Guidance

Effective Enhanced Customer Due Diligence Measures

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), Money Service Businesses ("MSBs");
(vi) Insolvency Services; and
(vii) Virtual Asset Service Providers ("VASPs").

The FIA is responsible for the supervision and monitoring of designated non-financial businesses and professions in the VI:

(i) Legal Practitioners, Notaries Public and Accountants;
(ii) Real Estate Agents;
(iii) Dealers in Precious Metals and Stones ("DPMS");
(iv) High Value Goods Dealers ("HVGD");
(v) Vehicle Dealers; and
(vi) 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 supervised entities 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 both FIs and DNFBPs to ensure proper risk mitigation and enhance transparency, while maintaining the VI's reputation as a place to conduct legitimate and quality business.

These Guidelines have been developed for the benefit of assisting FIs and DNFBPs in the implementation of a risk-based approach for applying measures to mitigate against ML, TF, and PF risks related to higher risk business. 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 ("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.

Comprehensive AML/CFT/CPF compliance by FIs and DNFBPs is essential to remain up-to-date with evolving risks and threats that could adversely impact operations and compliance. 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

The requirement to conduct customer due diligence (CDD) procedures on customers is an obligation that falls to all FIs and DNFBPs that are subject to the AML Regulations and the supervisory regimes of the FSC and FIA. All licensees have obligations to comply with AML/CFT/CPF laws and regulations. These legal requirements are primarily derived from the international standards developed by the Financial Action Task Force (FATF) and are promulgated globally.

Engagement with customers is one aspect of a licensee's operations that can expose it to risks. These risks include exposure to the ethically challenged who may seek to use the services and/or products offered by a firm or entity for ML, TF and PF purposes. As a mitigating measure in response to these risks, licensees must ensure that they conduct CDD measures. CDD is the process through which you develop an understanding of your customers and the ML, TF and PF risks they pose to your business.

In the VI, the requirement to conduct CDD is captured in the AMLTFCOP and the AML Regulations. The primary requirements for effecting due diligence measures can be found in Part III of the AMLTFCOP. As part of standard CDD, licensees must obtain sufficient information to accurately identify and verify that their customers are who they say they are and to assess the ML, TF, PF and sanctions evasion risks posed by the customer. The risk assessment then further informs the type of due diligence that should ultimately be conducted on the customer. In the case of customers presenting higher risks, licensees must conduct enhanced customer due diligence (ECDD), which is the focus of these Guidelines.

These Guidelines seek to assist FIs and DNFBPs in distinguishing between standard or low risk situations and higher risk customers and situations, which require that ECDD be conducted, and have been developed to provide clarity on what is required of licensees to implement effective ECDD procedures and controls.

Licensees must ensure that their compliance procedures provide a clear and differentiated approach between ECDD and CDD and in some cases simplified CDD (SCDD) where lower risks are identified. This includes providing examples of cases where ECDD must be conducted. Additionally, a well-written compliance manual should also provide for flexibility in the approaches for conducting SCDD, CDD and ECDD. In conducting ECDD, it is important that licensees implement more robust measures when obtaining and verifying information. This is particularly important in relation to verifying the Source of Wealth (SoW) and Source of Funds (SoF) for a higher risk customer.

REQUIREMENT TO CONDUCT ENHANCED CUSTOMER DUE DILIGENCE

The AMLTFCOP sets out ECDD as supplementary measures required to be undertaken for CDD purposes when a licensee is dealing with *"an applicant for business or a customer in relation to a business relationship or one-off transaction in order to forestall and prevent the higher risk of money laundering, terrorist financing, proliferation financing and other financial crime that have been identified by the entity or professional."*[1] Box 1 below details the Explanatory Note of Section 20 of the AMLTFCOP which provides examples of these measures.

Box 1 - Explanatory notes following section 20 of the AMLTFCOP

(i) Enhanced customer due diligence (ECDD) must be viewed as an additional precautionary measure designed to assist in truly identifying an applicant for business or customer (including a beneficial owner) and verifying the information relating to it or him or her and ensuring that the risks that may be associated with the customer are minimal or manageable; this is in addition to ensuring that the source of funds or wealth is legitimate. These additional measures are relative to what an entity or a professional is already required to undertake for CDD. However, the type of ECDD applied in high-risk scenarios will differ on a case-by-case basis, taking into account the higher ML/TF risk, the particular circumstances of the customer, and the measures that will enable them to manage and mitigate the higher ML/TF risks presented.

(ii) Examples of ECDD measures that could be applied for high-risk business relationships include

- obtaining additional information on the applicant for business or customer (e.g. volume of assets, information available through public databases, internet, etc.);
- requiring additional information from the applicant for business or customer to gain a deeper understanding of the applicant's or customer's activities;

[1] Section 20(1) Anti-money Laundering and Terrorist Financing Code of Practice

- undertaking further research, where considered necessary, in order to understand the background of the applicant for business or customer and its or his or her business and verify such information;
- obtaining additional information on the source of funds or source of wealth of the applicant for business or customer and verifying this information (i.e. obtaining more than standard information on source of funds and source of wealth, including requiring evidentiary documentation to confirm the customer's source of funds and wealth, and verifying information provided against publicly available information sources);
- obtaining the approval of senior management to commence or continue the business relationship with a higher risk applicant for business or customer;
- requiring additional information before effecting transactions above an established threshold amount;
- requiring senior management sign-off when engaging in transactions with a higher risk applicant for business or customer;
- requiring the first payment to be carried out through an account in the applicant for business' or customer's name with a bank or similar financial institution subject to anti-money laundering, terrorist financing and proliferation financing requirements that are consistent with the FATF Recommendations and are supervised for compliance with such requirements; and
- conducting enhanced monitoring of the business relationship (e.g. increasing the number and timing of controls applied, obtaining information on the reasons for a particular transaction, selecting patterns of transactions that need further examination).

(iii) Where an existing customer is subsequently assessed by a customer risk assessment review as posing a higher ML/FT risk, the AML/CFT measures must be heightened and ECDD measures must be conducted immediately after the customer (or beneficial owner) has been determined to be high risk.

EXAMPLES OF CHALLENGES ENCOUNTERED BY LICENSEES THAT MAY IMPEDE EFFECTIVE ENHANCED CUSTOMER DUE DILIGENCE

Licensees may encounter various challenges that affect the effective implementation of ECDD measures. The following illustrates common issues that may impact the thorough assessment of customer risk and adherence to compliance obligations.

Lack of material differentiation between customer due diligence and ECDD

A significant challenge to applying ECDD is the lack of material differentiation between standard CDD and ECDD. This lack of differentiation impacts the documents to be obtained and/or the procedures to be followed. Where compliance procedures leave minimal scope for an understandably different requirement for high-risk customers, a licensee runs the risk of not carrying out ECDD when required. This failure is also compounded where staff are not clear on the different elements needed when undertaking standard CDD as opposed to ECDD.

Identifying the cause of a lack of differentiated approach and rectifying it is essential for a licensee to mitigate its risk and demonstrate compliance to the FSC or FIA as the case may be. For example, a compliance manual may require two forms of government issued identification for all customers, irrespective of the outcome of risk assessment. However, one example of a differentiated approach could be to require one form of government issued identification for customers subjected to standard CDD, and two forms of government issued identification for those customers subjected to ECDD (i.e. higher risk customers).

Where a licensee has identified procedural or implementation issues with its level of documentation for standard CDD versus ECDD it is recommended that it carry out a comprehensive review of its processes and procedures relating to due diligence. This review should assess the adequacy of these processes and procedures with the objective of ensuring ECDD measures are effective, including identifying and verifying higher risk customers and monitoring such customers. In these cases, particularly where the root cause may be more difficult to detect, it may be useful to conduct an internal audit of the due diligence procedures and mechanisms to identify underlying cause(s). Ultimately, licensees should have a clear differentiation on the due diligence requirements for all tiers of risk assessed customers.

Licensees do not properly implement their Risk Assessment Framework

A licensee must have a robust Risk Assessment Framework (RAF) to properly implement its due diligence measures. The risk assessment process is integral to the conduct of financial services business and mitigating the risks of ML, TF and PF. A component of that business is the customer relationship process and how it is managed to mitigate these risks.

Risk assessments identify customers' risk levels, including where elevated risks exist. They also inform how CDD measures should be aligned according to that risk. Customers that present a medium or lower level of risk would be subject to a standard or simplified CDD process as the case may warrant. However, SCDD measures are not applied if the licensee suspects ML, TF or PF risk. Where customers are identified as high risk, ECDD must be applied. Section 20 of AMLTFCOP provides that the following scenarios present higher risk and therefore ECDD must be performed:

- A customer identified as a foreign Politically Exposed Person (PEP);
- a domestic PEP, or an international organisation PEP that presents a higher risk;
- a business activity, ownership structure, anticipated, or volume or type of transaction that is complex or unusual, having regard to the risk profile of the applicant for business or customer, or where the business activity involves an unusual pattern of transactions or does not demonstrate any apparent or visible economic or lawful purpose;
- a person, business relationship or transaction located in or from a country that is either considered or identified as a high-risk country (including a country identified as having higher risk by the FATF) or that has international sanctions, embargos or other restrictions imposed on it; or
- any other situation that may present a higher risk of money laundering, terrorist financing or proliferation financing;

Likewise, licensees' risk assessments should account for non-face to face relationships as these may also present a high level of risk and may require ECDD for identifying and verifying the customer in accordance with section 29 of the AMLTFCOP, including having regard to customers or business relationships or transactions located in countries that have international sanctions, embargos or other restrictions.

Deficient risk assessments that lead to improperly applied due diligence measures can also impact on the frequency and depth of transaction monitoring, updating of due diligence information and other compliance measures informed by the results of risk assessments. The cascading effect of an inadequate risk assessment on the applied compliance measures can expose a licensee to threats of ML, TF and PF.

Insufficient or no verification of due diligence information and customer

Due diligence procedures should consist of two parts: identification and verification of the identification information provided. For the due diligence process to be effective, it is essential to also ensure that verification of the due diligence subject is carried out. Verification of the customer is a vital step to validate the identity of the customer, including its beneficial owner, and ensure that the customer is, in fact, the person with whom the licensee is engaging in business with. The potential of a customer being used as a 'straw man'[2] to obscure true control behind a financial service or product is a risk. Risk also emanates from the possibility of nominee arrangements and persons acting on behalf of others. The risk that a licensee has not effectively enquired into the true beneficial owner and/or controller, is a material risk that could stem from sufficient ECDD measures not being employed in such instances.

No verification of Source of Wealth and Source of Funds of a customer

Licensees are required to take appropriate steps to verify the SoW and SoF for customers. This verification should seek to satisfy the licensee that SoW and/or SoF are not the proceeds of illicit financing activities. ECDD may be required to determine SoW and SoF for a customer who may not be rated high risk but is involved in a higher risk transaction. In these cases, the source of the customer's wealth as well as the origin of the funds being used for the transaction should be sought, verified and documented. Transactions that are outside the norm for a customer, including cases where the transactions are large compared to the person's wealth, should trigger a review of the customer and transaction to ensure that the transaction does not pose any additional ML, TF or PF risk.

Monitoring and Reassessing existing customers

Licensees must engage in ongoing monitoring of existing clients and be in a position to identify in a timely manner when the risk profile of a customer changes. Such changes may lead to the need to conduct ECDD on a customer previously assessed as lower risk. Likewise, it may lead to declassification of a higher risk person to a lower category.

Ongoing monitoring of existing customers may include the following:

- scrutinising transactions undertaken by the customer for the purpose of making an assessment of consistency between the transactions undertaken, the customer's business and risk profile including the source of funds;
- screening all customers to identify those that may present a higher risk, including customers that have become PEPs, are subject to applicable sanctions or are associated with criminal activities; and
- reviewing and updating CDD information of customers.

[2] Concealment of Beneficial Ownership published by FATF and The EGMONT Group - https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/FATF-Egmont-Concealment-beneficial-ownership.pdf

Information obtained during the ongoing monitoring process may trigger the need to amend the customer's risk assessment, including the need to carry out ECDD. Some examples of triggering events include the following:

- a customer becomes a PEP;
- a customer that engages a licensee to conduct a complex, unusually large transaction or unusual pattern of transactions that have no apparent or visible economic benefit or lawful purpose;
- a customer that seeks nominee shareholder services without a clear and rational reason that is in line with their business activities;
- a customer that is engaged in businesses utilising technologies that enhance anonymity, or new and developing technologies that leverage 'mixing' services that can obscure beneficial ownership and control;
- additional information obtained from the customer in relation to a transaction does not provide a logical explanation for the purpose of the transaction;
- monitoring of a customer's circumstances reveals that they have participated in a Citizenship by Investment Scheme[3] or other similar programme which was not disclosed to the licensee;
- involvement of a dual-purpose good within the customer's business operations which was not disclosed to the licensee;
- a customer applying to open a new account, requesting new products/ service or establishing a new relationship;
- a customer changing its geographic location or requesting services from a new geographic location;
- a material change in ownership and / or management structure;
- a customer becoming a PEP, the subject of a sanctions list, or associated with criminal behaviour.

Illustration – Citizenship by Investment Programmes

Many countries have introduced Citizenship by Investment Programmes and Residency by Investment Programmes as a means to generating revenue. However, these programmes can create risks that are relevant to licensees.

John has been a customer of licensee A since 2016. Initial due diligence evidences that John is a citizen of Country Z which is not a high risk country for ML, TF or PF. The initial risk assessment resulted in the customer being risk scored as medium risk. In a recent review conducted as a part of licensee A's ongoing monitoring, it was revealed that John has also been a citizen of Country X since Nov 2023 via a Citizenship by Investment Programme. A report issued by the OECD on the Misuse of Citizenship and Residency by Investment Programmes notes that there are a number of potential risks associated with these schemes. Risks include fraud, corruption, tax evasion, foreign bribery and other financial crimes. Licensee A reviews the findings from ongoing due diligence in 2024 and notes the following:

- John's name is reflected differently in travel documents issued by Country X.
- John holds a diplomatic passport issued by Country X.

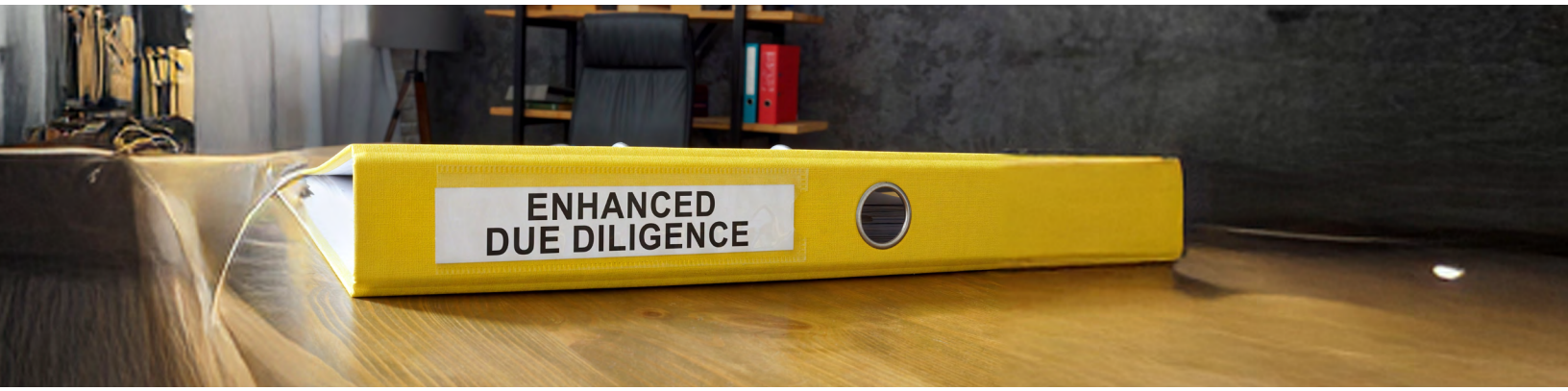
The Licensee A's initial risk assessment must be updated and consideration of ECDD to be undertaken.

[3]The FATF has published a report on the Misuse of Citizenship and Residency by Investment Programmes that may present heightened risks. A copy of the report can be found at https://www.fatf-gafi.org/en/publications/Methodsandtrends/misuse-CBI-RBI-programmes.html

Enhanced Customer Due Diligence controls are not geared towards the risks presented

Licensees should consider the ML, TF and PF risks presented by their customers as they develop their ECDD policies, procedures and controls. There is no standard procedure or set of documents to be requested when ECDD is required to be carried out. The ECDD process depends on each particular situation and should be appropriately tailored to manage the specific risks emanating from the higher risk customer, transaction or situation, as the case may be.

Licensees' ECDD policies, procedures and controls must have regard and due consideration of any findings from the licensee's institutional risk assessment and customer risk assessments, which in alignment with section 12 of the AMLTFCOP would allow the Licensee to "develop, establish and maintain appropriate ML, TF and PF Controls".



ENHANCED CUSTOMER DUE DILIGENCE AND BENEFICIAL OWNERSHIP

A core requirement of CDD and ECDD is to identify and verify customers' beneficial ownership arrangements to ensure that such arrangements are understood. It is crucial to know who the beneficial owner(s) are so that appropriate decisions can be made about the level of ML, TF and PF risk presented by the customer. Additionally, it is also required to identify and verify the identity of each director of the customer or any similar position responsible for the management of the customer.

Licensees wanting to do business with a customer that is not a natural person must identify and verify the identity of the beneficial owner(s) and should establish and understand the customer's ownership structure at each layer. In such cases, the beneficial owner may not necessarily be one individual as there may be several beneficial owners within the ownership structure. Where there are complex ownership layers with no reasonable explanation, licensees should consider the possibility that the structure is being used to hide the beneficial owner(s). In any event, under circumstances where such ownership structures exist the AMLTFCOP requires the licensee to conduct ECDD.

COUNTRIES WITH INSUFFICIENT AML/CFT MEASURES

If a customer is non-resident in the VI and from a country with insufficient AML/CFT/CPF measures and/or higher ML, TF or PF risks, ECDD must be undertaken. Such countries would include a country identified as being of higher risk by the FATF, CFATF or similar bodies. To determine which countries have insufficient AML/CFT/CPF measures in place, licensees should refer to the guidance in the AMLTFCOP, as well as other guidance material such as those published by the FIA, CFATF and the FATF and any updates published on the FSC or FIA websites. A country that is subject to an FATF call for action must always be considered a country with insufficient AML/CFT/CPF systems or measures in place.

ENHANCED CUSTOMER DUE DILIGENCE - NEW, DEVELOPING OR EMERGING TECHNOLOGIES OR PRODUCTS

New or developing technologies or products can present unknown ML, TF or PF risks and vulnerabilities, and new methods of delivery may be able to bypass existing AML/CFT/CPF measures to allow anonymity. Licensees' risk assessments should consider whether their business is, or may be, exposed to customers involved in new or developing technologies or products. Compliance programmes should then detail the procedures, policies, and controls that the licensee will implement for this type of customer and technology, including the implementation of ECDD measures.

Where a licensee has a customer who wants to establish a business relationship or conduct an occasional transaction or activity involving new or developing technology or products that might favour anonymity, it must take additional ECDD measures to mitigate and manage any potential ML, TF or PF risks. It is for the licensee to determine what measures are required according to the level of risk involved.

Where a licensee itself is introducing a new or developing technology or a new or developing product (including a new delivery mechanism), there is an explicit requirement for the licensee's risk assessment to be updated before doing so. This ensures that any new or evolving risks are fully examined, with mitigating steps taken as required before the new or developing technology or product is launched and offered to customers. This is required to minimise any potential risk that may arise by the uptake of these products or technology by the customer. Note that in practice, these steps should align with existing procedures, policies and controls to keep licensees' risk assessments (and in turn AML/CFT/CPF programme) up to date.

ENHANCED CUSTOMER DUE DILIGENCE – SOURCE OF WEALTH AND SOURCE OF FUNDS

An important measure of understanding a customer or an applicant for business is to obtain and verify information on SoW and SoF as part of the CDD process. This becomes particularly important during the ECDD process where a customer or applicant for business presents a higher level of risk. It is, therefore, important for licensees to understand and implement a differentiated approach to collecting and assessing SoW and SoF information. For ECDD, obtaining additional information on SoW and SoF is an additional measure that should implemented for higher risk business relationship and customers.

A customer's SoW is the origin and accumulation of their total asset portfolio. This information gives an indication of the amount of wealth a customer has built up and a snapshot of how they acquired it.

A customer's SoF is more narrowly focused. It is the origin of the funds used for the transactions or activities that occur within their business relationship with the licensee. This also applies for an occasional transaction or activity.

Obtaining and Verifying Information About Source of Wealth and/or Source of Funds

Licensees should ask customers to provide them with information about their SoW and/or SoF and record this information. Reasonable steps should be taken, according to the level of risk involved, to verify this information using reliable and independent sources.

Where a licensee identifies that the origin of a corporate customer's funds or wealth has come from their beneficial owner(s), it may be necessary, according to the level of risk involved, for the licensee to extend its level of verification to include the SoW and/or SoF of these persons.

Determining Source of Wealth

Licensees may be able to use publicly available information on the internet, or other commercially available databases to help verify information about SoW and SoF. However, in many situations, it will be necessary for the customer to provide documents issued by third parties that provide verification about the customer's SoW. In higher risk circumstances, it may be necessary to seek further information, either from the customer or directly from the relevant third party issuing the document related to the customer's SoW.

Licensees must develop an understanding of the size and nature of their customers' overall wealth and, importantly, how it was acquired. This does not require verification of their entire financial history or identification of every asset held, as they may have multiple income streams and assets.

However, it may be useful to establish the different categories of income or assets that make up their total wealth. Examples could include investments, inheritance, salary, family income or different types of commercial activity. Where there are multiple categories or income streams, licensees should prioritise verification on the more substantial ones, as well as those that are the most complex or obfuscated.

Determining Source of Funds

Verifying the source of customers funds should be a more granular process. The information, data, or documents used should be specific to the business relationship or to the customer's activities and transaction history. Licensees should be mindful that such verification procedures are also necessary in relation to an occasional transaction or activity that may be conducted for a customer.

Documents to Verify Source of Wealth and Source of Funds

When a licensee verifies SoW and/or SoF information, it should use data or documents issued by a credible and reliable source such as a multi-national company, a reputable third-party commercial provider, or a government department from a low-risk country with sufficient AML/CFT/CPF measures.

The types of data and documents used for verification will vary depending on the circumstances and the information that the customer provides. The following documents, data, or information could be considered reliable and independent:

- Government-issued or registered documents or data;
- Bank and other investment statements;
- Payslip or wage slip or other documents confirming salary;
- Inheritance (stamped grant of probate, stamped grant of letters of administration);
- Audited financial statements;
- Evidence of source of wealth (e.g. bill of sale or receipt from sale of property);
- Letter from an agent of the customer confirming they have knowledge of and established business relationships with the customer;
- A copy of a will; and
- Sales and purchase agreements.

For customers who conduct business activities with licensees there should be a range of documents that can be used to verify how funds have been acquired. Depending on the type of business, this could include contractual agreements, sales and purchase records or import and export related documents for the shipment of goods.

Documentation accepted to verify SoW or SoF should depend on the level of ML, TF or PF risk presented by the customer. The higher the risk, the more comprehensive and reliable the documents obtained should be. For instance, it would be expected for certified copies or originals to be sighted, or verification carried out via other reliable measures such as disclosure registers, for higher risk customers.

CONDUCTING EFFECTIVE ENHANCED CUSTOMER DUE DILIGENCE – SOME HELPFUL TIPS

Licensees may wish to consider the following steps in their review and revision of their due diligence measures to ensure an effective conduct of ECDD.

1. Establish and update AML/CFT/CPF compliance procedures to outline the steps to take to implement and maintain an effective CDD regime, which includes ECDD. These procedures should embed sufficient flexibility and detail to be clear on the different approaches that can be taken. The use of case studies within manuals can also add depth and context for a variety of issues that can be presented during the client onboarding process, as well as for ongoing monitoring.

2. Ensure that customer onboarding processes have sufficient depth to collect information that provides customer identification details as well as other particulars that evidence residence, SoF, SoW, citizenship, employment and/or appointments, business connections, related parties (particularly where they may result in the customer being a PEP), exposure to sanctions and financial soundness. The customer onboarding process should also cover risks of criminality (whether current or past convictions) and use of dual-purpose goods.

3. Ensure that the risk assessment methodology and framework is properly calibrated to assess customer risk, which will inform the level of due diligence to be conducted. Further, with reference to the guidance/explanatory notes accompanying section 12 of the AMLTFCOP, a Licensee's risk assessment tool should consider key risk aspects of a business relationship, inclusive of "risks associated with the customer's business or activity, customer's reputation, customer's geographic exposure and delivery channel risk factors."

4. Ensure that customers triggering ECDD are subject to annual review and sign-off by senior management (which has an oversight role in the operations and may include a member of the Board of Directors).

5. Conduct ECDD for any person acting on behalf of a customer, such as in the case of a Power of Attorney or other arrangement. This person must also be subject to verification procedures to determine the veracity of their ability to act and verify that they are not acting on behalf of an unknown person.

6. Updating information connected to a customer that triggers ECDD should be tailored to ensure that there is:

(i) sufficient lead-time to obtain any information required and to review that information;

(ii) reduce friction in collecting additional information by coordinating compliance efforts between operations / client-facing functions and compliance.

7. Train staff to recognise what additional information is needed for ECDD.

8. Ensure that the ongoing monitoring for existing customers allows for the prompt identification of new risks, threats or vulnerabilities that would elevate a customer to a high-risk rating and that procedures support the collection of ECDD without delay. The ongoing monitoring process should also cover a customer's account activity and transaction behaviour (which includes non-cash transactions).

9. Ensure continuous testing of due diligence measures to ensure that the compliance measures in place provide a high level of effectiveness and accuracy.

ENHANCED CUSTOMER DUE DILIGENCE - TREATMENT OF POLITICALLY EXPOSED PERSONS

PEPs must always be subject to ECDD, having been identified as persons of higher risk, as required by the AMLTFCOP (sections 20 and 22 of the AMLTFCOP refer). In order to ensure that licensees are aware of whether any customers are, or have become PEPs, it is essential to have documented procedures for onboarding and monitoring that would enable a licensee to identify PEPs. The definition of PEPs also includes close associates and relatives.

Based on the inherent risks associated with PEPs (and other high-risk customers) licensees may wish to consider the following actions to buttress ECDD measures:

- assessment of the customer to obtain reasonable assurance that SoW and/or SoF were not derived from corrupt practices;
- whether the nature of services or products being provided by the licensee is in line with expected business being conducted by the customer;
- enhanced ongoing monitoring should be sufficiently robust to identify any unexplained changes to the customer's details or circumstances within a reasonable timeframe; and
- determination of whether a PEP has obtained a diplomatic passport in addition to other government issued identification documents.

Furthermore, licensees may also wish to ensure they address and/or answer the following questions to ensure they fully understand the risks posed by PEPs:

- Is the PEP's transaction/activity in line with expectations?
- Is the PEP's identity data, address, employment, SoW or SoF and relatives and close associates' status up to date?
- Are there any unexplained changes to the PEP's details?
- If the PEP's net worth has grown substantially in a short amount of time, does the licensee have a clear explanation for the sudden growth?
- Has the licensee sought clarification from the PEP where necessary and updated their details?

While the above represents suggested measures licensees can take, licensees can employ other measures that enable them to properly carry out ongoing monitoring of their customers. Such measures must be properly recorded and monitored for effectiveness.

Illustration – Classification of a Politically Exposed Person

The licensee's customer – Francois – is an EU citizen. The licensee has had a business relationship with Francois since 2015. Due diligence information has been collected and the services being rendered by the licensee involves a BVIBC, which includes an ownership structure with a legal entity that was incorporated in an EU country. The licensee also acts as nominee shareholder and provides directors for the BVIBC. Based on aggregate details when risk assessed, Francois received a low risk score. The ultimate beneficial owner of the BVIBC is Francois holding majority ownership (91%). A close business associate – Charlie – holds minority ownership (9%).

In 2021, Francois was appointed Mayor of City X in EU Country Y. Francois appointed Charlie as his Chief of Staff. In 2024 Charlie was arrested and charged with bribery and money laundering for granting contracts in return for a fee.

The licensee immediately filed a SAR with the FIA and commenced an internal audit of its customer risk assessment processes and procedures. The licensee's findings were as follows:

- Though a customer risk assessment update was completed in 2022 the licensee failed to identify the change in status of Charlie;
- Francois was identified as a PEP during the customer risk assessment update but no ECDD was undertaken in this regard;
- Records of due diligence searches undertaken in 2022 during the customer risk assessment update provided a result which indicated the political appointments of both Charlie and Francois;
- Due to failures in the customer risk assessment the licensee did not conduct ECDD on Francois and Charlie; and
- Deficiencies in the ongoing monitoring processes, procedures and controls for clients were identified.

Some lessons to learn from the case:

- Ensure proper understanding of the definition of a PEP. For example, in the case of Charlie, his relationship with Francois should have also triggered a consideration as to whether he was a PEP at the time Francois was appointed Mayor;
- Ensure proper training of staff to identify where circumstances change that may require updating customer risk assessments ;
- Ensure proper and effective ongoing monitoring of customer; and
- Ensure proper and effective policies, procedures and controls related to ECDD.

ENHANCED CUSTOMER DUE DILIGENCE AND FILING OF SUSPICIOUS ACTIVITY REPORTS

In the course of business, a licensee may detect suspicious behaviour within its customer base that could be indicative of ML, TF, PF or other illicit financing activities. Where in the conduct of its business the licensee identifies activities or has a suspicion of ML, TF or PF the licensee must file a report with the FIA. In the conduct of both CDD and ECDD, there are several suspicious activities that may trigger internal reporting and also lead to filing an SAR with the FIA. These include, for example:

- transactions and/or activities that are not in line with the licensee's expectations for the customer;
- unexplained increases in wealth or liquid assets for which the customer cannot provide a reasonable and verifiable explanation; and
- ongoing monitoring of a customer reveals activities that suggest ML, TF or PF may be occurring.

All licensees are guided to consider the above, as well as the provisions set out in Part III of the AMLTFCOP, and the Explanatory Notes following section 20 of AMLTFCOP (see Box 1), when implementing effective ECDD measures. Licensees should also be mindful of the relevant guidance issued by FIA on red flags[4] and filing of SARs[5].

ENHANCED CUSTOMER DUE DILIGENCE – CUSTOMERS DERIVED THROUGH INTRODUCER RELATIONSHIPS

The elevated risk of non-face-to-face delivery channels should be factored into customer risk assessments for those customers introduced through third party. Licensees are not absolved of conducting due diligence on these customers, as when combined with other risk factors, such customers may present an elevated risk.

Licensees are, therefore, required to ensure that the elevated ML, TF and PF risks relating to introduced customers are mitigated through the conduct of ECDD as well as the ongoing monitoring of customer activities and transactions that may themselves pose an elevated ML, TF or PF risk.

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.

[4] https://fiabvi.vg/Analysis-Investigation/Suspicious-Activity-Reports/FAQ

[5] https://fiabvi.vg/Analysis-Investigation/Suspicious-Activity-Reports/Preparing-to-File

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 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
FATF	Financial Action Task Force
FIA	Financial Investigation Agency
FIs	Financial Institutions
FSC	Financial Services Commission
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
SCDD	Simplified Customer Due Diligence
SoF	Source of Funds
SoW	Source of Wealth
STR	Suspicious Transaction Report
TF	Terrorism Financing