2023

Trust and Corporate Services Providers' Guide to the Prevention of Money Laundering, Terrorist Financing and Proliferation Financing

Contents

1. Introduction

As a sector, Trust and Corporate Services Providers (“TCSPs”) have been subject to regulation in the Virgin Islands since 1990. The primary legislation for licensing of TCSPs are the Banks and Trust Companies Act, 1990 (BTCA) and the Company Management Act, 1990 (CMA). TCSPs are licensed with specific permissions on the scope of business that they may conduct from within the Virgin Islands. The ability of a TCSP to act as a Registered Agent is based on the licence type. TCSPs may conduct company management business or trust business services, or both. The Financial Services Commission (the "FSC") is the regulatory body with prudential and AML/CFT/CPF oversight of Trust and Corporate Services Providers ("TCSPs").

These Guidelines have been developed for the benefit of TCSPs and persons who may seek to become licensed as a TCSP. These Guidelines also further highlight risks TCSPs may face, including sanctions evasion, illicit financing activities and other financial crimes. Additionally, these Guidelines are geared towards assisting TCSPs in the implementation of a risk-based approach in applying measures to mitigate against ML, TF, and PF risks.

Importantly, these Guidelines also buttress the provisions for compliance with the Anti-Money Laundering Terrorist Financing Code of Practice (the "AMLTFCOP"), the Anti-Money Laundering Regulations ("AML Regulations"), the Regulatory Code (the "RC") and the Financial Services Commission Act (the "FSC Act"). In addition, the publication of the FATF Guidance for a Risk-Based Approach for Trust and Company Service Providers published by the Financial Action Task Force (the "FATF") has provided additional clarity on the unique risks impacting TCSPs. Therefore, this FATF Guidance has been factored into the development of these Guidelines[1]All TCSPs are guided to keep up to date with this and future publications from the FATF that may be relevant to the sector.

Comprehensive AML/CFT compliance by TCSPs, and other regulated entities operating in or from within the Virgin Islands (“VI”), also requires reporting and engagement with the FSC and other Competent Authorities, including law enforcement agencies. These include the Office of the Governor’s Office, Attorney General’s Chambers Royal Virgin Islands Police Force (RVIPF), the BVI Financial Investigation Agency (FIA) and the International Tax Authority (ITA).

Additionally, the Virgin Islands has expanded the scope of regulatory oversight to address evolving practices in the Fiduciary Services sector and has been at the forefront of the development of regulatory standards and the production of typology reports that relate to TCSPs. TCSPs face unique risks from bad actors who may seek to use TCSPs for money laundering (“ML), terrorist financing (“TF”) and proliferation financing (“PF”). The Virgin Islands Competent Authorities have contributed to the development of FATF Typology Reports – *The Misuse of Corporate Vehicles, including Trust and Company Service Providers* and *Money Laundering Using Trust and Company Service Providers*. Following the publication of these reports, TCSPs were alerted to the publications through different forums.

[1] The IMF’s publication, “Unmasking Control: A Guide to Beneficial Ownership and Transparency”, published on 7 October 2022, was also sourced for the development of this Guidance.

2. Applicable Persons to Whom these Guidelines Apply

2.1. These Guidelines are relevant for all persons operating as TCSPs in or from within the VI. Any entity wishing to provide company management and/or trust services in or from within the Virgin Islands is required to be licensed by the FSC. TCSPs may be licensed to operate under the following categories:

- Company Management business.
- Provider of Trustee services.

Company Management Business

Company management business includes the incorporation of legal structures and the provision of post-incorporation services or trust business services. Company management business can also include the provision of other services, such as directorship services or nominee shareholder services. Importantly, the laws of the VI do not recognise the concept of "nominee directors".

A TCSP that is licensed to provide company management business may also be authorised to act as a Registered Agent.

Trustee Services

Trust business services include a licensed TCSP acting as a trustee or protector of legal arrangements. A TCSP that is solely licensed to provide trust business services cannot be authorised to act as a Registered Agent under VI law.

3. Objective

3.1. These Guidelines give clarity on specific AML/CFT obligations for TCSPs under VI law, which includes requirements for robust customer due diligence and enhanced customer due diligence procedures, proper record-keeping measures, frameworks to fulfil statutory reporting obligations and monitoring and assessment of risks that are present in the use of legal structures and legal arrangements, as well as in the operations of TCSPs themselves. These Guidelines also highlight other critical considerations that TCSPs should address to develop and maintain a dynamic framework that enables robust compliance measures to be effective.

4. ML/TF/PF Risks and TCSPs

4.1. It is essential that TCSPs understand the importance of mitigating the risks of ML, TF, PF and other illicit activities. AML/CFT/CPF requirements for entities operating in or from within the Virgin Islands are primarily set out in the AMLTFCOP, AML Regulations, Proceeds of Criminal Conduct Act ("PCCA"), Criminal Justice (International Cooperation) Act, 1993, Counter-Terrorism Act, 2021 ("CTA"), Proliferation Financing (Prohibition) Act, 2021 ("PFPA") and the relevant Orders-in-Council related to terrorism and terrorist financing. TCSPs are alerted to existing and developing risks by Competent Authorities on an ongoing basis.

4.2. All TCSPs licensed in the VI are required to have AML/CFT measures in place towards combatting global money laundering and terrorist financing. TCSPs are required to appoint a Compliance Officer unless otherwise exempt. The duties of the Compliance Officer include, among other things, the development and implementation of the compliance framework, which addresses all areas of operation. The compliance framework must therefore be designed to prevent risks of a TCSP being used for ML, TF, PF, and other risks. Awareness of the risks that exist with the formation and use of legal structures and legal arrangements is critical for TCSPs to develop a resilient compliance framework.

4.3 FATF Recommendations 10, 11 and 17 in relation to customer due diligence, record-keeping, and reliance on third parties, respectively, are especially important for TCSPs to ensure that proper customer due diligence information is collected and maintained for all customers. TCSPs must also consider other FATF Recommendations, and in particular, Recommendations 12, 19, 20, 21, 22, 23, 24 and 25, in the development of their compliance framework.

4.4 TCSPs have been sensitised to the risks of ML and TF on an ongoing basis as a regulated sector in the VI. The following publications are relevant to TCSPs:

- FATF Typologies study on The Misuse of Corporate Vehicles, including Trust and Company Services Providers.
- FATF Report – Money Laundering Using Trust and Company Service Providers.
- The Joint FATF and EGMONT Group Report on Concealment of Beneficial Ownership.

4.5 These documents are also cited in the Guidance for a Risk-Based Approach for Trust and Company Service Providers, which was published by the FATF in June 2019. This Guidance was issued with the proviso that it be read in conjunction with the FATF Recommendations, and in particular, Recommendations 1, 10, 11, 12, 17, 19, 20, 21, 22, 23, 24, 25 and 28 and their Interpretive Notes (INR), as well as other Guidance documents issued by FATF. This Guidance provided a common understanding of TCSPs and outlined the key elements for applying a risk-based approach (RBA) to AML/CFT as it relates to TCSPs, among other things.

Taken together, these documents guide TCSPs on indicators which may point to a person engaging in ML, TF, PF or other illicit activity. Incorporating this guidance into a TCSP's systems and controls will help with the timely identification of potentially suspicious activities and mitigate risk.

5. Risks to be Monitored by TCSPs

5.1 TCSPs may be exposed to ML/TF/PF and other risks through their operations where criminals may seek to obscure the origin and ownership of criminally obtained assets through placement in legal structures or legal arrangements. Risks may also be presented where clients may seek services that are unusual or unconventional. Where TCSPs engage clients with exposure to jurisdictions that lack an effective framework for the supervision of AML/CFT risks, a thorough risk assessment should be undertaken.

5.2 The FATF Guidance for a Risk-Based Approach for Trust and Company Service Providers provides details that TCSPs should consider in carrying out risk identification and assessment. An extract of these factors have been provided in Box 1 below.

Box 1 – Extract from the FATF Guidance for a Risk-Based Approach for Trust and Company Service Providers

54. TCSPs should take appropriate steps to identify and assess the risk firm-wide, given the particular client base that could be used for ML/TF. They should document those assessments, keep these assessments up-to-date and have appropriate mechanisms in place to provide risk assessment information to competent authorities and supervisors. The nature and extent of any assessment of ML/TF risks should be appropriate to the type of business, nature of clients and size of operations.

55. ML/TF risks can be organised into three categories: (a) country/geographic risk; (b) client risk, and (c) transaction/service and associated delivery channel risk. The risks and red flags listed in each category are not exhaustive but provide a starting point for TCSPs to use when designing their RBA

56. TCSPs should also refer to their country's NRAs and risk assessments performed by competent authorities and supervisors.

57. When assessing risk, TCSPs should consider all the relevant risk factors before determining the level of overall risk and the appropriate level of mitigation to be applied. Such risk assessment may well be informed by findings of the NRA, the supranational risk assessments, sectoral reports conducted by competent authorities on ML/TF risks that are inherent in TCSP services/sector,

risk reports in other jurisdictions where the TCSP based in and any other information which may be relevant to assess the risk level particular to their practice. For example, press articles and other widely available public information highlighting issues that may have arisen in particular jurisdictions.

58. TCSPs may well also draw references to FATF Guidance on indicators and risk factors. During the course of a client relationship, procedures for ongoing monitoring and review of the client's risk profiles are also important. Competent authorities should consider how they can best alert TCSPs to the findings of any national risk assessments, the supranational risk assessments and any other information which may be relevant to assess the risk level particular to a TCSP practice in the relevant country.

59. Due to the nature of services that a TCSP generally provides, automated transaction monitoring systems of the type used by financial institutions will not be appropriate for most TCSPs. The TCSP's knowledge of the client and its business will develop throughout the duration of a longer-term and interactive professional relationship. However, although individual TCSPs are not expected to investigate their client's affairs, they may be well-positioned to identify and detect changes in the type of work or the nature of the client's activities in the course of the business relationship. TCSPs will also need to consider the nature of the risks presented by short-term client relationships that may inherently, but not necessarily be, low risk (e.g. one-off client relationship). TCSPs should also be mindful of the subject matter of the professional services (the engagement) being sought by an existing or potential client and the related risks.

60. Identification of the ML/TF risks associated with certain clients or categories of clients, and certain types of work will allow TCSPs to determine and implement reasonable and proportionate measures and controls to mitigate such risks. The risks and appropriate measures will depend on the nature of the TCSP's role and involvement. Circumstances may vary considerably between TCSPs who represent clients on a single transaction and those involved in a long-term relationship.

61. The amount and degree of ongoing monitoring and review will depend on the nature and frequency of the relationship, along with the comprehensive assessment of client/transactional risk. A TCSP may also have to adjust the risk assessment of a particular client based on information received from a designated competent authority, SRB or other credible sources (including a referring TCSP.

62. TCSPs may assess ML/TF risks by applying various categories. This provides a strategy for managing potential risks by enabling TCSPs, where required, to subject each client to reasonable and proportionate risk assessment.

63. The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential ML/TF may vary given the size, sophistication, nature and scope of services provided by the TCSP and/or firm. These criteria, however, should be considered holistically and not in isolation. TCSPs, based on their individual practices and reasonable judgements, will need to independently assess the weight to be given to each risk factor.

64. Although there is no universally accepted set of risk categories, the examples provided in this Guidance are the most commonly identified risk categories. There is no single methodology to apply

these risk categories, and the application of these risk categories is intended to provide a suggested framework for approaching the assessment and management of potential ML/TF risks. For smaller firms and sole practitioners, it is advisable to look at the services they offer (e.g. carrying out company management services may entail greater risk than other services.

5.3 ML and TF risks in relation to "shelf companies" being used by bad actors also need to be considered. These include the obfuscation of key details such as the date of operations, origin of assets and beneficial ownership information. As such, TCSPs must ensure that they are aware of the material risks presented by persons seeking "shelf companies".

5.4 Furthermore, TCSPs must remain vigilant to emerging risks and new typologies that may diminish existing risk mitigation strategies. Therefore, TCSPs must be diligent in ensuring that their risk assessment frameworks are regularly updated and calibrated to changes in risks.

5.5 TCSPs must also ensure that their culture of compliance is not undermined by external factors, such as compliance provisions being imposed that do not appropriately address ML, TF, PF risks or risks of financial crime. These external factors may include inputs originating from an affiliate TCSP not licensed in the VI or another entity that is associated with the subject TCSP through a Group of Companies.

6. Institutional Risk Assessments

6.1 TCSPs are required to assess the risk inherent in their own business, taking into consideration relevant factors, i.e. their customers, countries or geographical areas to which they are exposed, the products, services or transactions they offer and the delivery channels used to access customers. An institutional risk assessment should assist a TCSP in holistically understanding the ML/TF/PF risks to which it is exposed and identify the areas that should be prioritised to combat ML/TF/PF. For a TCSP, particular attention must be paid to the technology and cyber security risk it faces.

6.2 An important part of an institutional risk assessment is identification of the level of risks posed by each relevant factor and development of a risk rating. TCSPs must be able to identify the areas that pose higher risks and apply enhanced measures accordingly.

6.3 Records of the TCSP's institutional risk assessment must be maintained and made available to the FSC and all other competent authorities. Such records will include the findings, recommendations and steps taken to implement any recommendations. It is expected that the personnel at the highest level of

a TCSP (i.e. directors/senior management) will consider and execute the findings of the institutional risk assessment.

7. Risk Assessments of Third-Party Introductions

7.1 Section 31 of the AMLTFCOP sets out requirements wherein TCSPS can rely on an introduction made for an applicant for business. Sections 31A and 31B of the AMLTFCOP also require TCSPs to enter into written agreements and test relationships with third parties. Regulations 7, 7A and 7B of the AML Regulations also set out requirements for TCSPs in relation to reliance on Third Party Introductions (commonly referred to as Introducers). These requirements are in line with FATF Recommendation 17 and reflect good business practices for risk mitigation against ML, TF, PF and other financial crimes where a TCSP may rely on a third-party introduction.

7.2 A risk assessment taken in relation to Introducers is required and should assist a TCSP to holistically understand the ML/TF/PF risks to which it or he or she is exposed and identify the areas that should be prioritised to combat ML/TF/PF.

7.3 TCSPs should give particular attention to the risks based on the business activities/profession of the Third Party, as well as geographical and service risks that may be presented. FATF Recommendation 17 and the accompanying INR should be reviewed in the development of risk assessments conducted on Third Parties.

7.4 An important part of the risk assessment is to identify the level of risks posed by each relevant factor and develop a risk rating. TCSPs must be able to identify the areas that pose higher risks and apply enhanced measures accordingly. External factors can influence the frequency and/or risk rating of a Third Party. Therefore, TCSPs that rely on Third Parties may have to undertake more frequent risk assessments based on changing business activities, geopolitical factors or other circumstances that could impact a Third Party with whom they have a relationship.

7.5 Records of a TCSP's risk assessment of Third Parties must be maintained and made available to the FSC and all other competent authorities. Such records will include the findings, recommendations and steps taken to implement any recommendations. It is expected that the personnel at the highest level of a TCSP (i.e. directors/senior management) will consider and execute the findings of risk assessments conducted in relation to Third Parties.

7.6 Where a TCSP develops a suspicion of ML, TF or PF in relation to a Third Party, a suspicious activity report should be filed with the FIA. The TCSP should also take all appropriate steps to discontinue its relationship with the Third Party. Where a TCSP exits its relationship with a Third Party, the TCSP must undertake thorough risk assessments of all related business prior to entering into direct business relationships with clients.

8. Matters for Consideration

8.1 Record-keeping and Transaction Monitoring by TCSPs

8.1.1 Part IV of the AMLTFCOP require TCSPs to maintain records that are sufficient to show and explain transactions and fiscal positions, as well as ensure that all customer due diligence records are obtained and maintained. TCSPs must also ensure that records are maintained in a manner that allows for retrieval without undue delay, as set out by regulation 11 of the AML Regulations.

8.1.2 Section 38 of the Regulatory Code also places record-keeping requirements on TCSPs, which sets out that TCSPs must maintain records that enable the FSC to monitor compliance with its regulatory and AML/CFT obligations.

8.2 Customer Due Diligence

8.2.1. CDD relates to forestalling and preventing the activity of ML, TF and PF. TCSPs are considered to have business relationships with persons who seek services or products in the course of providing company management services and/or trust business services. In such circumstances, TCSPs are required to carry out CDD to identify and verify the applicant for business or customer. Similar identity verification is required in the case of one-off transactions. Part III of the AMLTFCOP provides the detailed requirements for undertaking customer due diligence ("CDD").

8.2.2. In addition to carrying out CDD measures when one sets up a business relationship with a customer or carries out an occasional transaction, CDD should also be carried out if the TCSP:

- suspects ML, TF or PF;
- has determined that the relationship presents a higher-than-normal risk; or
- has any doubt about any information provided by the customer for identification or verification purposes.

8.2.3. To effectively carry out the act of CDD, a TCSP must:

- have systems to identify those persons who cannot produce standard documents;
- take account of the greater potential for money laundering in higher-risk cases, specifically in respect of politically exposed persons[2];
- not deal with persons or entities if due diligence cannot be executed or the results are not satisfactory; and
- have a system for keeping customer information up to date.

8.3 Applying CDD Measures

8.3.1. The extent to which CDD measures are applied may vary to the extent permitted or required by law, based on the ML/TF/PF risk identified or associated with the business relationship or a one-off transaction. This means that the amount or type of information obtained, or the extent to which this information is verified, must be increased where the risk associated with the business relationship or transaction is higher. Conversely, it may be simplified where the risk associated with the business relationship or transaction is lower. It should, however, be noted that applying and adopting simplified CDD measures is not acceptable where there is a suspicion of ML or TF or PF, or where specific higher-risk scenarios apply.

8.3.2. Additionally, the AMLTFCOP allows TCSPs and other relevant entities to utilise technological mechanisms to effect CDD as well as record keeping. TCSPs must be able to demonstrate to the FSC that any technological means are consistent with the requirements to undertake CDD, primarily with respect to identifying and verifying applicants for business and customers, including beneficial owners. Such technological developments must neither hinder the TCSPs' ability to effectively apply CDD measures nor the exchange of information with the FSC, other competent authorities or law enforcement agencies.

8.4 Simplified CDD Measures

8.4.1 Where a TCSP determines that a customer poses a significantly low risk, having regard to the ML, TF and PF risks identified by a Virgin Islands' national risk assessment, or a risk assessment conducted by a competent authority, law enforcement agency or any other authority with responsibility relating to ML, TF or PF in the Virgin Islands, simplified CDD measures may be applied.

[2]Politically exposed persons (PEPs) are persons (foreign and domestic) who are or have been, entrusted with prominent public functions (Heads of state or government, politicians, senior government officials, judicial or military officials, senior executives of statutory bodies, senior political party officials) or who hold prominent functions within an international organisation (senior managers and members of the Board).

8.4.2 In cases where a TCSP determines that simplified CDD measures may be applied, the following non-extensive actions may be taken:

a) fewer elements of customer identification data may be obtained (production of one form of ID instead of two, for example);
b) less robust identity verification procedures may be employed;
c) collection of specific information, or the carrying out of specific measures to understand the purpose and intended nature of the business relationship may not be required (the purpose and nature of the business relationship may be inferred from the type of transactions or business relationship established);
d) the identity of the customer and the beneficial owner(s) may be verified after the establishment of the business relationship;
e) in the case of an existing business relationship, the frequency of customer identification updates may be reduced; and
f) the degree and extent of ongoing monitoring and scrutiny of transactions may be reduced, based on a reasonable monetary threshold.

8.5 Enhanced CDD Measures (ECDD)

8.5.1 ECDD refers to the additional steps a TCSP is required to undertake to limit or manage the risk posed by a customer who poses a higher level of risk. This will be the case in relation, for instance, to a politically exposed person, a person from a jurisdiction that is considered to pose a high ML/TF risk, or a person who trades in products that are of a complex nature.

8.5.2 In cases where a TCSP determines that ECDD measures should be applied, the following non-extensive actions may be taken:

a) additional identifying information from a wider variety or more robust sources should be obtained and corroborated and the information used to inform the individual customer's risk profile;
b) additional searches (e.g. verifiable adverse internet searches) should be carried out to better inform the individual customer's risk profile;
c) where appropriate, further verification procedures should be undertaken on the customer or beneficial owner to better understand the risk that the customer or beneficial owner may pose to the TCSP;
d) the source of funds and wealth involved in the transaction or business relationship should be verified to satisfy the TCSP that they do not constitute the proceeds of crime;
e) the information provided with regard to the destination of funds and the reasons for the transaction should be evaluated; and
f) additional information about the purpose and intended nature of the transaction or the business relationship should be sought and verified.

8.5.2. TCSPs should also consider the following specific higher-risk factors, which may also trigger the need to conduct ECDD:

a) Clients are connected to industries or sectors where opportunities for ML and TF are particularly prevalent. These may include clients that:
    i. become a politically exposed person; and
    ii. operate or reside in a jurisdiction that is subject to recent sanctions or has been recently listed as having major deficiencies in their AML/CFT framework.
b) The client:
    i. is involved in the shipment and/or sale of dual-purpose goods;
    ii. has been transferred to a TCSP's portfolio with little or no notification;
    iii. changes or expands its business activities into volatile markets;
    iv. frequently requests endorsements from the TCSP on their bona fides; and
    v. refuses to send complete information following a request made for more clarification for a transaction or other activity.

8.5.3. Where a TCSP is unable to verify the identity of an individual after carrying out ECCD, it should not enter a business relationship or execute a one-off transaction with that individual. If the business relationship already exists, the TCSP should terminate the business relationship. In all circumstances, the TCSP should consider filing a suspicious transaction report with the FIA in relation to the customer or individual.

8.6 Ongoing CDD and Transaction Monitoring

8.6.1 Once a business relationship is established, TCSPs have an obligation to ensure that CDD/ECDD measures are carried out on an ongoing basis. Such measures are required to determine whether executed transactions are consistent with the TCSP's information about the customer and the nature and purpose of the business relationship, wherever appropriate. These ongoing CDD/ECDD measures should allow TCSPs to identify changes in customer profiles (for example, their behaviour, use of products and the amount of money involved), and to keep them up to date, which may require the application of enhanced CDD measures.

8.6.2 An essential component in identifying transactions that are potentially suspicious is transaction monitoring. Transactions that do not fit the behaviour expected from a customer's profile or that deviate from the usual pattern of transactions may be potentially suspicious. Where new patterns of transactions emerge, TCSPs should ensure that measures are taken to determine whether there is an increased risk of

ML, TF or PF. TCSPs must also consider non-cash transactions in their monitoring processes; for example, a non-cash transaction includes requests for the provision of corporate documents. Changes in the pattern of such requests should also be factored into the assessment of ML/TF/PF risks. Monitoring should, therefore, be carried out on an ongoing basis.

8.6.3 The level of transaction monitoring should be based on a TCSP's institutional risk assessment and individual customer risk profiles, with enhanced monitoring being executed in higher-risk situations. The adequacy of a TCSP's monitoring system, and the criteria used to determine the level of monitoring to be implemented, should be reviewed regularly to ensure that they are in line with the TCSP's AML/CFT/CPF risk programme.

8.6.4 Transaction monitoring systems may be manual or automated based on the volume of transactions processed by a TCSP on a regular basis. However, where automated systems are used, TCSPs should understand their system tolerances, verify their suitability and integrity on a regular basis and verify that they take account of identified ML/TF/PF risks.

8.6.5 Transactions performed or initiated by an outsourced party must also be subject to regular monitoring under the same conditions as transactions of the TCSP itself. Such monitoring should be conducted under the TCSP's control by the TCSP itself, or in collaboration with a third party, based on appropriate agreements complying with requirements of the AMLTFCOP.

8.6.6 TCSPs should consider creating thresholds in relation to clients' assets under management, based on a risk-based approach, to determine the level of scrutiny for transaction monitoring purposes. Additionally, TCSPs should properly document, retain and communicate to the relevant personnel, including senior management and front-line staff, the results of their monitoring, as well as any queries raised and resolved. TCSPs must also undertake relevant training with regard to transaction monitoring.

9. Targeted Financial Sanctions and Sanction Screening

9.1 TCSPs must ensure that their compliance framework allows for immediate sanctions screening when an entity or individual is designated by the UN or UK. Consequently, it is expected that TCSPs should be able to screen their client base immediately upon receiving a designation notice in order to identify any designated persons and take appropriate measures in keeping with the requirements of the relevant sanctions Orders, including asset freezing and compliance reporting.

9.2 TCSPs must also ensure that they have mechanisms in place to promptly act on new designations. Such mechanisms could include subscription directly to the UN or the UK Office of Financial Sanctions

Implementation (OFSI) websites for immediate receipt of the most up-to-date designations lists to ensure that customers, clients, or applicants for businesses are not designated persons. Additionally, TCSPs must have mechanisms in place to regularly keep up-to-date with updates to the BVI sanctions regime, which can be found here. Where a TCSP has detected a customer or assets of someone that is the subject of a sanction, they are required to take freezing actions, prohibit transactions and report to BVI Competent Authorities (Governor's Office, FSC and FIA) without delay.

10. Filing of Suspicious Activity/Transaction Reports

10.1 TCSPs must ensure that their compliance frameworks include mechanisms, policies, procedures, and internal controls to promptly report suspicious transactions/activities internally and report suspicious transactions and activities (SARs) to the FIA. TCSPs must ensure that any mechanism accounts for, amongst other things, attempted activity and transactions or customer relationships that the TCSP has refused.

10.2 TCSPs' internal controls must detail how an employee should report suspicious activity and to whom. An internal SAR log should be maintained and should indicate, amongst other things, the date the suspicious activity took place, the date the report was made, the circumstances surrounding the activity and the outcome of the investigation.

Accordingly, TCSPs are required to appoint a qualified individual as its Money Laundering Reporting Officer ("MLRO") to file SARs. TCSPs are guided to note that section 17(1) of the AMLTFCOP requires the MLRO to make a report to the FIA of every suspicious transaction or customer. This report must be made in a form that ensures compliance with section 55 of the AMLTFCOP. Therefore, TCSPs are guided to adhere to requirements of reporting SARs as a means of minimising risk, including operational and reputational risk. Once a SAR has been filed with the FIA, TCSPs should take swift action to mitigate the risk of being abused by that customer for criminal purposes. This may mean reassessing the risk entailed in maintaining the business relationship and escalating the relationship to management.

10.3 Some examples of suspicious patterns or behaviour include the following (this should be read in conjunction with any other examples included in the AMLTFCOP, other documents issued by the FIA or relevant competent authority in the VI or other international standard setters such as FATF):

a) clients conducting business through or requesting services that involve unusual or complex structures without a rationale that is clear and understandable to the TCSP;
b) unexplained urgency in requesting services or products;
c) requests from clients that do not provide a clear explanation to the TCSP;

d) frequent or irregular changes of beneficial ownership or controllers or other fiduciaries of a legal structure or legal arrangement;
e) unexpected and/or frequent changes in the business activities of a legal structure or legal arrangement;
f) transactions that have no apparent benefit or purpose to the client or involves a closely connected person or entity with whom the TCSP has no business relationship with;
g) changes in method of payment for services at the last minute and without justification, or a transaction is being completed through a third party (this excludes a client that is linked to a third party that the TCSP relies upon in line with FATF Recommendation 17);
h) use of virtual assets and other anonymous means of payment and wealth transfer within the transaction without apparent legal, tax, business, economic or other legitimate reason; and
i) clients that start or develop an enterprise with an unexpected profile or abnormal business cycles or clients that enter into new/emerging markets.

10.4 There may be other emerging practices that are indicative of suspicious patterns or behaviour. As such, TCSPs are to remain vigilant and review publications of typologies of risks in relation to the use of legal structures and legal arrangements. The FATF Guidance on Transparency and Beneficial Ownership should be considered by TCSPs in the development of their risk assessment frameworks. TCSPs should also consider the FATF Guidance for a Risk-Based Approach for the Accounting Profession, as well as the FATF Guidance for a Risk-Based Approach for Legal Professionals where their activities extend to the accounting and legal services sectors. TCSPs should also pay particular attention to their specific circumstances and customers to ensure that they are able to identify suspicious factors which may present themselves or be unique to the TCSP, its services, products, or its client base.

TCSPs should also be mindful that if it, or an employee, knows or suspects that an ML/TF/PF investigation is happening or about to take place, it is an offence to disclose information to anyone else, which is likely to prejudice that investigation. Equally, if the TCSP knows or suspects that a disclosure of suspicion has been or is being made, it is an offence to leak information that could prejudice any investigation conducted. This extends beyond ML, TF, PF or other investigations to disclosures which would prejudice a confiscation investigation. Interfering with documents and other materials relevant to an investigation is also an offence. TCSPs must therefore ensure that all staff are appropriately trained and understand their legal obligations in relation to tipping off.

11 Other Risk Indicators – Concealment of Beneficial Ownership

11.1 The FATF and Egmont Group of Financial Intelligence Units carried out a study that examined mechanisms and techniques that can be used to obscure the ownership and control of illicitly gained assets. The resultant report from this joint study – Concealment of Beneficial Ownership – was published in 2018 and focused on services provided by lawyers, accountants and TCSPs. Three areas that are of

particular relevance for TCSPs in the development of their ML and TF risk mitigation strategies have been covered below.

11.2 Generating complex ownership and control structures

11.2.1 Bad actors may use complex chains of ownership to disguise beneficial ownership by using numerous layers of legal structures and legal arrangements. These legal structures and legal arrangements may be incorporated or otherwise established in multiple jurisdictions and may also be formed through the use of different DNFBPs (such as lawyers, accountants or other foreign TCSPs). While complexity in and of itself is not illegal, TCSPs should undertake additional steps to ensure that they are not being used to obscure beneficial ownership that could further ML, TF, PF or other financial crimes.

11.2.2 In assessing complex structures, TCSPs should ensure that they assess whether features that present heightened risks are present. These may include:

- Shell companies (that is, companies with no real economic activity);
- Straw men (persons who are included in the ownership structure to conceal the true beneficial ownership of a legal structure); and
- Illegal phoenix activity (where a company is created to continue the operations of another company to avoid paying creditors, taxes, and other liabilities).

11.3 Obscuring of a relationship between beneficial owners and assets

11.3.1 The use of nominee shareholders and the provision of directorship services is lawful in the VI and many other jurisdictions. As such, bad actors may seek to use nominee shareholders and directors to disguise beneficial ownership and/or control of a legal structure or legal arrangement. Importantly, the laws of the VI do not recognise the concept of "nominee directors", as all persons acting as a director of a legal structure incorporated in the VI have fiduciary duties set out in law to which they must adhere.

11.3.2 Additionally, bad actors may also use informal nominee shareholders and directors who are typically personal connections of the true beneficial owner for the purpose of maintaining a fiction of ownership. This practice is often cited as the use of "front" men or "straw" men. These persons acting as "front" men may be unaware of the true activities of the legal structure that they act for. Bad actors may also use stolen identities to establish legal structures. For example, the victims of identity theft may be used as nominees, shareholders or directors without their consent. Given the risks that may be present in the use of nominee shareholders or in the provision of directorship services, TCSPs must ensure their risk assessment processes are sufficiently robust to detect and mitigate against these risks.

11.4 Falsifying activities

11.4.1 Bad actors may hide beneficial ownership through criminal activities, which include the falsification of documents. Several methods have been identified that have been used for this purpose. More common schemes include:

- False loans and invoices, and other transactional documents to disguise the beneficial ownership of a transaction (or multiple transactions).
- Use of "load-back" schemes where a loan is issued to a third party following the payment of a business invoice.
- Falsifying prospectuses, accounting records and other statements to attain a favourable outcome in a registration, acquisition, or other business transaction.

11.4.2 TCSPs are guided to ensure that they keep abreast of future developments and publications by the FATF and other international standard setters in relation to developing risk indicators.

11.5 Bearer Shares

11.5.1 Prior to 2023, the use of bearer shares in legal structures incorporated in the VI was permitted, providing that any bearer shares issued were immobilised through placement with a Custodian. Effective 1 January 2023, bearer shares may no longer be issued. All existing bearer shares must be redeemed or converted to registered shares on or before 1 July 2023. Any bearer shares not redeemed or converted by that date will be deemed to have been converted to registered shares. As a part of efforts to ensure compliance with VI laws, TCSPs are required to take all steps to ensure that in the rare cases where bearer shares are in issue, they are redeemed or converted.

11.5.2. The use of bearer shares and similar instruments continues in other jurisdictions. Therefore, TCSPs must be vigilant where foreign legal structures may be utilised by a customer or applicant for business and may contain bearer shares, bearer warrants or other similar instruments. In such cases, TCSPs must ensure that they conduct enhanced due diligence and determine whether there is a valid reason for the use of such instruments. Due to the nature of bearer shares, TCSPs must ensure that they can effectively monitor beneficial ownership on an ongoing basis or exit a business relationship where beneficial ownership cannot be accurately determined and monitored, including due to bearer shares.

12 Employee Screenings

12.1 TCSPs must ensure that they screen their employees in accordance with section 49 of the AMLTFCOP. To safeguard against ML, TF, PF and other risks, measures must be in place to assess the competence and probity of employees at the time of recruitment and intermittently thereafter. These assessments of employees must include background checks as well as an assessment of integrity, skills, knowledge, and expertise to ably carry out their functions. Additional assessments and screening of employees must also be carried out to mitigate against operational and compliance risks where there is an anticipated change in their role or functions. This is of particular importance where the employee is responsible for the implementation of or monitoring of AML/CFT/CPF controls, which may occur directly in relation to the compliance function or indirectly in relation to other functions.

12.2 TCSPs must also ensure that the screening of employees is proportionate to the ML/TF/PF risks to which that employee may be exposed, regardless of the level of seniority of any employee. In addition, systems must be established to address potential conflicts of interest for staff with AML/CFT/CPF responsibilities. TCSPs must also be aware of their responsibility to report employee misconduct to the FSC and, where relevant, any other competent authority or law enforcement agency.

13 Powers of the FSC

13.1 The FSC has the power to inspect a regulated entity or any other entity that falls under its supervisory remit. Inspections may occur without notice and include a review of compliance against AML/CFT/CPF laws, as well as other regulatory requirements. The FSC's powers also include its ability to take enforcement action for non-compliance with financial services legislation, including AML/CFT legislation, against a TCSP, its directors, shareholders, and senior officers. Where a TCSP may be operating in or from within the VI but has not been licensed, the remit of the FSC extends to that entity in its ability to take enforcement action for an unauthorised business.

14 Information Exchange

14.1 Information exchange between TCSPs and other financial institutions, as well as regulatory and law enforcement authorities, is an important part of the VI's strategy for combating ML/TF/PF and should also form part of a TCSP's ongoing controls. Where authorities are armed with suspicion or evidence of a person's link or suspected link to ML, TF, or PF, they should be able to share that information with the TCSPs so that the latter can better engage its processes in dealing with such a person. Conversely, TCSPs should also be able to share general information about the type and nature of suspicious activities that

may be linked to ML, TF or PF with other financial institutions and government agencies, including the regulator, subject to the requirements to ensure that there is no tipping off related to the filing of a SAR. This can only help to strengthen the TCSP sector and insulate it from abuse and misuse for ML, TF and PF purposes.

14.2 There are various types of information that can be shared between regulatory and law enforcement agencies and TCSPs. Such information may include:

- ML/TF/PF risk assessments;
- General feedback on suspicious transaction reports and other relevant reports;
- Typologies of how money launderers or terrorist financiers have misused TCSPs;
- Targeted unclassified intelligence which, subject to appropriate safeguards such as confidentiality agreements, may be shared with TCSPs, either collectively or individually; and
- Sanctions lists issued through the Governor's Office and published by the FSC and FIA include countries, persons, or organisations whose assets or transactions should be frozen pursuant to targeted financial sanctions.

14.3 Domestic cooperation and information exchange between TCSPs and the FSC (as the supervisor of the TCSP sector), among law enforcement and intelligence agencies, and between the FIA and FSC, is extremely important in the effective monitoring and/or supervision of the TCSP sector.

14.4 Cross-border information sharing between authorities and their international counterparts with regard to information held within the TCSP sector is also vitally important given the multi-jurisdictional reach of many TCSPs. TCSPs must ensure that they fully comply with the CDD and record-keeping requirements, as well as all other requirements of the AMLTFCOP and AML Regulations, to ensure that the VI is able to meet its international cooperation obligations, including those relating to beneficial ownership.

15 Overarching Requirement for Compliance

15.1 All TCSPs must remain vigilant in relation to evolving ML, TF and PF threats, as well as other threats that can negatively impact their operations. To mitigate against these threats and risks, TCSPs must be diligent in the application of AML/CFT/CPF measures. These measures must be holistic and integrate prudent governance and modern risk management strategies with a robust compliance framework. TCSPs must remain agile and embed systems to allow for continual improvement in the efficiency and effectiveness of compliance.