
ANTI-MONEY LAUNDERING & COMBATING THE FINANCING OF TERRORISM POLICY

Table of Contents

PURPOSE.....	3
DEFINITIONS OF MONEY LAUNDERING AND TERRORISM FINANCING.....	4
RESPONSIBILITIES.....	5
ENFORCEMENT.....	5
REVISION AND CHANGES.....	5
ANTI-MONEY LAUNDERING POLICY.....	5
GENERAL POLICY.....	5
<i>Restricted Territory.....</i>	6
<i>Monitoring and Control.....</i>	6
SPECIFIC POLICY.....	7
<i>Risk Assessment.....</i>	7
<i>Know Your Client Procedure.....</i>	8
<i>Customer Due Diligence Procedure.....</i>	8
<i>Customer Due Diligence Documents.....</i>	8
<i>Ongoing clients monitoring.....</i>	8
<i>Unusual Transactions.....</i>	9
<i>Cash Transactions.....</i>	9
<i>Withdrawal Processing.....</i>	9
<i>Abnormal Transactions.....</i>	9
<i>Payment Options.....</i>	10
<i>Suspicious Transactions.....</i>	10
<i>Transaction Recording.....</i>	10
<i>Internal Financial Transactions.....</i>	10
<i>Transaction Monitoring.....</i>	10
COMPANY OBLIGATIONS.....	10
COURSE OF ACTION IN CASE OF SUSPICION OF FRAUD.....	11
IMPORTANT NOTE.....	11
FRAUD/MONEY LAUNDERING INVOLVING INTERNAL STAFF.....	11
ANNEX 1.....	13
1. LIST OF DEFINITIONS.....	13
ANNEX 2.....	14
1. FACTORS OF HIGHER RISK SITUATIONS.....	14
1.2 Product, service, transaction or delivery channel risk factors.....	14
1.3 Geographical risk factors.....	14
2. FACTORS OF LOWER RISK SITUATIONS.....	14
2.2 Product, service, transaction or delivery channel risk factors.....	14
2.3 Geographical risk factors.....	14
ANNEX 3.....	15
CUSTOMER DUE DILIGENCE.....	15

Purpose

This document deals with the measures implemented by SOFTGENIUS NV, to present anti money laundering (**AML**) within gaming. Together with individual and corporate obligations, it describes the methods that can potentially be used to carry out anti money laundering in gaming, our identification techniques and the procedures to follow when money laundering is discovered. A reporting process is detailed for all suspicious activity towards the end of the document.

SOFTGENIUS NV take a zero-tolerance approach to being involved in illegal/illicit activity, and will fully comply with all relevant sections of the Prevention and Suppression of Money Laundering and Terrorist Financing Law 188(I)/2007 and subsequently amended, the EU Directive 2019/1153, and the CBC Sanctions Directive.

All partners and employees of the firm are under an obligation and duty to comply with the above. This policy & any related procedures aims to help partners and staff fulfil these responsibilities, by providing a clear framework, along with setting out the firm's key principles and obligations.

- Failure to fulfil these responsibilities may result in disciplinary action and may also result in criminal sanctions for the staff involved.
- Breaches may also be reportable to our AML Supervisor which may result in professional disciplinary action.
- Furthermore, a report may also have to be made to the law enforcement agencies, which may result in a criminal investigation.

As a company, we are committed to carrying on business in accordance with the highest ethical standards. This includes complying with all applicable laws and regulations aimed at combating money laundering and terrorist financing. This Policy has been developed by SOFTGENIUS NV to reduce the risk of money laundering and terrorist financing associated with its business and the sale of its products. This Policy explains our individual responsibility in complying with anti-money laundering and counterterrorist financing laws ("AML Laws") around the world and ensuring that any third parties that we engage to act on our behalf, do the same.

The Anti-Money Laundering Policy ("AML Policy") applies to SOFTGENIUS NV, its direct and indirect parent companies (i.e. SOFTGENIUS NV and SG HOLDING LTD, respectively), its direct wholly- and majority-owned subsidiaries and their directors, officers, full-time, part-time and seconded employees, and anyone working on SOFTGENIUS NV's behalf, e.g. consultants and representatives (collectively "Personnel", or the "Employees"). Personnel are expected to act in a manner that will enhance SOFTGENIUS NV's reputation for honesty, integrity and reliability. The AML Policy applies in all countries in which SOFTGENIUS NV operates or conducts business. When the laws of those countries require a higher standard, such standard shall apply. Adherence to this AML Policy is a condition of employment and/or engagement with the Company, and therefore the Employees must acknowledge on an annual basis that they have understood the AML Policy and have disclosed any suspected and actual violations through appropriate channels.

The AML Policy will not give answers for every ethical or legal situation. If Employees have any doubts about the right thing to do, they should seek advice from the relevant member(s) of

Compliance or from the General Counsel, as appropriate.

If Employees violate SOFTGENIUS NV's policies and procedures or any of the laws that govern SOFTGENIUS NV's business, SOFTGENIUS NV will take immediate and appropriate action up to and including termination of employment.

The purpose of this AML Policy is to substantially prevent, manage and mitigate the risk that SOFTGENIUS NV and their Employees become directly or indirectly involved in actual or potential money laundering activities, or terrorist financing activities.

This AML Policy sets out the key principles and obligations in relation to the AML Framework in order to identify and assess the Money Laundering ("ML")/Terrorism Financing ("TF") risks to which SOFTGENIUS NV is exposed to ("ML/TF", respectively the "AML" measures, or more broadly "AML"), as defined below.

For the purpose of this AML Policy, a counterparty comprises of: SOFTGENIUS NV's shareholders, companies that SOFTGENIUS NV has invested in, Employees, financial institutions, service providers and any business relationship. A 'business relationship' means a business, professional or commercial relationship which is connected with the professional activities of the institutions and persons covered by such law and which is expected, at the time when the contact is established, to have an element of duration.

If you have any questions about this Policy, you should contact the Ethics and Compliance or the Legal Department.

Definitions of money laundering and terrorism financing

Money Laundering is the process by which it attempts to hide and disguise the true origin and ownership of the proceeds from criminal activities, thereby avoiding prosecution, conviction and confiscation of criminal funds.

Money laundering means exchanging money or assets that were obtained criminally for money or other assets that are 'clean'. The clean money or assets don't have an obvious link with any criminal activity. Money laundering also includes money that's used to fund terrorism however it's obtained.

The following types of activities are considered to be "money laundering" and are prohibited under this Policy:

- a) the conversion or transfer of property (including money), knowing or suspecting that such property is derived from criminal or certain specified unlawful activity ("criminal property"), for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action;
- b) conducting a financial transaction which involves criminal property;
- c) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, ownership or control of criminal property;
- d) the acquisition, possession or use of criminal property;
- e) promoting the carrying on of unlawful activity; and
- f) participation in, association to commit, attempts to commit and aiding, abetting, facilitating

and counselling the commission of any of the actions mentioned in the foregoing points.

The broad definition of money laundering means that anybody (including any SOFTGENIUS NV employee) could be in violation of the law if he/she becomes aware of, or suspects, the existence of criminal property within the business and becomes involved in or continues to be involved in a matter which relates to that property being linked to the business without reporting his/her concerns.

Property can be criminal property where it derives from any criminal conduct, whether the underlying criminal conduct has taken place in the country where you are situated or overseas.

Terrorism Financing means: the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any terrorist act.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

Responsibilities

The teams / person responsible for the implementation and effectiveness of this policy are:

- Payment Officer
- Chief Financial Controller
- Anti-Money Laundering Compliance Officer (AMLCO)

Enforcement

Any employee found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment. Companies contracted to SOFTGENIUS NV found to be violating this policy will be deemed to be in breach of contract.

Revision and Changes

All SOFTGENIUS NV procedures are subject to an annual revision which has to be completed before the annual financial audit of the company. Significant changes to any policy or procedures are to be approved by the Key Official and communicated to the relevant Authorities.

Anti-Money Laundering Policy

Gaming operations are exposed to financial and reputational risk posed by fraud and money laundering. Good controls should be in place in order to establish a complete set of monitoring techniques to detect and continuously combat money laundering. Having controls and processes in place that can detect and prevent Money Laundering constitutes an essential part of sound risk management; it helps to protect the integrity of the company and its operations by reducing the likelihood of it becoming a vehicle for or a victim of financial crime. It forms part of a general responsibility to up hold the soundness of the financial system which we form a part of.

General Policy

In order to initiate AML Procedures SOFTGENIUS NV will adhere to the requirements of the Prevention of Money Laundering Act, the regulations and any guidance notes SOFTGENIUS NV and

shall as a minimum:

- Appoint one of its senior officers as the designated Anti-Money Laundering Compliance Officer (AMLCO) whose responsibilities will include the duties required by the laws, regulations and guidance notes.
- Retain identification and transactional documentation as defined in the laws, regulations and guidance notes.
- Keep at all times a secure online list of all registered players.
- Take reasonable steps to establish the identity of any person for whom it is proposed to provide its service. For this purpose, the process for the registration of players provided for under the General Terms and Conditions provides for the due diligence process that must be carried out before the opening of a User Account.
- Ensure that this policy is developed and maintained in line with evolving statutory and regulatory obligation and advice from the relevant authorities.
- Provide initial and on-going training to all relevant staff so that they are aware of their personal responsibilities and the procedures in respect of identifying players, monitoring player activity, record-keeping and reporting any unusual/suspicious transactions.
- Report any suspicion or knowledge of money laundering or terrorism financing to the Unit for Combating Money Laundering (MOKAS) set up by law as a Government Agency responsible for the collection, collation, processing, analysis and dissemination of information with a view to prevent money laundering and combat the funding of terrorism.
- Examine with special attention, and to the extent possible, the background and purpose of any complex or large transactions and any transactions which are particularly likely, by their nature, to be related to money laundering or the funding of terrorism.
- Co-operate with all relevant administrative, enforcement and judicial authorities in their endeavor to prevent and detect criminal activity.

Restricted Territory

1. Jurisdictions considered as high risk or restricted:

Albania, Antigua and Barbuda, Bahrain, Belgium, Belize, Bolivia, Brunei, Burkina Faso, Burundi, Cambodia, Cayman Islands, Curacao, Dutch West Indies, Estonia, Ecuador, Egypt, Ethiopia, Finland, France and its overseas territories (Guadeloupe, Martinique, French Guiana, Réunion, Mayotte, St. Pierre and Miquelon, St. Barthélemy, French Polynesia, Wallis and Futuna, New Caledonia) Gibraltar, Greece, Ghana, Indonesia, Israel, Jamaica, Jersey, Jordan, Kenya, Kuwait, Lithuania, Mauritius, Morocco, Netherlands, Nigeria, Oman, Panama, Qatar, Romania, Russia, Spain, Slovakia, Sao Tome and Principe, Saudi Arabia, Senegal, Seychelles, Sierra Leone, Sri Lanka, Tanzania, Thailand, Turkey, Ukraine, United Arab Emirates, the United Kingdom (including United Kingdom Overseas Territories), Uruguay, US or any of its states, Vietnam.

2. Jurisdictions that are sanctioned or black-listed:

Afghanistan, American Samoa, Angola, Belarus, Barbados, Bosnia and Herzegovina, Botswana, Central African Republic, Côte d'Ivoire, Cuba, Democratic Republic Congo, Fiji, Eritrea, Guinea, Guinea-Bissau, Guam, Guyana, Haiti, Iran, Iraq, Laos, Lebanon, Liberia, Libya, Mali, Myanmar (Burma), Nicaragua, North Korea, Pakistan, Palau, Palestine, Samoa, Somalia, South Sudan, Sudan, Syria, The Crimea Region (Russia/Ukraine), Trinidad and Tobago, Tunisia, Turkmenistan, Uganda, Uzbekistan, Vanuatu, Venezuela, Yemen, Zimbabwe.

Monitoring and Control

In gaming, rousing of suspicions of money laundering should occur when certain client behaviors are observed, these can manifest as but are not limited to one or many of the below:

- Observing money being placed into the site and then withdrawn a different way either before or after gaming especially if the depositing and withdrawing methods are located in different countries. Note with an e-wallet it's generally not possible to know the country where funds are going; unsurprisingly e-wallets are commonly used for money laundering.
- Suspecting an account is being controlled under a false identity either with fake documentation being supplied or with genuine documentation but the account being controlled not by the person who is stated / verified on file.
- Observing a customer holding large volumes of money in the site unnecessarily/not in order to game (to conceal it from authorities).
- Observing manipulated game play designed to deliberately move money from account to account or to manipulate the odds of the game.

Specific Policy

The following are some specific cases where monitoring and control should be exercised. Monitoring and control should not be limited only to the following list of cases.

Risk Assessment

This procedure consists in identifying and assessing the ML/FT risks one is exposed to, and vary and adapt measures, policies, controls and procedures in a way that ensures that resources are applied where most needed. The assessment is carried out in order to be able to identify potential risks upon entering into a business relationship or carry out an occasional transaction, therefore, it enables to develop a risk profile and to categorize the ML/FT risk posed as low, medium or high.

Customer and Business Risk Assessment (CRA/BRA) are performed taking in consideration the following risk factors:

- Customer risk.
- Product, Service, and Transaction risk.
- Interface risk.
- Geographical risk.

Once created, a client's risk profile shall be monitored for any unusual activity and/or behaviour which could alter the original profile.

As measure of prevention against Financing of Terrorism and Sanctions Obligations, further screenings shall be implemented against:

- Adverse Media + Google check and
- Sanctioned persons list against relevant EU and UN lists of designated persons, groups or entities check ;

Standalone screening based on adverse media will be used in order to identify certain points such as:

- *Ultimate beneficial ownership (UBO)*, as media screening can help identify the beneficial owners of shell companies and other instances of money launderers disguising their crimes using corporate structures;

- *Terrorist Financing*, as news stories concerning terrorism, sourced from international outlets, represent a supplementary channel through which financial institutions can address the risk of individuals being involved in groups suspected of terrorism;
- *Politically Exposed Persons*, as news stories involving politically exposed persons (PEP) may expose instances of corruption or financial crime before the information is confirmed in official channels;

Know Your Client Procedure

Each client must register and follow the KYC procedure. This procedure is the roots of identifying and verifying the players that have access to the system, effect financial and gaming transactions and participate in the games offered.

Customer Due Diligence Procedure

This procedure's role is to know who the customer is and to build a customer profile of which the customer's identity can be assessed and any unusual behavior can be identified. If any such behavior is found to lead to a suspicion of ML/FT, it shall be reported to the FIAU. CDD shall have four measures:

- Identification and Verification of the Customer.
- Identification and Verification of the Beneficial Owner.
- Obtaining Information on the Purpose and Intended Nature of the Business Relationship.
- On-Going Monitoring.

Depending on risk, the Customer Due Diligence shall be simple or enhanced.

Customer Due Diligence Documents

At registration stage

- A valid and unexpired national government-issued identity card;
- A valid unexpired passport;
- A valid unexpired residence card;
- A valid unexpired driving licence;

At verification stage

- A bank statement or reference letter issued by a recognised credit institution or entity carrying out relevant financial business;
- A utility bill (electricity, water bill, internet), mobile phone bills are not accepted;
- Any other government-issued document not mentioned above;

The documents listed above must not be more than three (3) months old.

The documents subjected to verification shall be obtained in hard copies and may be gathered also in electronic means through, amongst others, *electronic mail* and *audio-visual means*. Nonetheless, it is imperative that such documents shall be **clear, legible and of good quality**.

The documentation used for identification and verification purposes must be authentic or reproduced authentic ones.

Ongoing clients monitoring

The monitoring shall take place in situations in which a client seeks to form or has formed a business relationship, and not an occasional transaction.

The monitoring shall have several steps.

First one is the **Scrutiny of Transactions**, which consists in using the information provided by the customer to identify any transactions that are unusual.

At this step, any unusual transaction served as red flag or event trigger which shall require immediately scrutiny of the relationship to establish if a transaction is suspicious and ought to be reported or whether there is a legitimate and plausible explanation.

The term *unusual* used here includes transactions which are unusual by their very nature (as they are suspicious, illogical, or unreasonable), as well as those which are inconsistent with the client's profile or are significantly different to what is usually carried out or requested by the client.

Second step is the **Periodic Review of the information, data and documents held on the client**, which consists in ensuring that information, documents and data on the client, as well as any assessment, remain up-to-date and relevant. Depending on risk assessment, the periodic review shall be performed as follows:

- | | |
|------------------|---------------|
| • Low | Every 5 years |
| • Low to Medium | Every 3 years |
| • Medium | Every 2 years |
| • Medium to High | Every 1 year |

All records of CDD documents and supporting evidence will be kept for five years.

Unusual Transactions

In case of unusual or unreasonable transactions, employees should report the transaction to the relevant persons. The Anti-Money Laundering Compliance Officer should always be informed and have the case investigated. Each suspicious transaction should be reported to the relevant authority accordingly.

Cash Transactions

Cash transactions for player deposits or withdrawal are not allowed. Player deposits and withdrawals have to be made through the available payment options.

Withdrawal Processing

All withdrawals should be checked before being processed. The Fraud Team should check each withdrawal for unusual activity. Any unusual transaction should not be processed before investigated and verified as being legitimate.

Abnormal Transactions

Abnormal transactions refer to substantial deposits and withdrawals or substantial wins or losses as compared to average player activity. In case of abnormal transactions, employees should investigate the abnormality of the transaction and if the outcome is still not clear report the transaction to the Anti-Money Laundering Compliance Officer should in order to investigate the case further. The

checks should include but not limited to verify player, check game play and verify account activity. Each suspicious transaction should be reported to the relevant authority accordingly.

High rollers and VIP players should be earmarked to avoid confusion; nonetheless, their transactions should still be monitored accordingly.

Payment Options

Withdrawals should only be processed to the same payment option used for depositing. If this is not possible use a method that can be verified and that is in the name of the same person making the deposit.

Suspicious Transactions

Investigate and report all suspicious transactions.

Transaction Recording

All player financial and gaming transactions should be recorded and accounted for.

Internal Financial Transactions

Internal financial transactions should also be recorded and accounted for. The CFO should follow the Accounting Standards accordingly.

Transaction Monitoring

Both player and corporate transactions should be monitored continuously and where possible implement verification requirements for substantial transactions.

Company Obligations

SOFTGENIUS NV aims to satisfy all responsibilities and requirements identified by the Prevention and Suppression of Money Laundering and Terrorist Financing Law 188(I)/2007 and subsequently amended, the EU Directive 2019/1153, and the CBC Sanctions Directive.

- Identification (KYC) and customer due diligence (CDD);
- Internal record keeping;
- Reporting (both internal and external); and
- Employee instruction and training.

SOFTGENIUS NV have suitable controls in place that allow the identification of customers via a 'know your client' (KYC) procedure. This procedure can be initiated ad hoc by the fraud department and occurs automatically based on certain low-level deposit and withdrawal criteria. Further CDD will be performed based on defined thresholds of activity by the fraud department.

SOFTGENIUS NV also have suitable internal controls in place that prevent money laundering such as having a tight card policy, examples of this include only allowing one card on an account at a time and always processing withdrawals by default back in the same direction as deposits (closed loop).

Appropriate transaction records are kept within the SOFTGENIUS NV game servers or in the accounting and auditing tool.

Course of Action in Case of Suspicion of Fraud

It is a duty as an operational member of staff to be alert for the signs of money laundering as detailed in this document, through further training and via usage of reasonable levels of skepticism and common sense.

Confidential money laundering issues should be reported to the AMLCO using a Suspicious Transaction Report (**STR**). The Anti-Money Laundering Compliance Officer (**AMLCO**) or Money Laundering Reporting Officer (**MRLO**) is responsible for the investigation cases of suspected money laundering and if deemed necessary escalation of them to the Unit for Combating Money Laundering (**MOKAS**).

Employees should email Suspicious Transaction Report directly to the AMLCO or COO who can then handle the document appropriately.

IMPORTANT NOTE

A customer should never be informed that a suspicious activity report has been raised against them or imply in any way to a customer that their account may be under investigation. Doing this would constitute ‘tipping off’ the customer. Tipping off a customer can unnecessarily alarm them if they are not committing an offence but most importantly, if they are involved in criminal activity, it could aid them by indicating they are being investigated. It would ‘tip off’ a criminal to quickly destroy incriminating evidence against them and change their mode of operation. This would jeopardize any investigation into them. In some countries ‘tipping off’ if proven can constitute a criminal offence and can in the absence of further evidence inadvertently implicate you in the operation of the crime. Do not inform or unnecessary staff either, as this may inadvertently lead to tipping off via a 3rd party route. Do not do anything to a client’s account that could tip them off which includes closing it, the AML team can handle this if needed.

An employee who has failed to act or acted negligently in the light of proven ‘reasonable grounds to suspect’ money laundering is also liable to prosecution.

Report suspicious activities and transactions, using an STR to the AMLCO or COO.

Do not inform a customer that a STR has been raised involving them.

Do not inform unnecessary personnel about your report or suspicions.

Fraud/Money Laundering involving Internal Staff

Although it is very rare and certainly not part of SOFTGENIUS NV agenda, money laundering and/or fraud unfortunately can also occur internally within a business.

Extreme candor should be exercised in handling any of the below scenarios, ideally one would have at least some basic evidence or indications of where evidence would lie to back up any reported

suspicious. Poorly handled or judged situations of this nature can result in significant unnecessary harm either to any of the individuals involved and/or the business.

1. Pressure or instructions by privileged members of staff to perform transactions or make changes that would deliberately ignore or avoid due diligence, should be reported to the AMLCO or a suitably senior executive such as the COO. It is advised that the person is not confronted by member(s) of staff, nor anyone else should be enquired about the activity by any member of staff. The investigation should be carried out by the appointed and responsible parties. Unnecessary people should not be informed about the report/suspicion.

2. If any employee sees a colleague, no matter how senior, engaging in suspicious activity such as performing unauthorized transactions, frequently working late/alone without apparent reason, taking sensitive documents from the office or being untruthful about their activity report it to the AMLCO or a suitably senior executive such as the COO. It is advised that the person is not confronted by member(s) of staff, nor anyone else should be enquired about the activity by any member of staff. The investigation should be carried out by the appointed and responsible parties. Unnecessary people should not be informed about the report/suspicion.

ANNEX 1

1. LIST OF DEFINITIONS

1.1 In this AML Policy, the following terms have the following meanings:

AML means anti-money laundering.

AML Policy means the Anti-Money Laundering Policy of SOFTGENIUS NV.

AMLCO means Anti-Money Laundering Compliance Officer

Board of Directors means the board of directors of SOFTGENIUS NV.

BRA means Business Risk Assessment.

Company means SOFTGENIUS NV, its direct and indirect parent companies, its direct wholly- and majority-owned subsidiaries.

Compliance Program means the compliance program of SOFTGENIUS NV as adapted by the Supervisory Board.

CRA means Customer Risk Assessment.

Employee means any director, officer, full-time, part-time and seconded employee including any third- party contractor, who receives or is entitled to receive remuneration for goods or services from SOFTGENIUS NV.

FIAU means Financial Intelligence Analysis Unit.

General Counsel means the general counsel of SOFTGENIUS NV.

ML means Money Laundering.

MLRO means Money Laundering Reporting Officer.

Money Laundering means Money Laundering as defined in this AML Policy in Clause 4.

PEP means Politically Exposed Persons.

Personnel means the directors, officers, full-time, part-time and seconded employees of SOFTGENIUS NV, and anyone working on SOFTGENIUS NV's behalf, e.g. consultants and representatives.

PMLFTR means Prevention of Money Laundering and Funding of Terrorism Regulations

Supervisory Board means the supervisory board of SOFTGENIUS NV. **Terrorist**

Financing means Terrorist Financing as defined in this AML Policy in Clause 4. **TF** means Terrorist Financing.

1.2 Save where the context dictates otherwise, in this AML Policy:

- a) unless a different intention clearly appears, a reference to a Clause or Annex is a reference to a clause or annex of this AML Policy;
- b) words and expressions expressed in the singular form also include the plural form, and vice versa;
- c) words and expressions expressed in the masculine form also include the feminine form; and
- d) a reference to a statutory provision counts as a reference to this statutory provision including all amendments, additions and replacing legislation that may apply from time to time.

1.3 Headings of clauses and other headings in this AML Policy are inserted for ease of reference and do not form part of this AML Policy for the purpose of interpretation.

ANNEX 2

1. FACTORS OF HIGHER RISK SITUATIONS

1.1 Counterparty risk factors

- a) the business relationship is conducted in unusual circumstances;
- b) counterparties that are resident in geographical areas of higher risk;
- c) legal persons or arrangements that are personal asset-holding vehicles;
- d) companies that have nominee shareholders or shares in bearer form;
- e) businesses that are cash-intensive; and
- f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;

1.2 Product, service, transaction or delivery channel risk factors

- a) products or transactions that might favor anonymity;
- b) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;
- c) payment received from unknown or unassociated third parties; and
- d) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products;

1.3 Geographical risk factors

- a) countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective anti-money laundering and counter terrorist financing systems;
- b) countries identified by credible sources as having significant levels of corruption or other criminal activity;
- c) countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations; and
- d) countries providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

ANNEX 3

CUSTOMER DUE DILIGENCE

In case of PEP's, additional measures shall be applied, such as:

- Obtain senior management approval to service the PEP.
- Establish their source of wealth and, where applicable, their source of fund.
- Conduct enhanced on-going monitoring of the customer's activity.

Documents used in the CDD procedure shall be:

- Proof of ID.
 - a. Signature Is there.
 - b. Full Name matches client's name.
 - c. Document does not expire in the next 3 months.
 - d. Owner is over 18 years of age.
- Proof of Residence.
 - a. Bank Statement or Utility Bill.
 - b. Full Name matches client's name and is same as in proof of ID.
 - c. Date of Issue: In the last 3 months.
- Selfie with ID (in Enhanced CDD).
 - a. Holder is the same as in the ID document above.

On-going monitoring to detect unusual activities and to keep information and profile updated shall be conducted regularly in order to avoid cases of ML/FT. Any suspected cases shall be reported immediately.

All clients (new/existing) from established in high-risk third countries as shown in the 2022 amended **PMLFTR** shall be subjected to Enhanced CDD. If the requirements are not met, they will be blacklisted.

Approval

This policy has been reviewed and approved as of 23 October 2024.



Craig Dinwoodie
MLRO