Sovereignty SRL
-
Financial Crime Prevention Policy

Version Control

Prepared By	Reviewed/Approved By	Revision Number	Approval Date
Sovereignty SRL	Manager	1	07/05/2025

Table of Contents

1.0 Rationale

The purpose of this Policy is to provide a consistent, proportionate and effective approach to deter and detect Financial Crime ("FC"), by managing risk through a framework of core compliance requirements.

In this Policy, the term FC covers the following subjects:

- Money Laundering ("ML");
- Terrorist Financing ("TF")
- Fraud; and,
- Sanctions.

The risks associated with this Policy are managed through the Business Wide Risk Assessment ("BWRA").

In addition, this Policy has been designed to support compliance with, amounts others, the following legislation and regulations:

- Sovereignty Gaming Act ("SGA") Gaming Act 2025.
- SGA Remote Gambling Anti-Money Laundering ("AML") Code of Practice.
- SGA General Code of Practice.
- SGA Regulations Concerning AML and Counter Terrorist Financing ("CTF"), "AML Regulations"; and,
- Other applicable legislation.

1.1 Scope

This Policy is mandatory for the entirety of the Company. Where the requirements of this Policy conflict with local laws or regulations, the jurisdictional requirements must take precedence, and the business must record these instances. The Company has no appetite for breaching FC legislation and regulation. To reflect the Companies commitment and risk appetite, this Policy clearly articulates a set of standards and requirements that the business must comply with.

No part of the Company, or anyone acting on its behalf must do anything to frustrate or circumvent the intended purpose of this Policy.

This Policy should be read in conjunction with supporting documentation, such as the Customer Due Diligence "CDD" Procedure and other relevant Policies and Procedures ("P&Ps").

2.0 The Compliance Framework

In accordance with the AML Regulations, the Company must prepare an AML/CTF program consisting of:

- A risk assessment; and,
- Applicable policies, controls and procedures

to ensure adherence with relevant legislation and regulation, in addition to identifying any emerging risks.

2.1 Senior Management/Nominated Officer Responsibility

Senior Management within the Company are responsible for the establishment and management of effective systems and controls to counter the risks of FC.

At a minimum, Senior Management must:

- Appoint appropriately skilled individuals to conduct the role of the Compliance Officer/Money Laundering Reporting Officer ("MLRO"), otherwise referenced as the "Nominated Compliance Officer";
- Ensure sufficient resourcing (people and systems) to effectively manage FC risk; and,
- Provide an appropriate level of training to ensure employees have the necessary skills, knowledge, and capabilities to carry out their role effectively.

The Nominated Compliance Officer must:

- Be suitably experienced.
- Demonstrate they have the capability to fulfil the role; and,
- Be of sufficient seniority to act independently.

2.2 Escalation Management

The Company must have clear and accountable governance processes to review Customers which raise FC concerns. Material FC risks should be escalated to a senior risk management forum and the Company must implement governance processes to allow for the escalation of such risks to either the Board of Directors ("BOD") overseeing the Company, or an appropriate Risk Committee composed of senior managers and the Nominated Compliance Officer.

Note:

- Such forums must be properly constituted, and minutes of meetings kept, using formal reports and assessment tools for identified cases; and,
- The Board should receive at least an annual report on FC activities and issues affecting the company from the Nominated Compliance Officer, including an annual update of the company risk assessment. More regular reports to the Board should be made as events dictate.

2.3 Employee Due Diligence

The Company must implement appropriate risk-based systems and controls to determine whether to, and in which manner to screen any prospective employee who, if employed, may be able to facilitate FC.

The systems should also describe whether to, and in what manager to, re-screen an employee where the employee is transferred or promoted and may be able to facilitate the commission of FC.

The Company must establish and maintain a system to manage any employee who fails, without reasonable excuse, to comply with any system control or procedure.

2.4 Employee Training

The Company must ensure that all staff receive adequate FC training in order to ensure that they understand the risks and associated responsibilities in connection with their employment. The training provided may include both general and role-specific training.

After the training is conducted, each attendee must undergo an assessment to test their recently acquired FC knowledge. If a score of at least 75% is not achieved, employees will be required to re-sit the test and/or repeat the training.

Annually, all employees must undergo refresher training. Any changes to relevant regulations and P&Ps must be covered within the scope of this annual training.

2.5 Business Wide Risk Assessment

The Company must undertake a risk assessment to identify and assess the risks of FC to which it may be subject.

In conducting the risk assessment, the Company must consider all relevant FC factors, including (but not limited to):

- It's Customers.
- The countries or geographic areas in which it operates.
- Its products or services.
- Its payments and transactions.
- Its operational set up and delivery channels; and,
- Any Third Parties ("TPs") that provide services to the Company.

In deciding how to conduct the BWRA, the Company must take into account its size and nature of business. The BWRA must be reviewed regularly (e.g., annually), with a clear methodology documented.

2.6 Independent Review

The Company's FC framework must be subject to regular, independent and, where appropriate, external review.

The frequency of the review should consider the nature, size and complexity of the Company's business, including the type and level of FC risk it might face. Thus, an independent review must be undertaken every two years at a minimum.

2.7 Systems, Controls and Processes

The Company must ensure that effective systems, controls and clearly defined processes and procedures are in place to manage and mitigate the risks of FC.

These must be proportionate to the nature and size of the business and support the requirements set out within this Policy, in addition to aligning with all relevant legislation and regulation.

Where instances of FC have occurred, risk sensitive analysis must be undertaken to understand the root cause and where appropriate, action must be taken to prevent reoccurrence.

Systems and controls must be reviewed regularly to ensure they remain up to date or reviewed and refreshed periodically where no changes have occurred.

3.0 Customer Onboarding

3.1 Customer Risk Assessment

Through the Customer Risk Assessment ("CRA"), all Customers will be categorised based on their FC risk, considering the following risk factors:

- Customer Risk.
- Geographical Risk.
- Product Risk; and,
- Payment Risk.

Proceeding the assessment of such factors, Customers will be risk rated:

- Lower.
- Standard; or,
- Higher.

3.2 Customer Due Diligence

3.2.1 Application of CDD

CDD should be applied to all Customers and TP relationships.

The Company should employ CDD in the following instances:

- When establishing a business relationship.
- When carrying out occasional transactions.
- Where there is a suspicion of FC; and/or,
- Where there is any doubt about the veracity or adequacy of previously obtained customer identification data.

In keeping with the requirements of the AML Regulations and within the context of the gaming industry, CDD must be undertaken at account opening and must be completed within 30 days of first deposit or before the Customer wagers more than an equivalent of EUR 2,000 of their own funds (as opposed to recycled winning) and before any money is paid out.

The Company must also complete the verification of identity and undertake such other applicable CDD measures as soon as reasonably practicable following the deposit of funds into the account.

In most cases, standard CDD measures will provide the required level of confidence that the Customer is who they say they are and the purpose and intended nature of the relationship is understood. However, in cases were the confirmed risk rating is Higher, (or equivalent) the Company must apply additional Enhanced Due Diligence ("EDD") measures to mitigate the higher risk nature of the Customer relationship.

3.2.2 CDD Measures

The CDD measures to be taken are as follows:

- Where applicable, the Company should understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship.

- The Company must identify the Customer and verify their identity using reliable, independent, primary source documentation (e.g. government issued photo ID) or utilise other appropriate electronic ID&V software.
- Gather supporting information and accompanying evidence (such as proof of date of birth and residential address);
- Conduct screening checks against relevant adverse media, Sanctions and Politically Exposed Persons ("PEP") lists; and,
- Conduct ongoing due diligence and monitoring of transactions throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the Company's knowledge of the Customer, including, where required, the Customer's Source of Funds ("SOF").

Where the Customer is a corporation, partnership, Limited Liability Company ("LLC"), trust or other business entity, the Company must take reasonable measures to verify the identity of the individual or individuals who are the beneficial owners of the Customer, such that the Company is satisfied that it knows who the beneficial owner is. This may require the Company to understand the ownership and control structure of the Customer, up to and including the Ultimate Beneficial Owner ("UBO").

Further to this, where the Company is unable to complete any aspect of the CDD requirements, it:

- Should cease to onboard or terminate the business relationship; and,
- Must document, through appropriate means, why CDD measures could not be completed, raising a Suspicious Activity Report ("SAR") if required.

3.2.3 EDD

The Company must apply EDD measures where there is:

- A material change in the risk rating of the Customer (an increase in risk to Higher) or where a high risk red flag is identified;
- Where there is doubt regarding the veracity of the Customer information provided, including their identity;
- Where there are any transactions which are not reasonably consistent with the Company's knowledge of the Customer; and/or,
- Suspicion of ML, TF, Fraud and/or Sanctions evasion.

EDD measures applied shall include:

- Obtaining additional information to verify the Customer's identity;
- Obtaining additional information as to the Customer's SOF;
- Obtaining the approval of senior management for establishing or continuing the business relationship; and,
- Conducting enhanced monitoring of the business relationship.

3.2.4 Inability to Complete CDD

The Company must have controls in place to ensure that where CDD cannot be completed, the Company does not:

- Establish a business relationship or carry out an occasional transaction (as per relevant thresholds) with the Customer;
- Terminate any existing business relationship with the Customer, without taking appropriate risk based measures, including escalation to the Nominated Compliance Officer and if required, file a SAR.

3.3 PEPs

A PEP is an individual who is or has been entrusted with a prominent public function and includes their immediate/close family or known associates. As such, those individuals who meet the definition of a PEP pose a higher FC risk.

Where the Company identifies a relationship with a PEP, it must:

- Obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;
- Take reasonable measures to establish the SOF;
- Clearly document the rationale for commencing, continuing or terminating the relationship with the PEP; and,
- Conduct enhanced ongoing monitoring of the business relationship.

For at least 12 months after a PEP is no longer entrusted with a prominent public function, should the Company consider the continuing risk posed by that individual.

3.4 Persons Connected to Sporting Events

In addition to performing normal CDD measures, the Company must also have appropriate risk-management systems to determine whether a Customer is a person, or a family member or close associate of such a person, who has a close connection to:

- A sporting event, team, sporting association or organisation; and/or,
- The Company accepts bets on that team, sport, or sporting event.

Where the Company identifies a relationship with such person, it must:

- Obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;
- Take reasonable measures to establish the SOF;
- Clearly document the rationale for commencing, continuing or terminating the relationship with the person; and,
- Conduct enhanced ongoing monitoring of the business relationship.

3.5 Prohibited & Sanctioned Jurisdictions

The Company will not do business with any entity or individual who is subject to European Union ("EU"), United Nations ("UN") and other international sanctions legislation.

Further to this, any countries denoted on the Tobique prohibited list[1] shall also be deemed outside of risk appetite.

3.6 Outsourcing of CDD Activities

Where the Company relies on TPs to perform elements of the CDD, it is the ultimate responsibility of the Company and its compliance function to ensure adherence with applicable legislation.

Where the Company uses TPs, it must:

- Ensure that appropriate measures are taken to assess whether the TP is suitable to undertake the task and has adequate controls to ensure compliance with all relevant legislation;
- Take adequate steps to satisfy itself that copies and records of identification data and other relevant documentation will be made available upon request without delay; and,
- The obligations of the Company and TP are clearly defined.

4.0 Periodic Reviews

The Company must conduct Periodic Reviews of all Customers. The Periodic Reviews will be commensurate to the FC risk associated with the Customer, as detailed in the KYC Procedure.

Periodic Review must comprise of a full CDD refresh, including CRA, CDD information and documentation gathered in support of the CDD requirements, in addition to relevant screening checks.

5.0 Event Driven Reviews

Event Driven Reviews ("EDRs") must consist of a full CDD refresh, in line with that collated throughout a Periodic Review (see section 4.0 above). The identification of a high-risk factor or red flag during the screening or Transaction Monitoring ("TM") process may trigger a EDR. Where TPs are concerned, a material change to the ownership or control of the entities corporate structure and/or ultimate ownership will also trigger an EDR.

6.0 Suspicious Activity Reporting

The Company must be aware of its obligation (including that of its employees) to raise a Suspicious Activity Report ("SAR").

6.1 Submission of a SAR

The Company must file a SAR in the following instances:

- The Company suspects on reasonable grounds that a Customer is not the person the Customer claims to be;
- The Company suspects on reasonable grounds that the provision, or prospective provision, of its services is related to a financing of terrorism offence, or a ML offence, or other criminal offence; and/or,
- A transaction, for whatever reason, does not appear to have a lawful economic purpose.

Note:

- A SAR concerning a possible ML offence or other criminal activity must be lodged with the TGC within 5 business days after the Company forms the relevant suspicion.
- A SAR concerning or in relation to possible financing of terrorism, must be lodged with the TGC within 24 hours after the time in which the Company forms the relevant suspicion;
- The Company must document the reasons for any decision regarding the submission or non-submission of a SAR; and,
- Where required, a SAR should be filed with the relevant Financial Intelligence Unit ("FIU").

6.2 Offence of Tipping Off

If the Company forms:

- A reasonable suspicion.
- Lodges a SAR with the SGA/FIU; or,
- Provides documents or other information to the SGA,

Neither the Company nor any person employed or associated with the Company may disclose to someone other than the SGA/FIU that the suspicion has been formed and report lodged.

7.0 Ongoing Monitoring

The Company must ensure that its customers are subject to ongoing monitoring for the duration of the relationship, not just at the initial onboarding stage.

Ongoing monitoring should include:

- Regular screening against adverse media, PEP and sanction databases; and,
- TM in terms of which the frequency, volume and value of bets placed by an individual Customer are monitored and compared to expected transactional profiles.

Note: Ongoing monitoring checks should include the identification and monitoring of 'linked' accounts owned by the same Customer.

8.0 Record Keeping

The Company will:

- Maintain, for at least 5 years, all necessary records on transactions, including domestic and international;
- Maintain records of the originator/payer information, and required beneficiary/payee information, on wire transfers, electronic fund transfers and other electronic payments; and,
- Keep records obtained through CDD including copies and records of official documentation account files and business correspondence, for at least 5 years after the business relationship has ended, or after the date of the occasional transaction.

9.0 Non-Compliance

In circumstances where compliance with this Policy is not possible, a formal Policy waiver (email to the Nominated Compliance Officer) must be obtained.

Note: Waivers cannot be granted from any requirements or obligations imposed by domestic legal/regulatory obligations or international standards.
Non-compliance with, or violation of, the Policies requirements by employees and personnel of the Company may result in:

- Disciplinary action, including termination in appropriate cases; and/or,
- Civil and/or criminal penalties.

All rights to this document are reserved to Sovereignty SRL (© 2025).