Guidance

AN EFFECTIVE APPROACH TO ONGOING MONITORING

Table of Contents

Introduction

These Guidelines are issued by the Financial Services Commission (the "FSC") as the supervisor of financial institutions (FIs) and the Financial Investigation Agency (the "FIA") as the Anti-Money Laundering, Counter-Financing of Terrorism and Counter-Proliferation Financing (AML/CFT/CPF) supervisor of Designated Non-Financial Businesses and Professions (DNFBPs) in the Virgin Islands (VI).

The FSC is responsible for the regulation and supervision of the financial services sector: (i) banking, (ii) insurance, (iii) trust and company services providers ("TSCPs"), (iv) investment business, (v) financing business (FB), (vi) money service businesses ("MSBs"), (vii) insolvency services, and (viii) virtual asset service providers ("VASPs"). The FIA is responsible for the supervision and monitoring of DNFBPs in the VI: (i) legal practitioners, (ii) notaries public, (iii) accountants, (iv) real estate agents, (v) dealers in precious metals and stones ("DPMS"), (vi) high value goods dealers ("HVGD"), (vii) vehicle dealers, and (viii) persons engaged in the business of buying and selling boats. For the purposes of these Guidelines, the entities supervised by both the FSC and FIA are collectively referred to as "licensees".

As supervisors, the FSC and FIA are cognisant of the need to ensure all licensees are aware of the various risks related to their business. As members of the Council of Competent Authorities' Joint Supervisory Committee, the FSC and FIA are committed to ongoing cooperation and collaboration on matters that impact licensees to ensure proper risk mitigation and enhance transparency, while maintaining the VI's reputation as a place to conduct legitimate and quality business.

Comprehensive AML/CFT/CPF compliance by licensees is essential to remain up to date with evolving risks that could adversely impact operations. These Guidelines have been developed for the benefit of assisting licensees in the implementation of a risk-based approach for applying measures to mitigate against money laundering ("ML"), terrorist financing ("TF") and proliferation financing ("PF") risks through ongoing monitoring of transactions and business relationships.

Importantly, these Guidelines also buttress the provisions for compliance with the Anti-Money Laundering and Terrorist Financing Code of Practice (the "AMLTFCOP"), the Anti-Money Laundering Regulations (the "AML Regulations"), the Regulatory Code (the "RC"), the Financial Investigation Agency Act (the "FIA Act") and the Financial Services Commission Act (the "FSC Act"), including any Explanatory Notes to these documents.

These Guidelines also serve as a complement to the ongoing need to report and engage with the FSC, FIA and other competent authorities, including law enforcement agencies, to achieve optimal results in preventing ML, TF and PF risks from being realised. These agencies include the Office of the Governor (GO), Attorney General's Chambers (AGC), Royal Virgin Islands Police Force (RVIPF) and the BVI International Tax Authority (ITA).

Background

Licensees have a responsibility to carry out ongoing monitoring of customers, including any legal persons and legal arrangements that are customers or to which customers may be connected. Effective monitoring involves an ongoing review of clients and business relationships as well as the monitoring of transactions, including one-off transactions in order to identify:

a) for the purpose of reassessing the client's risk rating, transactions that may present elevated risk;
b) unusual or suspicious transactions that may require filing a SAR; and
c) transactions that are in breach of targeted financial sanctions.

This duty is embedded in the VI's AML/CFT/CPF laws and regulations. Primarily, the requirement to undertake ongoing monitoring is contained in section 21 of the AMLTFCOP. These legal requirements are derived from the international standards developed by the Financial Action Task Force (FATF) and are promulgated globally.

Ongoing monitoring is an integral facet to the measures required of all licensees in mitigating against ML, TF, and PF. As a critical aspect of AML/CFT/CPF compliance, ongoing monitoring must be effectively and consistently carried out by licensees. Licensees should also establish procedures within their compliance manual outlining measures for effective ongoing monitoring of these entities. In addition, licensees identified through relevant risk assessments as presenting a higher level of risk (e.g. those providing incorporation and formation services to legal persons and legal arrangements) may better mitigate these risks through robust ongoing monitoring systems.

Prerequisites for Ongoing Monitoring

To ensure that licensees are in a position to carry out effective ongoing monitoring, it is important to collect proper due diligence on customers, including legal persons and legal arrangements, as customers can present varying levels of ML, TF and PF risks. Integral to ensuring that a licensee is positioned to conduct effective ongoing monitoring is: (a) having a clear understanding of customers' business activities; and (b) being able to establish whether there are connections, through the presence of legal persons or legal arrangements, that increase risks (this includes the presence of sanctioned persons or those connected to sanctioned persons or high risk countries, Politically Exposed Persons (PEPs), high risk industries, etc.).

Such initial due diligence enables the creation of a base profile of the nature of business and activities of the customer and an initial understanding of the ML, TF and PF risks presented. However, the circumstances or profile of a customer may change, which may lead to a licensee having to make an adjustment in the risk profile of the customer. Therefore, carrying out ongoing

monitoring is vital to being able to identify customers whose risk profile has changed to better enable the licensee to detect customers who may become involved in, or misuse legal persons and/or legal arrangements to facilitate ML, TF or PF.

Transaction Monitoring

Licensees must monitor all customer transactions and activity to identify notable transactions or activities that may indicate a change in customer circumstances or transactions that:

- are inconsistent with the licensee's knowledge of the customer (unusual transactions or activity);
- are complex or unusually large;
- form part of an unusual pattern; or
- present a higher risk of ML, TF or PF.

Such unusual transactions or patterns of transactions may require a licensee to conduct an enquiry to determine whether the transactions are indeed suspicious. Licensees must examine and enquire into, as far as possible, the background and purpose of transactions meeting the above criteria and record their findings in writing. If a licensee has knowledge or a suspicion that these transactions are questionable, they must file an internal suspicious activity report with their money laundering reporting officer.

Proper policies and procedures should be established to:

a) review customer transactions and customer activity using a risk-based approach depending on the risk of the customer;
b) provide training to staff on transaction monitoring, as well as detecting and handling unusual transactions
c) where appropriate, implement automated transaction monitoring systems
d) review the effectiveness of their transaction monitoring program periodically and have a system to remediate any deficiencies found

It is important to note that licensees' scrutiny of customer activities also includes business relationships that do not generally involve transactions, e.g., where a licensee provides investment advice, directorship services or nominee shareholder services.

Outsourcing

Where a licensee outsources and/or contracts a third party (including a Group entity) to carry out its ongoing monitoring or elements of its function, the licensee must ensure that it has adequate measures in place to confirm that the third party is effectively carrying on these functions as if that party was a licensee under the relevant legislation in the VI. The licensee's monitoring of the

outsourced functions must include testing, recording the findings of such testing and taking steps to mitigate results of such testing. Where the results of the licensee's testing of the relationship with the third party leads to less than acceptable findings, particularly findings not in compliance with the requirements of VI legislation and the third party is unable to correct the deficiencies in a timely manner, the licensee must terminate the agreement, seek an alternative service provider or perform the functions itself, including conducting a risk assessment of all entities for which the third party was responsible for monitoring. This will ensure that the licensee is aware and understands the risks posed by each individual customer.

Elements of an Effective Ongoing Monitoring System

An effective transaction and activities monitoring system would likely comprise the following elements:

- **Robust framework**: The risks licensees face are dynamic, and the transactions they carry out are varied and unique to certain types and categories of licensees. Certain licensees, based on class and type of licence and services provided, would also engage in a significant volume of transactions. Licensees should, therefore, regularly review and enhance their monitoring frameworks, which should be targeted at sustaining and/or improving system effectiveness. Not all relationships or transactions should be monitored the same way. The degree of monitoring employed will depend on the perceived risks presented by each customer or transaction. Licensees with higher inherent ML, TF or PF risks or specific control deficiencies should ensure their monitoring frameworks account for these elevated risks and sufficiently allow for more frequent monitoring and reviews to be performed in order to adequately mitigate their risks.
- **Robust culture of risk awareness:** Licensees must ensure that staff understand the importance of the licensees' monitoring functions, and that these functions are executed by competent and well-trained staff who exercise sound judgment in targeting unusual transactions, activities and behaviours. Staff should be fully versed in understanding the risks posed by the licensee's business and customers.
- **Meaningful and identifiable integration:** Licensees should ensure that their monitoring systems and frameworks reinforce, and are reinforced by, the broader AML/CFT/CPF controls that they employ, including by designating clear responsibilities for the effective conduct of the monitoring function across all business lines by staff such as frontline and compliance staff.
- **Active and continuous oversight:** Board and senior management must take an active role in overseeing the satisfactory performance of monitoring functions and should drive continual enhancement with a view to ensuring that key risks are appropriately mitigated. When outputs or outcomes are compromised due to factors such as inappropriate comparison of data based on factors that are irrelevant or provide an inaccurate measurement, process inefficiencies, staff issues or system failures, it is incumbent on the board and senior management to adequately resolve these matters in a prompt and

timely manner. The board and senior management should communicate clear risk appetites and set a firm tone from the top that the detection, prevention and mitigation of ML, TF and PF are a priority.

Monitoring Legal Persons and Legal Arrangements

Licensees will have legal persons and legal arrangements as customers or as part of the structure of customers' activities and therefore, will have to take measures to ensure ongoing monitoring is performed on these entities. Licensees should be mindful that the criteria for the identification and verification of legal persons and legal arrangements are different from those for natural persons. Generally speaking, each business relationship or occasional transaction involving a legal person or legal arrangement will also contain a number of associated natural persons, for example, as beneficial owners and directors. However, the nature of the business relationship with the licensee would determine the manner in which ongoing monitoring should be undertaken. Further, monitoring of legal persons, trusts or other legal arrangements by a licensee should involve qualified personnel who are familiar with the particular characteristics of the various types of legal persons, trusts and similar legal arrangements.

Where licensees' business relationships involve the establishment of legal persons and legal arrangements, those relationships would require targeted monitoring mechanisms. Given the nature of company formation in the VI, where establishment of legal persons and legal arrangements can only be facilitated through TCSPs, the risk of inappropriate and inadequate monitoring of legal persons and legal arrangements elevating ML, TF and PF risk is greater for TCSPs. This section therefore is primarily focused on TCSPs and how ongoing monitoring can be undertaken for legal persons and legal arrangements created or administered by those licensees. This section should be read in conjunction with Section 21 of the AMLTFCOP and the Explanatory Notes to that section, which provides additional guidance.

Monitoring of Legal Persons by TCSPs

Licensees that provide certain value-added services to legal persons, including corporate secretarial services, directorship services[1], acting as a nominee shareholder, or any other established service or service provided by the licensee where the licensee acts solely on the

[1] It is important to note that the concept of a 'nominee director' is not recognised in the Virgin Islands. Under BVI law, all directors have a fiduciary duty to the corporate structures for which they act. However, where a director is acting on instructions of a third-party individual, this fact is required to be disclosed to the company. The agent is also required to enquire whether this is the case, and where this is the case the company is required to provide this information to the Registrar. Sections 120 through 125 of the BVI Business Companies Act, 2004 are relevant for BVI Business Companies. Similar provisions exist in other legislation that allows for the incorporation of other BVI corporate structures.

instructions of another party, should also understand that these same services may elevate the risk of misuse of these legal entities.

The provision of additional services beyond solely incorporation services expands the scope for a licensee to actively monitor these legal persons. Procedures should, therefore, be developed to ensure that robust AML/CFT/CPF measures, including ongoing periodic monitoring and transaction monitoring, are in place during the provision of these services.

Monitoring activities of legal persons should also include monitoring of transactions that involve transfers of value (i.e. fiat or virtual assets) as well as non-cash transactions[2]. For TCSPs, transactions that are non-cash transactions would be particularly relevant for transaction monitoring given the services provided to legal persons. For example, obtaining a certificate of good standing is a non-cash transaction. A customer who owns a legal person may traditionally obtain one certificate of good standing annually for the purpose of maintaining a bank account. This establishes a transaction pattern. However, if the customer requests eight certificates of good standing, that is a deviation from the established transaction pattern. Therefore, a licensee should obtain information in relation to such a transaction that falls outside the expected transaction pattern for the customer.

Importantly, licensees also need to monitor changes to the business activities of their customers, including where those customers are legal persons or connected to a legal person (e.g. through ownership, directorship or other means). The established business activities at the time of onboarding a customer may change or expand over time. For example, a customer may own a legal person that provides commercial rental spaces in an EU country and those business activities are properly disclosed. After a year, the legal person may expand its operations into a high-risk country. This expansion does not change the nature of the business activities, but the potential risks have changed. If a licensee's monitoring systems are not sufficiently robust, this expansion may be overlooked. Alternatively, a customer may diversify the business activities of the legal person without properly disclosing the occurrence of this change. To ensure that licensees are aware of potential risks, they must ensure that they remain aware of the full scope of business activities of the legal persons that are connected to their customers, as well as be able to ascertain those activities that are expanding in scope, geographic reach, customer base, etc. Licensees should also be aware of higher risk business activities for ML, TF and PF. Such activities may include activities in industries such as mining, shipping (as it concerns proliferation financing) and VASPs.

Financial records of legal persons can also aid in the monitoring process. Reviewing financial statements – which may include bank statements and other records – can provide additional insights into the activities of the legal persons, as well as the types of assets held or owned. By

[2] Such monitoring also equally applies to legal arrangements as appropriate.

extension, the nature of the assets owned by a legal person can provide insights into its business activities and associated risk factors. In some cases, these assets may trigger the need for heightened monitoring. For example, a customer that owns a company that processes and ships radiological materials for oncological treatments presents risks through the materials being shipped. These materials can be classified as dual-purpose goods which could be used illicitly for proliferation activities. Therefore, the licensee would need to identify this as a high-risk activity and its risk assessment framework should adequately respond to such higher risk scenarios. In such circumstances the licensee should implement measures to mitigate the risk including taking steps to ensure that the legal person is carrying on the activity for which it was established and that the activities do not lead to the facilitation of, or direct conduct of illegal activity, including potential breaches of targeted financial sanctions or other sanctions applicable to the VI. For licensees that are TCSPs the financial returns[3] submitted by a company or a partnership can provide a source of monitoring.

Monitoring of Legal Arrangements

The monitoring of legal arrangements, which in the VI primarily relates to trusts, may have similarities to the monitoring of legal persons as the case may dictate. However, there are unique elements related to legal arrangements that licensees should consider as well. Licensees may act in a number of fiduciary roles to a legal arrangement, such as being appointed as a trustee, protector, enforcer or administrator. The nature of a licensee's role will impact its approach to monitoring the legal arrangement. Further, there are other specific characteristics of a trust that a licensee should be aware of and ensure it appropriately monitors. These include where the trust has flight clauses, as well as settlors' reserve powers including the power to revoke a trust, or where trusts are part of a larger complex ownership structure (i.e. a structure involving multiple legal persons and multiple connected jurisdictions).

While a trustee and other fiduciaries must act in the best interests of the beneficiaries, these fiduciaries also have AML/CFT/CPF obligations to develop a comprehensive policy for the monitoring of legal arrangements. As such, the monitoring mechanisms should be well documented to enable reviews by the licensee's compliance staff, and its internal audit function, as well as by the FSC or the FIA as the case may be.

Trigger Events: Legal Person and Legal Arrangements

Trigger events identify actions or conditions that, when materialised, may cause a change in a customer's circumstances. Licensees should have policies and procedures in place detailing systems and controls that will enable them to identify, assess, monitor and manage the risks that such trigger events may present.

[3] Financial returns required to be submitted under the BVI Business Companies (Financial Returns) Order.

In addition to the scenarios outlined above, trigger events for legal persons may also include[4]:

i. Sudden increase/decrease in volume and/or value of transactions;
ii. Change in normal payment methods;
iii. Change in directors, shareholders, beneficial owners or other connected persons;
iv. Change in business activities;
v. Change in place of business;
vi. Identified news (positive or otherwise) involving the customer and/or connected persons such as mergers, acquisitions, accusations of bad actions and links to higher risk jurisdictions; and
vii. Change in circumstances of connected persons such as addresses, PEP status, nationality, sanction designation or connection to sanctions persons etc.

In relation to legal arrangements, trigger events may include[5]:

i. disbursements;
ii. additions to trust assets;
iii. changes in investment strategy for trust assets;
iv. identification of beneficiaries not previously identified;
v. change of domicile of the trust; and
vi. disputes between beneficiaries and fully vesting trust assets.

The triggering events cited above can present opportunities to conduct more in-depth monitoring. Additionally, reviews of the financial records of trust assets can also aid a licensee in its obligation to carry out ongoing monitoring activities.

Red Flags/Warnings Signs: Legal Persons and Legal Arrangements Monitoring

Licensees should be aware of and be able to identify warning signs emanating from transaction monitoring activities that may constitute a red flag. Transaction monitoring of legal persons/arrangements is more effective where licensees understand or are aware of instances that may raise suspicion. Appendix 1 provides a list of potential red flags or warning signs that may emanate from transaction monitoring activities related specifically to legal persons/arrangements and which may require further assessment or filing of a suspicious activity report ("SAR"). While some red flags may appear suspicious on their own, it may be considered that a single red flag may not be a clear indicator of potential misuse of a legal person or legal arrangement for ML/TF/PF activity. However, a combination of these red flags, in addition to

[4] These trigger events should be read in conjunction with the red flags and warning signs examples contained in this guidance and the contents of the AMLTFCOP, including its Explanatory Notes.
[5] These trigger events should be read in conjunction with the red flags and warning signs examples contained in this guidance and contents of AMLTFCOP including its explanatory notes.

analysis of overall financial activity or business profile may provide a clearer indication that the legal person or legal arrangement is being potentially misused for ML/TF/PF activity. These red flags also act as trigger events for a licensee to consider whether additional measures, such as updating CDD or ECDD, are required to forestall any ML, TF or PF risk. These red flags or warning signs should be read in conjunction with those contained in the AMLTFCOP[6] and any issued by the FIA.

To assist staff and ensure the system remains effective, licensees should ensure that their lists of ML/TF/PF red flags/warning signs are continually updated to include new red flags as well as provide further guidance on existing ones, particularly when staff give feedback on a lack of clarity in interpreting these red flags (for example, with regard to the treatment of complex transactions or patterns, classifying higher risk geographies and business activities, or determining whether certain transactions and patterns make economic sense).

Scrutiny and Monitoring: Timing

Transaction monitoring is only effective if it is based on accurate data that can identify changes that may impact a licensee's level of exposure to ML, TF and PF in order for such risks to be effectively addressed in a timely manner. The timing of such monitoring is important, as well as the way in which monitoring is conducted. The integrity of the data used is also critical to ensuring licensees receive meaningful outputs that can be used to drive necessary changes to minimise their risk exposure.

Real Time vs Post Event Monitoring

Real time monitoring focuses on transactions and activities at the point when information or instructions are received and are reviewed during or prior to being actioned. On the other hand, post event monitoring may involve end-of-day, weekly, monthly or annual reviews of customer transactions and activity. Real time monitoring of transactions and activity is generally more effective in reducing a licensee's exposure to ML, TF and PF risk. Post event monitoring may be more effective at identifying unusual patterns. Licensees should incorporate both real time and post event monitoring to ensure they are able to identify any unusual activity in a timely manner.

Manual vs Automated Monitoring

Monitoring may involve manual or automated procedures or both. Automated monitoring procedures may add value to manual procedures by recognising transactions or activity that fall outside set parameters, particularly for licensees with a large number of customers and transactions. However, where automated monitoring procedures are not in place, procedures for manual monitoring should ensure proper checks and balances to minimise human errors, which may lead to ineffective monitoring.

[6] See Explanatory Note (iii) of Section 21 of AMLTFCOP.

Automated monitoring methods may be effective in recognising notable transactions and activity, and business relationships and one-off transactions with persons connected to higher risk jurisdictions, sanctioned countries or territories, or sanctioned persons.

Automated systems that provide outputs like exception reports can provide a simple but effective means of monitoring all transactions to, or from, particular accounts or geographical locations, as well as any activity that falls outside of pre-determined parameters, based on thresholds that reflect a customer's business and risk profile. This could lead to the identification of unusual transactions in a timelier manner. However, defining what constitutes unusual behaviour or transaction patterns is the ultimate responsibility of the licensee and must be determined based on the licensee's understanding of the customer's profile and the ensuing risks.

It is expected that where an automated monitoring approach (group or otherwise) is used, a licensee must understand:

- how the system works and when it is changed;
- its coverage (who or what is monitored and what external data sources are used);
- how to use the system, e.g., making full use of guidance; and
- the nature of its output (exceptions, alerts etc.).

When screening a business relationship (prior and subsequent to establishing that relationship) and transactions, the use of electronic external data sources may also be particularly effective. However, where a licensee uses group screening arrangements, the licensee will need to be satisfied that the group's systems provide adequate mitigation of risks applicable to the VI business. FIA and FSC will be keen to see clear focus on VI business with evidence including how such business risk is mitigated[7].

Implementation of an automated monitoring system does not remove the need for a licensee to remain vigilant and licensees should have regard for the fact that factors such as staff intuition, direct contact with a customer and the ability, through experience, to recognise transactions and activities that do not seem to make sense, cannot be automated.

Automated screening may also lead to issues of fuzzy matches. Therefore, licensees' systems and their understanding of such systems must lead to the ability to:

- understand which business relationships and transaction types are screened;
- understand the system's capacity for fuzzy matching (a technique used to recognise names that do not precisely match a target name but which are still potentially relevant);

[7] It is important that licensees have sufficient records to evidence full account of VI business within any group system.

- set clear procedures for dealing with potential matches, driven by risk considerations rather than resources; and
- record the basis for discounting alerts (e.g., false positives) to provide an audit trail.

The audit trail should enable licensees to review the dates on which screening checks were undertaken and the results of those checks (e.g., the number of false positives), thus allowing them to assess if the system is operating effectively. Where a licensee is part of a wider group and utilises a group-wide screening system, evidence would need to be obtained that such an audit trail exists. A copy of the records made would suffice in this instance.

Licensees should periodically sample the quality of their alerts handling in order to detect and rectify deficient cases, as well as any weaknesses observed in their transaction monitoring systems or processes. This can be achieved through internal testing or independent quality assurance to continually sample alerts handling and test the robustness of these processes.

Irrespective of which manner a licensee uses, the licensee must ensure that the level of testing performed is commensurate with the size of its business, volume of transactions, and nature and complexity of risks faced. It is expected that any findings and issues identified will be mitigated in a timely manner and reviewed by the licensee's board and senior management. Licensees should, therefore, ensure that they have systems available to provide their senior management with an adequate overview and the context of the timeliness and quality of the licensee's transaction monitoring alerts handling and resolution, as well as any remedial measures; and whether these measures effectively mitigate the licensee's ML/TF/PF risks. Records of these measures should be maintained for review by the FSC or FIA as applicable.

Monitoring Data Integrity

Output and effectiveness of a licensee's transaction monitoring system is directly correlated to the quality of its data. Licensees should periodically review the completeness and validity of data used in their transaction monitoring systems, through for instance, the performance of data integrity checks to ensure that data being used is complete (i.e., covers relevant areas for review) and accurate (i.e. information input is accurate, primarily with regard to risk criteria of customers). Where systems include mechanisms such as transaction and other technological codes, licensees should have systems in place to periodically assess and monitor these codes. Further, licensees should have controls in place, such as procedures to conduct trend analyses and generate exception reports to identify where the system is working outside agreed rules or scenarios caused by data integrity issues, so these may be properly assessed. Consideration should be given as to whether root cause analyses should be performed, and the findings and remedial actions escalated to the appropriate senior management.

Licensees should ensure that staff's access rights to their transaction monitoring systems are commensurate with their roles, responsibilities and seniority to safeguard the integrity of data.

While sufficient access must be provided to key staff (e.g. analysts, compliance staff and quality assurance teams) in order to perform their duties effectively, licensees should perform periodic checks on the levels of access being granted and take steps to identify and reduce the number of unauthorised persons or those who no longer require access to the system.

Higher Risk Scenarios and Sanctions Compliance

The risk that a business relationship may be used for concealment of the proceeds of criminal conduct or instrumentalities, or for TF or PF, is elevated where the business relationship or one-off transaction involves a sanctioned person or entity, or a legal person or arrangement connected with a sanctioned person, country or territory or a higher risk jurisdiction for the purpose of ML, TF or PF[8].

To minimise this risk, licensees must comply with all asset-freezing and reporting obligations to prevent funds or other assets being made available, directly or indirectly, for the benefit of a designated person. FATF Recommendations 6 and 7, as implemented in VI legislation, require the implementation of UN TFS "without delay", which should be understood as no more than 24 hours and interpreted in the context of:

- the need to prevent the flight or dissipation of funds or other assets which are linked to TF or PF; and
- the need for global, concerted action to swiftly prevent and disrupt TF and PF flow.

As a part of on-going monitoring procedures, licensees must establish and maintain appropriate policies, procedures and controls to monitor all customer transactions and activity in order to recognise whether any business relationships or one-off transactions are directly or indirectly connected to sanctioned persons, organisations, or other parties.

Licensees must undertake sanctions screening for all business relationships and one-off transactions. This screening must include the customer, any beneficial owners and other associated or connected parties. The screening must be carried out at the time of client take-on, during periodic reviews and when there is a trigger event, e.g., amendments made to the sanctions designations lists.

Effective sanctions compliance may include, but is not limited to:

- having appropriate policies, procedures and controls in place to ensure that the content of targeted financial sanctions notices is reviewed without delay, including screening of customer data against the sanctions designations lists;

[8] Licensees should pay particular attention to higher risk jurisdictions as identified by the VI in its various risk assessments. Higher risk jurisdictions are separated for the purpose of ML, TF and PF as different jurisdictions pose different types of risk, threats and vulnerabilities relative to ML, TF, or PF.

- in the case of an identified positive match, freezing of any accounts, and other funds or economic resources without notice and without delay;
- refraining from dealing with the funds or assets or making them available (directly or indirectly) to such persons unless a license is obtained from the Sanctions Unit; and
- ensuring required sanctions compliance reporting forms are filed as soon as practicable with the Sanctions Unit
- criteria for filing a SAR with the FIA in instances where a breach of sanctions may be suspected/confirmed.

A licensee must ensure its sanctions monitoring system includes an assessment of the effectiveness of its sanctions controls and its compliance with the VI sanctions regime. A record of such assessment should be maintained, and any findings should be appropriately corrected and/or mitigated.

Oversight of Monitoring Functions and Controls

The MLRO/Compliance Officer[9] should have access to, and familiarise him or herself with, the results and output from the licensee's monitoring processes. Such output should be reviewed by the MLRO/Compliance Officer who in turn should report regularly to the board, providing relevant statistics and key performance indicators, together with details of any trends and actions taken where concerns or discrepancies have been identified, as well as any issues that cause elevation of ML, TF or PF risk to the licensee's business.

The board should consider the appropriateness and effectiveness of the licensee's monitoring processes as part of its annual review of the licensee's institutional risk assessments and associated policies, procedures and controls. This should include consideration of the extent and frequency of such monitoring, based on materiality and risk as set out in the institutional risk assessments.

Where a licensee identifies weaknesses within its monitoring arrangements, it should ensure that these are rectified in a timely manner and consideration should be given to notifying the FSC or the FIA as appropriate, where these findings are considered material.

Staff Training

To ensure the quality and consistency of staff assessments of transactions, licensees should periodically provide staff with training on identifying suspicious activities, the institution's policies and procedures for transaction monitoring and how to communicate and identify any anomalies found within the customer profile as a result of transaction monitoring. Training should include,

[9] Responsibilities of the MLRO and Compliance Office must be clearly delineated within the organisation where the functions are separately performed.

amongst other things, any updates to ML/TF/PF red flags, and current risk understanding, and any new or emerging ML/TF/PF trends or typologies.

Licensees should also ensure that training is commensurate with the specific tasks assigned to staff and the risks faced based on specific functions (i.e. one module for all staff may not be appropriate). Senior management should also receive specified training, including with respect to their oversight and approval functions. Training attendance should be tracked and enforced. A testing element should also be included.

Licensees must also consider how to incorporate transaction monitoring and other ML/TF/PF metrics into performance indicators to drive staff ownership and accountability of the process.

Understanding what to do when a transaction is suspicious

Where transactions are identified as having sufficient grounds for suspicion of ML, TF or PF, licensees are required to file SARs with the FIA. Such reports must be filed in a timely manner using the prescribed form as contained on the FIA website. Internal processes must not unduly delay the prompt filing of SARs.

Where a licensee identifies suspicious activities in relation to a customer's accounts or transactions, in addition to filing a SAR, should the licensee decide to retain the relationship, it should ensure that appropriate enhanced measures are taken to manage the risks of these accounts being abused for ML/TF/PF purposes. These enhanced measures include subjecting the accounts to increased scrutiny, obtaining compliance and/or senior management approvals prior to executing further transactions, and reviewing the risk classification and/or further business relations with the customer. These actions would be in keeping with ECDD requirements; licensees must, therefore, consider the Guidance on ECDD. It is also important that licensees pay particular attention to any obligations to, or ongoing cooperation they have with relevant competent authorities or law enforcement agencies, including having regard to the obligation not to tip-off the customer.

Transaction Monitoring: Customers Via Introduced Business

Licensees' transaction monitoring procedures must cover all customers including those introduced through third parties. Therefore, licensees' systems must account for the unique nature and elevated ML, TF and PF risk of business related to third party introducers. Licensees should incorporate the Guidance on Mitigating the Risk with Introduced Business within their transaction monitoring system. For example, it is important that TCSPs, based on the risk of introduced business, appropriately monitor and test that their introducers employ effective monitoring systems in place and those monitoring systems are consistent and collaborative with their own transaction monitoring systems to ensure they are able to accurately identify the risks associated with the clients introduced by these third parties.

Key Takeaways

An effective transaction monitoring system is essential for licensees to detect and report suspicious transactions in a timely and effective manner and take appropriate steps to mitigate the associated ML/TF/PF risks. Licensees should prioritise transaction monitoring and embed it into their organisational wide culture, including through ensuring a strong tone is set from senior management and the Board about its importance.

Licensees are encouraged to consider the use of new technology and data analytics to improve their transaction monitoring effectiveness. Licensees must be able to demonstrate that the systems employed are effective and that data inputted into the system is appropriate and leads to the desired result of identifying suspicious activities or activities outside the normal behavior of a customer.

Licensees should ensure that they review section 21 of the AMLTFCOP and the accompanying Explanatory Notes in their entirety. The FSC and the FIA will be assessing compliance with the requirements of section 21 of the AMLTFCOP on an ongoing basis.

Overarching Requirement for Compliance

Licensees 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 resulting risks, licensees 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. Licensees must remain agile and embed systems to allow for continual improvement in the efficiency and effectiveness of their AML/CFT/CPF compliance.

Table of Abbreviations and Acronyms

AML/CFT/CPF	Anti-money laundering, countering financing of terrorism and countering proliferation financing
AML/CFT supervisors	Financial Services Commission and Financial Investigation Agency
AMLTFCOP	Anti-Money Laundering and Terrorist Financing Code of Practice
AML Regulations	Anti-Money Laundering Regulations
CDD	Customer due diligence
DNFBPs	Designated Non-Financial Businesses and Professions
ECDD	Enhanced Customer Due Diligence
EU	European Union
FATF	Financial Action Task Force
FIA	Financial Investigation Agency
FIs	Financial Institutions
FSC	Financial Services Commission
IRA	Institutional Risk Assessment
Licensees	Financial Institutions and Designated Non-Financial Businesses and Professions
ML	Money laundering
PEP	Politically exposed person
PF	Proliferation financing
RAF	Risk Assessment Framework
RBA	Risk-based approach
SAR	Suspicious activity report
SoF	Source of funds
SoW	Source of wealth
STR	Suspicious transaction report
TF	Terrorism financing
TFS	Targeted Financial Sanctions
UN	United Nations
UNSC	United Nations Security Council

Appendix 1

Transaction Monitoring Warning Signs/Red Flags

Legal Person/Arrangement

Customer Behavior:

- When a legal person/arrangement or its beneficial owner or any of its associated natural persons or transactions originate from a high-risk jurisdiction where the FATF has called for countermeasures or enhanced client due diligence measures, or a jurisdiction known to have inadequate measures to prevent money laundering, the financing of terrorism and proliferation financing.
- The legal person/arrangement is associated with terrorism activities, or the legal person has been declared a designated person under UN, UK or other relevant VI sanctions regimes.
- Any associated natural person of the legal person/arrangement is designated under UN, UK or other relevant VI sanctions regimes.
- An employee, director, signatory, and/or beneficial owner of the person/arrangement is unusually concerned with the reporting threshold or AML /CFT/CPF policies.
- The legal person/arrangement is linked to negative/adverse news or criminal activity (e.g., named in a news report on a crime committed or under Law Enforcement investigation/inquiry).
- The legal person/arrangement or any of its associated natural persons/entities are found to be a positive match while screening against sanctions listings relative to UN Security Council Resolutions (UNSCRs) for TF and PF.
- The legal person/arrangement attempts to establish a business relationship but fails to provide adequate documentary proof regarding its beneficial ownership details to the satisfaction of the Financial Institution or DNFBP.
- The legal person/arrangement is part of a complex structure that is not commensurate with the nature of business activities of the legal person/arrangement.
- The legal person/arrangement is consistently invoiced by organisations located in a jurisdiction that does not have adequate AML/CFT/CPF laws.
- The legal person/arrangement's beneficial owners, shareholders or directors are also listed as beneficial owners, shareholders or directors in multiple other companies.
- Unexplained use of nominee shareholder arrangements.
- Directors acting on instructions of others who may not be disclosed.

Transactional Patterns:

- Transactions that are not consistent with the usual business profile of the legal person/arrangement:
    - transactions that appear to be beyond the means of the legal person/arrangement based on its nature of business or declared business profile,
    - transactions that appear to be above the usual amount, based on the nature of business in which the legal person/arrangement is involved.
- Frequent/multiple transactions involving entities with the same beneficial owner with no or little economic value.
- The legal person/arrangement is engaged in a business that is not normally cash-intensive but appears to have substantial amounts of cash transactions.
- The legal person/arrangement deliberately avoids traditional banking services without legitimate reasons for doing so.
- The legal person/arrangement's transactions are structured to avoid reporting threshold requirements.
- Large or frequent cash-based transactions occur, which are not commensurate with the stated business profile/activities of the legal person/arrangement.
- Numerous small transactions by a legal person/arrangement, especially over a short period, but taken together are material and do not match the transactional pattern of the legal person/arrangement's declared business profile.
- Export/Import proceeds and other receipts and payments to/from unrelated counterparties, which are not in line with the legal person/arrangement's business nature.
- No clear relationships between connected companies or transactional counterparties of the legal person/arrangement.
- Proceeds received from, or payments sent to, an unrelated foreign buyer against which no export shipments were sent or no imports were received.
- Proceeds received/sent against under- or overvalued invoices of goods exported/imported.
- The legal person/arrangement has demonstrated a long period of inactivity post incorporation, followed by a sudden and unexplained increase in financial activities.
- The legal person/arrangement is registered at an address that does not match the profile of the entity.
- The legal person/arrangement is registered at an address that cannot be located on internet mapping services (such as Google Maps).
- Directors, shareholders, beneficial owners and connected persons demonstrate limited business acumen despite substantial interests in the legal person/arrangement.
- The legal person/arrangement describes themself as a commercial business but cannot be found on the internet or social business network platforms (such as LinkedIn, Facebook, X, etc.).

- The legal person/arrangement is registered under a name that does not indicate the activity of the company.
- The legal person/arrangement is registered under a name that indicates that the legal person/arrangement performs activities or services that it does not provide.
- The legal person/arrangement is registered under a name that appears to mimic the name of other companies, particularly high-profile multinational corporations.
- The legal person/arrangement has an unusually large number of beneficiaries and other controllers without any clear rationale.
- The legal person/arrangement has authorised numerous signatories without sufficient explanation or business justification.
- Directors or controlling shareholder(s) do not appear to have an active role in the legal person/arrangement without clear justification.
- The legal person/arrangement receives large sums of capital funding quickly following incorporation/formation, which is spent or transferred elsewhere in a short period of time without commercial justification.
- The legal person/arrangement maintains a bank balance of close to zero, despite frequent incoming and outgoing transactions.
- Unexplained use of powers of attorney by the legal person/arrangement.

<u>Legal Arrangements</u>

- Unexplained use of express trusts, and/or incongruous or unexplained relationships between beneficiaries and the settlor.
- Unexplained or incongruous classes of beneficiaries in a trust.
- There is a discrepancy between the supposed wealth of the settlor and the object of the settlement.