designated persons* employ a range of mechanisms intended to preserve economic benefit from assets that may be subject to sanctions-related restrictions or asset-freezing measures. Three recurring approaches were identified.

**Exploiting ownership thresholds:** Combined family shareholdings are used to argue that no single designated individual meets an ownership threshold, despite the family collectively maintaining influence or control over the structure. In some cases, attempted asset sales at below-market value and transfers at nil value were used to further distance the designated individual from the assets.

**Post-Designation Transfers:** Ownership interests and economic benefits are transferred to non-designated family members immediately following designation. These individuals are then positioned as trust beneficiaries, shareholders, or other controlling parties. In several cases, such arrangements were observed after UK trust services sanctions had come into effect, making the provision of trust services to, or for the benefit of, the designated individual a sanctionable activity.

**Pre-Emptive Transfers:** Shares or interests are transferred at nil value to undisclosed parties shortly before an anticipated designation, with no formal documentation. The arrangements suggest the potential retention of influence or control by the designated person despite the apparent transfer of ownership.

Across these patterns, legal arrangements appear to be used to distance designated persons from assets while preserving the potential for continued economic benefit or influence over those assets.

### TYPOLGY 2 — TRUST STRUCTURE TRANSFERS AND PROFESSIONAL ENABLEMENT (THIRD PARTY INTRODUCERS)

#### HOW IT WORKS

Professional intermediaries, including incoming trust service providers, third-party introducers, and internal compliance functions, may facilitate or fail to identify high-risk activity within trust structures. In some cases, trust structures associated with sanctions exposure or other elevated-risk indicators are accepted or maintained by incoming service providers after existing providers have exited the relationship. This may occur where permissive interpretations of sanctions obligations are applied, or where available regulatory or escalation mechanisms are not pursued, thereby reducing scrutiny of the underlying client relationship. Third-party introducers may also act as the point of entry for trust-related client relationships, including in circumstances where the introducer itself presents adverse sanctions, reputational or beneficial ownership concerns. This can channel high-risk business into the jurisdiction without full disclosure of the underlying risk profile. In some instances, concerns identified in relation to trust structures were ultimately brought to light through external review processes rather than through routine internal monitoring. These cases suggest that weaknesses in the administration or oversight of trust relationships may reduce the visibility of sanctions exposure, beneficial ownership concerns, or other material risk indicators. Across these patterns, trust structures appear to be maintained, transferred, or administered in a manner that may reduce transparency regarding ownership, control, and sanctions exposure, while allowing elevated-risk relationships to remain active within the financial system.

### TYPOLGY 3 — UNAUTHORISED DIVERSION OF TRUST PROCEEDS

#### HOW IT WORKS

Trust assets or sale proceeds are diverted from the trust structure to personal accounts or personally controlled entities without prior trustee authorisation. Typically, a trust asset is sold or a transaction completed, with the proceeds directed to a personal account or separate corporate vehicle rather than the trust's designated holding structure. Following the transfer, the beneficial owner may seek retrospective documentation or a formal distribution letter to legitimise the movement of funds. In the more sophisticated variant, a new corporate entity is incorporated on an accelerated basis shortly before a significant asset sale under a stated commercial purpose rationale that is subsequently contradicted by information obtained during the due diligence process. The newly established entity is then used to receive or route proceeds through personally controlled accounts or entities rather than through the trust's holding structure, reducing transparency over the movement and ultimate destination of the funds. Across these patterns, trust proceeds appear to be redirected outside established trust administration processes, reducing trustee oversight and increasing the risk that the true purpose, destination, or beneficial control of the funds may be obscured.



# 06 - GEOGRAPHICAL DISTRIBUTION

## ASSOCIATED JURISDICTIONS BY TOP OFFENCES

Subjects connected to BVIBCs appearing in TCSP SARs are predominantly non-residents of the BVI, consistent with the offshore nature of BVI-based TCSP services. The following table illustrates jurisdictions that show up most frequently across the major and high-risk predicate offences during the reporting period, based on the origination of suspicious activity, nationality, residency, or the location of criminal proceedings/judicial measures.

Figure 8. Geographical Analysis of Jurisdictions Heat Map

| Jurisdiction   | Fraud | Corruption | Tax Evasion | Organised Crime | Sanctions   | TF  | PF | Other High-Risk |
|----------------|-------|------------|-------------|-----------------|-------------|-----|----|-----------------|
|                |       |            |             |                 | (UK/EU/US ) |     |    |                 |
| Bangladesh     | 3%    | 4%         | 0%          | 4%              | 0%          | 0%  | 0% | 0%              |
| Brazil         | 15%   | 13%        | 7%          | 30%             | 0%          | 0%  | 0% | 0%              |
| Cambodia       | 4%    | 0%         | 2%          | 11%             | 4%          | 0%  | 0% | 22%             |
| China          | 4%    | 6%         | 10%         | 7%              | 0%          | 0%  | 0% | 10%             |
| Cyprus         | 0%    | 0%         | 0%          | 0%              | 13%         | 9%  | 0% | 0%              |
| France         | 0%    | 4%         | 7%          | 0%              | 3%          | 0%  | 0% | 0%              |
| Hong Kong      | 4%    | 7%         | 10%         | 4%              | 0%          | 0%  | 0% | 24%             |
| India          | 7%    | 6%         | 0%          | 4%              | 0%          | 0%  | 0% | 0%              |
| Israel         | 2%    | 0%         | 7%          | 0%              | 4%          | 0%  | 0% | 0%              |
| Malaysia       | 5%    | 6%         | 0%          | 0%              | 0%          | 0%  | 0% | 0%              |
| Panama         | 2%    | 6%         | 0%          | 7%              | 0%          | 0%  | 0% | 0%              |
| Russia         | 14%   | 4%         | 0%          | 11%             | 30%         | 18% | 0% | 0%              |
| Singapore      | 5%    | 6%         | 0%          | 7%              | 0%          | 0%  | 0% | 0%              |
| Switzerland    | 1%    | 7%         | 0%          | 0%              | 7%          | 9%  | 0% | 0%              |
| Taiwan         | 4%    | 4%         | 0%          | 4%              | 0%          | 0%  | 0% | 0%              |
| UAE            | 1%    | 8%         | 0%          | 4%              | 4%          | 9%  | 0% | 0%              |
| Ukraine        | 7%    | 6%         | 7%          | 7%              | 2%          | 0%  | 0% | 0%              |
| United Kingdom | 5%    | 3%         | 10%         | 19%             | 22%         | 0%  | 0% | 10%             |
| United States  | 7%    | 17%        | 18%         | 41%             | 42%         | 0%  | 0% | 33%             |

## **GEOGRAPHIC CONCENTRATION OF MAJOR AND HIGH-RISK OFFENCES**

Many suspicious activity reports reference criminal proceedings and/or judicial measures undertaken in other jurisdictions, rather than suspicious activity occurring within the BVI legal person or arrangement itself. Brazil, Russia, and the United States appear most frequently in the major and high-risk categories. Higher-impact predicate offences are reported most often in connection with Brazil and Russia. In general, proceeds linked to these offences appear to flow to the United States or the United Kingdom, where they are held in various asset forms and become subject to law-enforcement action. Brazil is frequently referenced in the dataset in connection with anti-corruption investigations. Although the underlying anti-corruption investigations concluded several years ago, associated SAR reporting continues as new information emerges regarding individuals connected to BVIBCs. Russia is one of the most frequently referenced jurisdictions in sanctions breach/evasion and terrorist financing-related SARs during the review period. Sanctions placed on Russian nationals regarding the Ukraine/Russian war prompted SAR filings containing information of BVIBCs that are directly owned by designated persons. Further, Russian nationals are commonly identified in fraud-related SARs each year.

In contrast to other high-risk areas, fraud-related suspicious activity is spread more broadly across jurisdictions. However, Brazil and Russia remain notable in public-sector embezzlement, large-scale corporate fraud, and bank fraud. A smaller but increasing number of fraud-related reports were also identified in Bangladesh and Thailand.

Cambodia emerged as a notable jurisdictional nexus in 2025 in SARs involving sanctions exposure, sexual exploitation, and human trafficking. This development stemmed from a transnational criminal network suspected of using international business companies to launder illicit proceeds from fraud and human trafficking (Allard, 2026). Outside of this pattern, Cambodia has historically appeared only minimally across offence categories. Individuals from Thailand and China were allegedly identified as key actors within organised crime networks operating in Cambodia.

TF-related reporting remained limited throughout the review period and was dispersed across a broad range of jurisdictions. Russia, Qatar, Yemen, and Lebanon appeared more frequently than other jurisdictions based on nationality and address indicators.

## **DUAL CITIZENSHIP**

Cyprus, Switzerland, and the UK frequently appeared as dual-citizenship jurisdictions for Iranian and Russian subjects. This pattern was most often identified in SARs related to sanctions and terrorist financing. St. Kitts and Nevis, Dominica, and Ireland appeared less frequently. The use of dual citizenship may contribute to the obscuring of an individual's connection to a high-risk jurisdiction, particularly where the original nationality is linked to sanctions exposure, terrorist financing concerns, or other elevated-risk indicators.

## **CENTRES FOR LEGAL ENTITIES**

Hong Kong and China feature prominently in sanctions evasion/breach matters and major predicate offences-related SARs, particularly as jurisdictions of incorporation or domicile for legal persons connected to BVIBCs. These jurisdictions are also frequently associated with the provision of directorship and corporate administration services. Switzerland appears most commonly as an asset-holding and banking jurisdiction, particularly in matters involving cross-border asset preservation and wealth management.

## **LOW-FREQUENCY COUNTRIES**

More than 50 countries across the Americas, Europe, and Asia were identified in SARs spanning multiple offence categories. While these jurisdictions appeared infrequently and did not indicate consistent trends, they may point to specialised risk corridors or isolated high-risk matters. For example, corruption-related SARs linked to Macau stemmed largely from a single 2023 criminal proceeding that resulted in 17 convictions and custodial sentences of up to 24 years. Other infrequently referenced countries included Panama, India, Taiwan, Malaysia, Macau, Honduras, Venezuela, Argentina, Qatar, and the Cayman Islands. The broad geographic dispersion of countries reflects the international nature of the risks and exposures associated with the TCSP sector.



# 07 - RECOMMENDATIONS

To mitigate the ML/TF/PF risks and compliance challenges identified in this report, the FIA recommends that the following risk mitigation measures be considered and implemented by the relevant competent authorities, regulatory bodies, and TCSP industry participants:

## 1. IMPROVE SAR QUALITY & TIMELINESS

- Considering the positive impact on outreach, the FIA should continue to develop and publish TCSP-specific SAR guidance, including red flag indicators, typology examples, and guidance on reporting thresholds for complex corporate transactions.
- SARs should be filed as soon as reasonably practicable upon the formation of suspicion, consistent with section 30A of the Proceeds of Criminal Conduct Act, 1997 (as amended).
- Reasonable internal investigations/enquiries should be conducted upon the formation of suspicion, to support the submission of complete and well-substantiated SARs without unduly delaying reporting obligations.
- Include photographic identification with SAR submissions to support identity verification and related analytical or investigative measures.
- SAR reporting platforms should be enhanced to capture information unique to trust-related SARs, including details relating to settlors, trustees, beneficiaries, protectors, and other relevant trust relationships.

## 2. INVEST STRATEGICALLY INTO THE DIGITAL PUBLIC INFRASTRUCTURE AND DIGITAL VERIFICATION

- To strengthen the Territory's AML/CFT/CPF framework, a coordinated and strategic investment in technological capabilities across relevant government agencies and within the private sector is recommended. Such investments should focus on enhancing detection, verification, monitoring, and risk mitigation capabilities.
- As artificial intelligence continues to evolve, the Territory should anticipate the emergence of new ML/TF/PF risks and typologies. Appropriate technological solutions should therefore be adopted to detect, mitigate, and respond to the misuse of AI in financial crime activity.
- Particular emphasis should be placed on KYC and customer due diligence processes, given the increasing use of AI to facilitate fraud, forgery, and identity manipulation. The adoption of advanced verification technologies, including document authentication solutions incorporating metadata forensics, OCR, data validation, image analysis, EXIF analysis and MRZ verification, would assist in assessing the authenticity of identification and corporate documentation.
- The adoption of facial recognition, liveness detection, digital identity (e-ID), and KYC (e-KYC) solutions is recommended to support a more secure and efficient verification ecosystem, reduce fraud risks, and maintain alignment with evolving international standards.

## 3. PRIVATE SECTOR RESPONSIBILITIES

- Notwithstanding the provisions of the Anti-money Laundering and Terrorist Financing Code of Practice, 2008 (as amended), TCSPs should apply enhanced due diligence where beneficial ownership cannot be established to the required standard, and should not enter into, or continue, a business relationship in such circumstances.
- Control measures employed by reporting entities should be commensurate with the Territory's ML/TF/PF risk profile and the specific risks associated with complex legal persons, sanctions exposure and cross-border business relationships.
- Conduct independent enhanced due diligence before accepting any transferred business and seek to establish the reasons the prior relationship was terminated rather than relying solely on the client's stated explanation.
- The receiving TCSP should treat records obtained from a prior provider as a reference point only, and should independently verify identity, source of wealth, beneficial ownership and risk classification before accepting the relationship.

#### **4. VERIFY THIRD PARTY INTRODUCERS THOROUGHLY**

•TCSPs should apply the same level of KYC, source of wealth, adverse media, and sanctions screening to third-party introducers as they apply to the clients being introduced. Ongoing due diligence should also be conducted throughout the business relationship.

•Where an introducer also performs another role within the structure, (e.g. shareholder, director, protector, beneficiary, trustee or authorised representative), this concentration of influence or control should be explicitly identified, documented, and incorporated into the entity's risk assessment.

#### **5. PUBLIC AND PRIVATE SECTOR COLLABORATION**

•Introduce an Enhanced Due Diligence List shared via a secure web portal. The FIA may assess filed SARs and add names that meet a defined threshold, with periodic updates. The list is not intended to prohibit the establishment or continuation of business relationships, but to trigger mandatory enhanced due diligence and enhanced monitoring measures.

•Continue to publish sector-specific typologies, red flags and strategic intelligence products to assist industry participants in identifying emerging risks and enhancing the quality of suspicious activity reporting. Particular emphasis should be placed on high-risk offences, sanctions-related activity, virtual assets, and emerging threats.

#### **6. ONBOARDING**

•A declaration of the estimated value of trust or company assets should be obtained at onboarding, rather than only when a transaction, review or trigger event occurs.

•Subjects holding dual or multiple nationalities, particularly where one nationality was obtained through a citizenship or residency by investment programme, should be considered for enhanced due diligence based on the overall risk profile of the client.

•Declared sources of wealth should be verified against independent evidence rather than accepted solely based on client-provided documentation.

•The basis for the risk rating assigned at onboarding should be clearly documented, including the rationale for applying or not applying enhanced due diligence, so that a subsequent reviewer can assess whether the original classification was reasonable given the information available at the time.

## **08 - CONCLUSION**

The Trust and Corporate Service Provider sector occupies a position of unique strategic importance to the financial integrity of the BVI. As the analysis in this report demonstrates, TCSPs are not merely passive bystanders in financial crime; they represent both a potential vector for exploitation and, when supported by effective compliance controls, a critical frontline defense against ML/TF/PF.

The SAR intelligence gathered over the reporting period reveals a sector that is growing in compliance awareness, reflected in the increasing volume and improving quality of SAR filings. However, persistent risks, including the misuse of nominee arrangements, the misuse of BVIBCs and Trusts to obscure beneficial ownership, and the exploitation of cross-border corporate structures in connection with major and high-risk predicate offences— continue to demand vigilant oversight from the FIA, the FSC, law enforcement, and TCSP industry participants alike.

The FIA remains committed to the regular preparation and dissemination of strategic intelligence to strengthen the BVI's AML/CFT/CPF framework. It is imperative that the TCSP sector, the FSC, and all competent authorities continue to work collaboratively to stay ahead of evolving risks and ensure that the BVI's reputation as a trusted and well-regulated international financial centre is maintained and strengthened.

# REFERENCES

The following references informed the analytical framework and contextual background of this report:

- Allard, T.(2026). How Cambodia Became a Haven For Criminals. OCCRP. <https://www.occrp.org/en/feature/how-cambodia-became-a-haven-for-criminals>
- British Virgin Islands Financial Services Commission. (2026, March). Statistical bulletin: Q1 2026 (Vol. 82). [https://www.bvifsc.vg/sites/default/files/q1\\_2026\\_statistical\\_bulletin\\_kp\\_kc\\_.pdf](https://www.bvifsc.vg/sites/default/files/q1_2026_statistical_bulletin_kp_kc_.pdf)
- BVI Business Companies (Amendment) Act, 2024 (Act No. 15 of 2024).
- Chainalysis(2026). The 2026 Crypto Crime Report. <https://www.chainalysis.com/wp-content/uploads/2026/03/the-2026-crypto-crime-report-3-17-release.pdf>
- European Commission. (2022). Commission staff working document accompanying the document report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities (SWD(2022) 344 final). European Commission. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022SC0344>
- European Commission. (2022). Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities (COM(2022) 554 final). European Commission. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0554>
- Financial Investigation Agency 2003 (as amended). <https://laws.gov.vg/laws/financial-investigation-agency-act>
- Government of the British Virgin Islands (2025a). National Money Laundering, Terrorist Financing And Proliferation Financing Risk Assessment Of Legal Persons And Legal Arrangements – 2025. [https://www.bvifsc.vg/sites/default/files/vi\\_lpla\\_risk\\_assessment\\_2025.pdf](https://www.bvifsc.vg/sites/default/files/vi_lpla_risk_assessment_2025.pdf)
- Government of the British Virgin Islands. (2025b). Virgin Islands terrorist financing risk assessment 2025. British Virgin Islands Financial Services Commission. [https://www.bvifsc.vg/sites/default/files/vi\\_tf\\_risk\\_assessment\\_report\\_2025.pdf](https://www.bvifsc.vg/sites/default/files/vi_tf_risk_assessment_report_2025.pdf)
- INTERPOL(2026). INTERPOL Global Financial Fraud Threat Assessment Second Edition. <https://www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat>
- Money Laundering Reporting Office Switzerland (2026). Annual Report 2025. [https://www.fedpol.admin.ch/dam/en/sd-web/05JKPvNklrsY/%3AVolumes%3AData%3ABEREICH%20LAYOUT%3AEJPD%3AFEDPOL%3AMROS\\_Jahresbericht-2025%3AMROS-Jahresbericht-2025-en.pdf](https://www.fedpol.admin.ch/dam/en/sd-web/05JKPvNklrsY/%3AVolumes%3AData%3ABEREICH%20LAYOUT%3AEJPD%3AFEDPOL%3AMROS_Jahresbericht-2025%3AMROS-Jahresbericht-2025-en.pdf)
- U.S. Department of the Treasury. (2025, October 14). U.S. and U.K. take largest action ever targeting cybercriminal networks in Southeast Asia [Press release]. <https://home.treasury.gov/news/press-releases/sb0278>
- Proceeds of Criminal Conduct Act 1997. [https://www.bvifsc.vg/sites/default/files/proceeds\\_of\\_criminal\\_conduct\\_act.pdf](https://www.bvifsc.vg/sites/default/files/proceeds_of_criminal_conduct_act.pdf)

