

ANTI-MONEY LAUNDERING POLICY OF SA TECHNOLOGY N.V.

POLICY STATEMENT AND PURPOSES OF THIS POLICY

SA Technology N.V. takes a zero-tolerance approach to money laundering and terrorist financing activities and is committed to implementing and enforcing effective internal controls to counter such activities.

SA Technology N.V.'s policy is to apply at a minimum the standards set out in this Policy and is developed based on requirements of the applicable normative acts of the Curacao, European Union, Financial Action Task Force (FATF) recommendations and on generally accepted standards of international practice.

The purpose of this Policy is to:

- Set out the responsibilities of SA Technology N.V. and its all staff working for SA Technology N.V. in respect of observing, complying with, and upholding policies on Anti-Money Laundering (“**AML**”), Financing of Proliferation of Weapons (“**FP**”) and Counter-Terrorist Financing (“**CTF**”); and provide information and guidance to SA Technology N.V.
- Individuals on the money laundering/terrorist financing risks arising in relation to SA Technology N.V.'s activities, due diligence procedures, and how to recognise and deal with any potential money laundering/terrorist financing issues if they arise.
- This Policy may be amended from time to time to reflect updates to the laws and regulations on which it is based.

MONEY LAUNDERING, TERRORIST FINANCING AND FINANCING OF PROLIFERATION OF WEAPONS

Money Laundering (“**ML**”)

All acts done with money of illegal origin to change its identity so that it appears to have originated from a legitimate source, can be considered money laundering (ML). It is the process of making dirty money look clean. Money Laundering consists of three phases:

Placement - During this stage, the money launderer introduces the illegal proceeds into the financial system through financial institutions, shops and other cash intensive businesses. This is done among other things by buying chips for cash, then redeeming value without playing or with minimal playing, funding casino accounts with credit and debit cards, prepaid cards, checks and cryptocurrency and then requests for pay out and inserting funds into gaming machines and immediately claiming those funds as credits;

Layering - This stage involves converting the proceeds of crime into another form to disguise the audit trail, source and ownership of funds. It can involve transactions such as transfers of funds from one account to another, sometimes to or from other jurisdictions, currency exchange, structuring and refining and gambling accounts held for storing moneys and hiding them from the authorities;

Integration - The re-entry of funds into the economy in what appears to be normal business or personal transactions. Examples are: the purchase of luxury assets, financial investments, investing in gaming companies or commercial investments.

Terrorist Financing (“TF”)

Financing of Terrorism (FT) is the financing of terrorist acts, of terrorists and terrorist organizations. A terrorist act is an act to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.

The most basic difference between financing of terrorism and money laundering involves the origin of the funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. Money laundering always involves the proceeds of illegal activity.

There is a need for the terrorist group to disguise the link between it and its legitimate funding sources. In doing so, the terrorists use methods similar to those criminal organizations use to launder money like cash smuggling, structuring, wire transfers, purchase of monetary instruments, use of debit and credit cards. While ML is concerned with obscuring the source of funds, FT is mostly concerned with obscuring the end recipient of the funds.

Financing of Proliferation of weapons (FP)

Financing of proliferation (FP) is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

Targeted Financial Sanctions

Targeted Financial Sanctions require countries to freeze funds and assets and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of any designated persons or entities.

SA Technology N.V. is required to freeze all natural and legal persons without delay and without prior notice, the funds or other assets of designated persons and entities.

This is to comply with United Nations Security Council resolutions and the Common Foreign and Security Policy of the European Union. Compliance with sanctions imposed by the UN Security Council is mandatory under the Charter of the United Nations. EU sanctions are binding for Curaçao on the basis of the Kingdom Sanctions Act.

We have to check the sanction status of a withdrawing participant so that a sanctioned person or organization cannot remove money from an account that should be frozen. In such cases, a report must be filed with the FIU.

We are required to check for amendments of Sanctions Decrees and Regulations on a regular basis and update the CDD- and AML/CFT-policies and - procedures accordingly to reflect such amendments.

RISK ASSESSMENT OF SA TECHNOLOGY N.V.'S ACTIVITIES

Overview

SA Technology N.V. is required to apply a Risk-based Approach when designing policies, procedures and controls to combat money laundering, financing of terrorism and financing of proliferation of weapons. By adopting a Risk-based Approach, it is possible for SA Technology N.V. to ensure that measures to prevent or mitigate money laundering, financing of terrorism and proliferation of weapons are commensurate with the risks identified.

When drawing up the anti-money laundering compliance program, SA Technology N.V. takes a risk-based approach. That means the higher the risk, the more measures the SA Technology N.V. has to take to mitigate the risk. Where the risks are higher enhanced measures must be taken. Where the risks are lower, they may take simplified measures, provided that this is consistent with the country's assessment of its money laundering/financing of terrorism risks.

Applying Risk-based Approach means that SA Technology N.V. has to:

- Assess the risks that money laundering or terrorist financing may occur within the organization;
- Design and implement appropriate policies, procedures and controls to manage and mitigate the identified and assessed risks;
- Monitor and improve the effective operation of these policies, procedures and controls;
- Document their risk assessments, including everything that has been done and the reason for this being done.

The risk assessment considers all relevant risk factors, including the Customer, Countries or Geographic areas, Products, Services & Transaction and Distribution Channels before determining what the level of overall risk is. Based on the risk assessment, the appropriate level and type of mitigation to be applied is determined.

SA Technology N.V. should also take notice of the outcomes of the National Risk Assessment (NRA) of the jurisdictions where they operate and take these outcomes into account when conducting their risk assessment.

SA Technology N.V. applying the Risk-based Approach must document the policies, procedures and controls relative to the applied Risk-based Approach.

SA Technology N.V. must, on an on-going basis, monitor the effective operation of the policies, procedures and controls concerning the Risk-based Approach and, when needed, make the necessary amendments to these policies, procedures and controls.

The risk assessment should also be made available to the GCB upon request.

Customer Due Diligence

Introduction

SA Technology N.V. is prohibited from keeping anonymous accounts or accounts in obviously fictitious names.

SA Technology N.V. must identify the Customer and ask for the Customer's name and other relevant information to determine the purpose and nature of the business relationship.

Without sufficient knowledge, SA Technology N.V. may not establish or maintain a business relationship or carry out occasional transactions.

The customer's risk profile is essential to allow SA Technology N.V. to apply a certain level of Customer Due Diligence commensurate to the identified ML/TF risk.

The purpose of collecting information is to provide the SA Technology N.V. with documentation to assess the risk that may be associated with the Customer and to build a Customer profile to assess how the customer is going to act within the framework of the business relationship. Such an assessment is necessary in order to detect deviations from the expected behavior.

Any unusual behavior needs to be reported to the FIU. If FIU Curaçao, after proper analysis of an unusual transaction, concludes that there is a suspicion of money laundering and/or terrorism financing, this transaction will be reported to the Public Prosecutor's Office as a suspicious transaction.

SA Technology N.V. has the obligation to undertake Customer Due Diligence measures when:

- a. before establishing a business relationship with the customer;
- b. there is a suspicion of money laundering or terrorist financing;
- c. the SA Technology N.V. has doubts about the veracity or adequacy of previously obtained customer identification data.
- d. suspects that the customer or the customer's account is involved in ML/TF.

Whenever the Customers presents a high risk of ML/TF, the enhanced due diligence measures must be applied.

The CDD measures

The CDD measures to be taken are as follows:

- a. Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information;
- b. Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the SA Technology N.V. is satisfied that it knows who the beneficial owner is. For legal persons and legal arrangements this should include understanding the ownership and control structure of the customer;

c. Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;

d. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the SA Technology N.V. 's knowledge of the customer, its business and risk profile, including, where necessary, the source of funds.

The SA Technology N.V., their directors, officers and employees are prohibited to disclose the fact that an unusual transaction is being reported to the FIU.

A risk exists that customers could be unintentionally tipped off when the SA Technology N.V. is seeking to perform its CDD obligations in these circumstances. Therefore, if the SA Technology N.V. has a suspicion that transactions relate to ML or TF, it should take into account the risk of tipping-off when performing the CDD process.

If the SA Technology N.V., reasonably believes that performing the CDD process will tip-off the customers, it may choose not to pursue that process, and should file an unusual transaction to the FIU.

Customer Acceptance Policy (CAP)

SA Technology N.V. will accept only those customers whose identity is established by conducting due diligence appropriate to the risk assessment of the customer. Collecting sufficient and relevant data and documentation about the customer before the account relationship is established.

Accepting new customer

When accepting new customers, the responsible employees must act with the highest degree of care and caution in customer identification and identity verification. This applies also to the process of collecting necessary data, relevant information, and mandatory documentation.

Identification and verification of the customer

Identification refers to the collection of details of the customers to establish the identity of the customer. Verification on the other hand consists in confirming the customer details collected for identification purposes using reliable, independent source documents, data or information. The information required and extent of verification to be carried out, will vary depending on risk.

1. When establishing a new business relationship with the customers, SA Technology N.V. should identify the customer, at a minimum the following information and completed the Due Diligence ("DD") Form must be collected:

- Full legal name and trading name (if different);
- Certificate of Incorporation and subsequent Certificate of Change of Name, if applicable - Certification on copy documents must be within 6 months of submission date.
- Corporate and business registration number;

- Registered address and primary business address (if different) proof such as utility bills issued in the last 3 months;
- Nature/type of business; and
- If privately owned (i.e., not publicly listed):
 - Full names of Directors
 - Full names of any individual shareholders owning more than 25% of the entity (“beneficial owners”).
- Company Gaming Operations Details such as Intended URL(s) and Server Location (Jurisdiction)
- Certified copies of Passports/ ID cards for all UBOs, directors and authorized signatories - Certifications on copy documents must be within 3 months of submission date.
- Certified copy of Proof of Address for all UBOs, directors and authorized signatories - Certifications on copy documents must be within 3 months of submission date.
- Certified copy of a board resolution/ power of attorney/ M&A confirming the powers of the individuals to act as authorised signatories.
- Certified copy of Company charter documents (memorandum /articles of association) and any amending resolutions - Certifications on copy documents must be within 6 months of submission date.
- Ownership structural diagram of each Intermediate owner up to the Ultimate Beneficial Owners of the company, showing all companies and UBOs (signed by a Director or Company Secretary) - Certifications on copy documents must be within 6 months of submission date.
- Copies of Register of Directors and Register of Members (signed by a Director or Company Secretary) - Certifications on copy documents must be within 6 months of submission date.
- Original or certified copy of current dated Certificate of Incumbency/Good Standing (if Entities Incorporated Overseas) - Certifications on copy documents must be within 6 months of submission date.
- Certified copies of all gaming licenses and permits - Certifications on copy documents must be within 6 months of submission date.

2. Carry out a Customer Risk Assessment

This is done to have sufficient information available to detect unusual activity in the course of the business relationship. At this stage, a provisional risk rating will be assigned based on the initially collected information. This is revised once questions are answered or additional information received.

3. Verification of an identity refers to actions taken to verify that a person exists and is who he claims to be. This is done by checking reliable, independent (of the person whose identity is being verified) sources.

As a rule, verification of identity has to be carried out by making reference to an unexpired government-issued document containing identification information of the customers (e.g. (a) certificate of incorporation; (b) record in an independent company registry; (c) certificate of incumbency; (d) certificate of good standing;). Where such a document does not allow verification of the customer’s business address, the SA Technology N.V. can obtain other documents like a bank statement, utility bill, letter from a public authority or rental agreement, which should not be more than 3 months old to verify the address.

The SA Technology N.V. can also contact the customer by letter, e-mail or telephone to verify the information supplied. It can also send a verification code to the e-mail address to verify that the address is current and genuine. Verification can also be done by checking telephone, directories, company's registries and news sources.

There are also circumstances in which the SA Technology N.V. is able to cross reference the information in his possession with geo-location information, IP address data, funding method data etc.

Verification is carried out for the SA Technology N.V. to determine to its own satisfaction that the customer is who he declared himself to be. The documents should be clear, legible and of good quality.

Verification of evidence of identity implies a check whether the document presented is legitimate and that it has not been stolen from the true owner.

If we obtain foreign documentation, extra care should be taken with regard to verifying its authenticity, particularly where the type of document is unfamiliar.

Where the SA Technology N.V. does not have sufficient comfort that it knows its customers, it is expected that it will take additional measures to do so. Some of these measures include requesting additional identification documents, asking the customers to provide a photo of himself holding the ID, requiring a first payment through an account held in a reputable jurisdiction, using systems which generate codes for transmission to customers through a verified mobile phone and requiring it to be returned.

Sanctions screening and PEP status screening

All customers should be screened against sanctions lists of the UN and EU. If Curaçao publishes a local list with designated persons and organizations, the SA Technology N.V. should also take that local list into account.

The SA Technology N.V. must ensure it does not do business with customers that are subject to international sanctions or in Prohibited Country List. Before doing business or performing an occasional transaction for the first time with the customers, the SA Technology N.V. should check published lists of known or suspected terrorists or other sanctioned persons or companies:

- U.S. Treasury's Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons List <https://sanctionslist.ofac.treas.gov/Home/SdnList>
- EU Sanctions List <http://www.sanctionsmap.eu/#/main>.

For PEP status screening SA Technology N.V. can rely on internet search or consult reports and databases on corruption risk, like the Transparency International Corruption Perceptions Index or on www.knowyourcountry.com.

Identification and verification of the Beneficial Owner

SA Technology N.V. in general, are also required to identify and verify the identity of the beneficial owner. As a general rule, SA Technology N.V. should make sure that customers are registering an account to transact on their behalf. This can be achieved by including specific wording in the terms and conditions that a registering customers must explicitly accept, together with a declaration in the form of a tick box that the customer is transacted on his/her own behalf. SA Technology N.V. is not expected to merely rely on said declaration, but have to ensure that their ongoing procedures allow for the detection of possible instances where the customer is actually playing on behalf of third parties.

SA Technology N.V. must in case of business participants obtain satisfactory evidence to identify the business participants. It has to take reasonable steps to verify the identity of the beneficial owner, using information or data that was obtained from a reliable source.

At the minimum identification information, verification and evidence must be gathered for all persons holding 25% or more of the shares or voting rights or a person who otherwise exercises ultimate effective control of the customer. Where no natural person is identified under the 3 items mentioned above, the natural person who holds the position of senior managing official should be identified.

Obtaining information on the Purpose and Intended Nature of the Business Relationship

SA Technology N.V. has to collect sufficient information and, where it is necessary, documentation to establish a customer's source of wealth as well as the expected level of activity.

Source of wealth consists of determining the activities which generate the customer's net worth and whether this justifies the projected and actual level of account activity. As to the extent of the information that SA Technology N.V. is to collect, it is essential that this reflects the level of ML/FT risk identified through the customer risk assessment.

Where the risk is not high, a declaration from the customer with some details (e.g. nature of business, usual income etc.) can be sufficient. Social media can also be used as a source of information.

However, where the risk of ML/FT is higher or SA Technology N.V. has doubted as to the veracity of the information collected, the information obtained would need to be substantiated by independent and reliable information and documentation.

In developing a customer risk profile, SA Technology N.V. may also consider using statistical data to develop behavioural models against which to eventually gauge a customer's activity rather than collect source of wealth information. Where a SA Technology N.V. opts to adopt this approach, it can use data collected from the Central Statistics Department such as average national income, average disposable income etc.

It is important to note that the use of statistical data is incompatible with high-risk situations as the transactional pattern will fall outside the average behavioural model. In such circumstances, SA Technology N.V. would have to collect source of wealth information as set out above.

In developing a customer business and risk profile, SA Technology N.V. form the basis for the scrutiny of activity required to meet part of their on-going monitoring obligation.

On-Going Monitoring

The SA Technology N.V. must conduct ongoing due diligence on the business relationship and scrutinize the transactions undertaken throughout the course of that relationship to ensure that they are consistent with the SA Technology N.V.'s knowledge of the customer, the customer's business and risk profile.

Ongoing monitoring of identity

In conducting ongoing due diligence on the business relationship, the SA Technology N.V. should hold accurate and up to date identification data of its customers.

Since identity may change due to circumstances, the SA Technology N.V. should be able to show that if identification information changes, it will be detected and re-evidenced.

This means that the SA Technology N.V. should consider to obtain evidence of identity periodically to detect any changes, refresh the data on key events (i.e. change of payment instrument) or should consider tracking expiry dates on evidence of identity and refreshing it as it expires. SA Technology N.V. should determine on a risk-sensitive basis whether changes are substantial as to require re-assessment of customer risk of the business relationship.

Ongoing monitoring of transactions

Transaction monitoring is executed to prevent involvement of the SA Technology N.V. with ML/TF and to safeguard the reputation of the SA Technology N.V.

While in conducting ongoing scrutiny of transactions SA Technology N.V. notices that customer's transactions are not consistent with what it knows or expects from the customer, the SA Technology N.V. has to question this unusual activity and, where necessary, establish the source of the funds used for that transaction.

Source of funds refers to how the funds for a particular transaction were obtained by the customers.

The SA Technology N.V. has to understand what the reason for this deviation is and obtain sufficient information and documentation with regard to the transaction. It is also one of the situations in which the risk profile of the customer may have to be revised.

After receiving this information, the SA Technology N.V. has to decide whether the transaction is an unusual transaction and need to be reported to the FIU.

Timing of CDD Measures

For SA Technology N.V., should verify the identity of a customer and any beneficial owner of the customer before or during the course of establishing a business relationship and conduct the sanctions screening & PEP status screening.

However, SA Technology N.V. may exceptionally verify the identity of a customer and any beneficial owner of the customer after establishing the business relationship, provided that:

- (a) any risk of ML/TF arising from the delayed verification of the customer's or beneficial owner's identity can be effectively managed;
- (b) it is necessary not to interrupt the normal conduct of business with the customer;
- (c) verification is completed as soon as reasonably practicable;
- (d) keeping senior management periodically informed of any pending completion cases;
- (e) ensuring that funds are not paid out to any third party.

Enhanced Due Diligence

A risk-based approach should be taken, so more thorough checks should be undertaken for higher risk customers. The Enhanced Due Diligence (EDD) measures should be consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual.

Enhanced Due Diligence has to be conducted where the risks of money laundering or terrorist financing are higher. This concerns for example:

- Customers of higher risk geographic areas;
- Political Exposed Persons (PEPs);
- Products or transactions that might favour anonymity;
- 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.

The applied measures must be consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

Examples of enhanced due diligence measures include:

- Obtaining additional information on the customer, like previous address and information available through public databases, internet, etc.;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining information on the source of funds or source of wealth of the customer
- Obtaining information on the reasons for intended or performed transactions;
- Obtaining the approval of senior management to commence or continue the business relationship;
- Conducting enhanced monitoring of the business relationship;
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

In situations presenting a higher risk of ML/TF, source of funds information has to be requested from time to time even though there may not be any change in pattern or activity conducted by the customer.

Simplified Due Diligence

Where the risks of money laundering or terrorist financing are lower, SA Technology N.V. is allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk.

Examples of possible measures:

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship;
- Reducing the frequency of customer identification updates;
- Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

Politically Exposed Persons

SA Technology N.V. is required, in relation to foreign politically exposed persons (PEPs), (whether as customer or beneficial owner) in addition to performing normal customer due diligence measures, to:

- a. has appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;
- b. obtain senior management approval to service the PEP (for establishing the business relationship for new customers, continuing the business relationship for existing customers or for conducting the occasional transaction). Senior management are the persons who determine the day-to-day operations or those directly below the level of those determining the day-to-day operations. The approval can also be from the Money Laundering Reporting Officer;
- c. take reasonable measures to establish the source of wealth and the source of funds. The investigation must then determine whether the customer's spending pattern matches his legal source of funds.

SA Technology N.V. requests a statement from the customer about the source of funds and verifies them by consulting independent and reliable sources. Depending on the risk in specific cases, this can in the first place be public sources. When public sources cannot, or can insufficiently verify the received information, SA Technology N.V. can request the customer to provide documents; and

- d. conduct enhanced ongoing monitoring of the business relationship.

SA Technology N.V. is required to take reasonable measures to determine whether a customer is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization.

In cases of a higher risk business relationship with such persons, SA Technology N.V. is required to apply the measures referred to in items b, c and d.

The measures are tailored to the risk of the PEP, where the following is taken into consideration:

- the type of public function of the PEP;
- the country from which the PEP originates;
- the transactions that the PEP carries out.

The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

Screening for PEP status has to be carried out before establishing the business relationship or conducting the occasional transaction. In addition, SA Technology N.V. must regularly screen for PEP status during the business relationship.

Application of CDD measures to existing customers

SA Technology N.V. should also apply the CDD measures to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

All customers that present high ML/TF risks should be subject to a minimum of an annual review, medium ML/TF risks should be reviewed every two years, low ML/TF risks should be reviewed every three years or more frequent reviews if deemed necessary by the SA Technology N.V. to ensure the CDD information retained remains up-to-date and relevant.

The termination of the business relationship

In case the obligations arising from the customer due diligence cannot be met, the SA Technology N.V. cannot establish the business relation or perform the transaction or it is obliged to terminate the business relationship with the customer.

SA Technology N.V. must also keep a record of all the attempts made to get the necessary information and documentation. To this end, SA Technology N.V. may decide to either close the account or to keep it blocked and suspended in its entirety.

SA Technology N.V. is to consider whether there are any grounds giving rise to suspicion of ML/TF/FP.

The reluctance of the customer to provide CDD on its own should not be automatically equated to a suspicion of ML/TF/FP. SA Technology N.V. should consider all factors and information it has at his disposal to decide whether there are grounds to suspect ML/FT/FP. If, however the presumption of ML/FT/FP exist the SA Technology N.V. should submit an unusual transaction report to the FIU with regard to this customer.

Where there is no reason for the retention of funds, the funds are to be remitted back to the customer. This has to be done through the same channels used to receive the funds.

Reliance on third parties to perform customer due diligence

SA Technology N.V. may rely on third parties when performing the CDD measures, provided that the criteria set out below are met. The ultimate responsibility for ensuring that CDD requirements are met remains with the SA Technology N.V.

The third party should be subject to CDD and record-keeping requirements.

The criteria to be met are as follows:

1. SA Technology N.V. should have an agreement with the third party being relied upon that copies identification data or other relevant documentation relating to CDD requirements will be made available upon request and this arrangement must be tested from time to time to ensure that it actually functions as set out in the agreement. The SA Technology N.V. however, remains responsible for the carrying out of a customer-based risk assessment, determining whether the customer is a PEP and conducting on-going monitoring; .
2. SA Technology N.V. should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and recordkeeping requirements.
3. SA Technology N.V. should be periodical assessments of how the service provider is fulfilling its obligations under the outsourcing arrangement both quantitatively as well as qualitatively. However, the decision whether to on-board a customer or to continue a business relationship on the basis of risk cannot be outsourced.

The Business Risk Assessments (BRA)

SA Technology N.V. is required to carry out a business risk assessment to identify the ML/TF risks to ensure that the policies, controls and procedures adopted are adequate to prevent and mitigate those risks.

The risk assessment should address the ways in which the SA Technology N.V.'s products and services could be used to launder money, finance terrorism and finance proliferation and the extent of the risk that this will happen. All factors that may have an impact on the risks of money laundering, financing of terrorism and financing of proliferation must be taken into account in the risk assessment, but special consideration must be given to the type of customers, products and services offered, delivery channels and geographical risk factors including outcomes and recommendations of the National Risk Assessment in their business risk assessment.

SA Technology N.V. could expect to revise the business risk assessment whenever there are changes to the environment within which they are operating and within their business activities, such as introduction of new payment methods, new markets or regulatory changes.

In the absence of changes, SA Technology N.V. have to assess the business risk at least once a year, to evaluate whether any changes thereto are necessary.

This risk assessment has to be documented and approved by the Board of directors of the SA Technology N.V.

It should also be made available to the GCB upon request.

All aspects of the Business Risk Assessment should be covered, including:

- The methodology adapted;
- The reasons for considering a risk factor as presenting a low, medium or high risk;
- The outcome of the BRA;
- Any information sources used.

In order to work risk-based, it is important that SA Technology N.V. continuously follow the latest reporting regarding money laundering and terrorist financing.

Customer Risk Assessment (CRA)

The customer specific risk assessment has to be carried out either prior to the carrying out of an occasional transaction, or prior to the establishing a business relationship.

The information collected to draw up the CRA will formulate the customer's risk profile.

Policies, Procedures and Controls

SA Technology N.V. must establish and maintain policies, procedures and controls to mitigate and manage effectively the risks identified in the operator's risk assessment of money laundering, terrorist financing and proliferation of weapons.

The measures, policies, controls and procedures to mitigate ML/FT/FP risk are to include:

1. Customer Due Diligence (CDD);
2. Record keeping procedures;
3. Reporting procedures;
4. Risk management measures including Customer Acceptance Policies (CAP), Customer Risk Assessment (CRA) procedures, internal control, compliance management and communications of such policies, procedures and controls, employee training and employee screening policies and procedures.

It is important that these measures are clearly documented and approved by the Board of directors.

SA Technology N.V. should monitor the implementation of those controls and enhance them if necessary.

It should take enhanced measures to manage and mitigate the risks where higher risks are identified.

There are four risk areas that the business risk assessment and the customer-specific risk assessment have to cover and that are likely to pose a higher-than-average risk of ML/FT/FP. These are:

1. Customer risk

Customer risk is the risk of ML/TF that arises from maintaining relations with a given Customer. The assessment of the risk based on Customer's economic activity and/or source of wealth.

Categories of customers whose activities may indicate a higher risk include:

- Customers who have multiple sources of income;
- PEPs;
- Disproportionate spenders (inconsistent with Customer's information about customer's known source of income/assets);
- Whether source of funds is generated from own economic activity or whether reliance is placed on others;
- Whether the apparent source of the Customer's activity can easily be verified;
- Frequent and unexplained movement of accounts to different entities.

2. Geographical risk

The geographical risk is the risk posed to the geographical location of the Customers and the source of wealth of the business relationship.

Countries that have a weak AML/CFT system, countries known to suffer from a significant level of corruption, countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction and countries which are known to have terrorist organizations operating are to be considered as high risk, such as of the following:

- Countries on the FATF list of High - Risk Jurisdictions subject to a Call for Action;
- Countries on the FATF list of Jurisdictions under Increased Monitoring;
- Countries on the CFATF Public Statement;
- Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR);
- Countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime;
- Countries sanctioned by the OFAC;
- Countries identified by credible sources as providing funding or support for terrorist activities or have terrorist organizations operating within them;
- Countries on the Corruption Perception Index compiled by Transparency International.

SA Technology N.V. must have a list of countries that are considered as high risk and those that are considered low risk.

3. Product, service and transaction risk.

Some products or services are inherently riskier than others and are therefore more attractive to criminals. These include products or services which are identified as being more vulnerable to criminal exploitation such as gaming products or services that allow the customer to influence the outcome of a game, be it individually or in collusion with others. These include:

- Proceeds of crime. Risk that money transferred is derived from illegal activities such as check fraud, narcotics trafficking;
- Provide products and services to new customer (i.e., operator) or third-party distributor that are inherently riskier than others and a likelier channel for criminal activity.

4. Distribution channels risk

The channels through which the Customers establish a business relationship or through which transactions are carried out may also have an impact on the risk profile of a business relationship or a transaction:

- Channels that favor anonymity increase the risk of ML/FT if no measures are taken to address the risk;
- Where there is the involvement of a third party in the interactions between SA Technology N.V. and the customer, there is also an increase of risk. This is especially the case where these third parties are not themselves subject to any form of AML/CFT obligations.

Technological developments risk assessment

SA Technology N.V. should maintain appropriate procedures and controls for preventing the misuse of technological developments for the purpose of money laundering or the financing of terrorism. It should identify and assess the money laundering or terrorist financing risks that may arise whenever:

- A new product is developed;
- A new business practice emerges;
- A new delivery mechanism becomes available;
- A new or developing technology is used for both new and pre-existing products.

In those cases, a risk assessment should take place prior to the launch of the new products, business practices, delivery mechanism or the use of new or developing technologies. This is done to determine whether the innovation creates a weakness that can be misused by money launderers or those seeking to finance terrorism. Such risk assessments must be documented.

Where risks are identified, measures must be taken to mitigate these risks.

Reporting of unusual transactions

Reporting obligations

SA Technology N.V. is required to detect and report either intended or completed unusual transactions. It is important for SA Technology N.V. to have adequate procedures in place that covers the following:

- a) The recognition of unusual transactions;
- b) The documentation of unusual transactions; and
- c) The reporting of unusual transactions.

Recognition of unusual transactions

An unusual transaction is a transaction inconsistent with the customer's profile. Therefore, the first key to recognizing that a transaction or series of transactions is unusual is to know enough about the customer.

The purpose of collecting information is to provide SA Technology N.V. with documentation to assess the risk that may be associated with the customer and to build a customer profile to assess how the customer is going to act within the framework of the business relationship.

Based on the National Ordinance on a customer's transaction qualifies as an unusual transaction. the Reporting of Unusual Transactions (NORUT) legislation, objective and subjective indicators have been established by means of which SA Technology N.V. must assess whether a customer's transaction qualifies as an unusual transaction.

Management must provide its staff with specific guidance and training in recognizing and adequately documenting unusual transactions. All these unusual transactions must be reported to the Money Laundering Reporting Officer in the format approved by management.

All additional documents available, such as copies of identification documents and other records must be also submitted as supplements. The Money Laundering Reporting Officer must keep an adequate filing system of these records.

If internally reported transactions are not reported to the FIU, the reason shall be adequately documented and signed off by the Money Laundering Reporting Officer and/or management.

In order to implement FATF recommendation 11, SA Technology N.V. must pay special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

The following transactions or intended transactions are deemed unusual:

- a. Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
- b. Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- d. Presumed money laundering transactions or terrorist financing: Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

Reporting of unusual transactions

By virtue of article 11 of the National Ordinance on the Reporting of Unusual Transactions (NORUT), SA Technology N.V. must report unusual transaction or any intended unusual transaction to the FIU without delay.

All unusual individual transactions or series of transactions, as mentioned in the Regulation Indicators Unusual Transactions, must be reported internally, without any delay. Also supporting documents must be submitted as part of the reporting.

The documentation of unusual transactions

SA Technology N.V. has to register with the FIU and to get access to the goAML reporting portal after validation by the FIU.

The Money Laundering Reporting Officer must prepare a report of all unusual transactions for external reporting to the FIU according to the reporting regulations of the FIU.

SA Technology N.V. shall report to the FIU the details of the transactions by means of the goAML reporting portal. The reports and the submission of the thereto related information (all supporting documents) should be done in English.

SA Technology N.V. and its directors, officers and employees are protected by law from criminal and civil liability for breach of any restriction on disclosure of information when reporting to the FIU.

Prohibition of disclosure

SA Technology N.V. and its senior management and employees shall not disclose any details or information in connection with a report filed to the FIU or a request for information made by the FIU.

They are not permitted to disclose information to the customer nor to third parties.

Record Keeping

SA Technology N.V. shall maintain, for at least five years, all necessary records on transactions (both domestic and international), to enable them to comply with information requests from the competent authorities.

Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

All records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence must be kept for at least five years after the business relationship is ended, or after the date of the occasional transaction.

The CDD information and the transaction records should be available to domestic competent authorities based upon appropriate legal authority.

Anti-Money Laundering Compliance Program

Introduction

An anti-money laundering program is an essential component of SA Technology N.V.'s compliance regime.

The primary goal of every good program is to protect the organization against money laundering and to ensure that the organization is in full compliance with relevant laws and regulations.

An AML program should be risk-based, and should be designed to mitigate the money laundering and terrorist financing risks the organization may encounter.

The AML program should establish minimum standards for the organization that are reasonably designed to comply with applicable laws and regulations.

The basic elements of SA Technology N.V. must address in an anti-money laundering compliance program are:

1. A system of internal policies, procedures and controls;
2. A designated Money Laundering Reporting Officer with day-to-day oversight over the AML program;
3. An employee screening program and ongoing employee training program; and

The anti-money laundering program also ensures that the obligations regarding customer due diligence, reporting unusual transactions, retention periods, data protection and training are met.

The AML program has the approval of senior management.

SA Technology N.V. must ensure that their foreign branches and subsidiaries, if any, implement AML/CFT/CFP measures consistent with the requirements of Curaçao.

A system of internal policies, procedures and controls

SA Technology N.V. must have policies and procedures, including a policy statement in place that clearly expresses the senior management's commitment to combat the abuse of its facilities, products and services for the purpose of money laundering, terrorist financing and the proliferation of weapons of mass destruction purposes.

SA Technology N.V. shall also have a process in place to stay on top of regulatory changes, which should keep the program current.

The anti-money laundering policies and procedures should be in writing and shall be approved by senior management or the board of directors. SA Technology N.V.'s policies and procedures shall be communicated to its employees.

The appointment of a Money Laundering Reporting Officer

SA Technology N.V. shall formally designate a senior officer at management level and independent from the operations, responsible for the detection and deterrence of money laundering and terrorist financing.

The Money Laundering Reporting Officer must have timely access to customer identification data and other CDD information, transaction records, and other relevant information.

The Money Laundering Reporting Officer must be able to act independently. The Money Laundering Reporting Officer shall be assigned at least the following responsibilities:

- To design and implement the AML program;
- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- To review compliance with SA Technology N.V.'s policy and procedures;
- To organize training sessions for the staff on various compliance-related issues;
- To analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- To review all internally reported unusual transactions for their completeness and accuracy with other sources;
- To keep records of internally and externally reported unusual transactions;
- To execute closer investigation of unusual transactions if necessary;
- To prepare the external report of unusual transactions;
- To make necessary changes to the AML program;
- To remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements; and
- To prepare periodic information against money laundering and financing of terrorism and financing of proliferation.

The above-mentioned responsibilities shall be included in the job description of the Money Laundering Reporting Officer. The job description shall be signed off and dated by the officer, indicating his/her acceptance of the entrusted responsibilities.

Name of the Money Laundering Reporting Officer: Raffaele Magliulo

Email: compliance@sagaming.com

Employee screening program and ongoing employee training program

SA Technology N.V. shall ensure that their business is conducted at a high ethical standard and that the laws and regulations pertaining to financial transactions are followed.

SA Technology N.V. shall establish and adhere to proper policies and procedures in screening their employees for criminal records.

SA Technology N.V. shall develop training programs and provide training to all personnel who handle transactions that may be qualified as unusual based on the indicators outlined in the Ministerial Decree regarding the Indicators for Unusual Transactions (N.G. 2015 no. 73).

Training includes setting out rules of conduct governing employee's behavior and their ongoing education to create awareness of the SA Technology N.V.'s policies against money laundering and terrorist financing.

Training must at least address the following person:

a) New employees

A general training of the nature and process of money laundering and terrorist financing, and the need to report any unusual transactions to the Money Laundering Reporting Officer must be provided to all new employees who will handle customers or their transactions, irrespective of their level of seniority.

They shall be made aware of the existing internal policies, procedures and regulations concerning money laundering, terrorist financing, proliferation of weapons and the reporting requirements.

They must also be trained on the money laundering methods and trends. They must receive an explanation on customer due diligence and objective and subjective indicators for reporting unusual transactions.

b) AML Compliance staff

These are the people who run the AML program. They will need specialized training to be able to stay on top of new trends or changes that impact the organization and the way it manages risk. This will require attending conferences or AML-specific presentations to go into greater detail.

c) Supervisors and Managers

A higher level of instruction covering all aspects of money laundering, terrorist financing policies, procedures and regulations must be provided to those with the responsibility to supervise or manage the staff.

d) Senior management and board of directors

Money laundering issues and dangers should be regularly and thoroughly communicated to the board. This to keep board members aware of the reputational risk that money laundering poses to the institution.

Refreshment training must be arranged at regular intervals to ensure that staff members are kept informed of current and new developments regarding money laundering and terrorist financing techniques, methods and trends.

To demonstrate compliance with aforementioned staff training guidelines, SA Technology N.V. shall maintain records that include:

- Details on the content of the training programs;
- The names of the staff members who have received the training;
- The date on which the training was provided;

- The results of any testing carried out to measure staff understanding of money laundering and terrorist financing requirements; and
- An ongoing training plan.

Examination by the Regulators

SA Technology N.V. shall provide information or documentation on the money laundering and terrorist financing policies and deterrence and detection procedures to the examiners during an examination and upon Regulators request during the year. SA Technology N.V.

SA Technology N.V. shall make the following items readily available:

- a. Its written and approved AML Compliance Program on money laundering, terrorist financing and financing of proliferation;
- b. Records of its Business Risk assessment;
- c. The name of each Money Laundering Reporting Officer responsible for the SA Technology N.V.'s overall money laundering and terrorist financing policies and procedures and his/her designated job description;
- d. Records of reported unusual transactions;
- e. Records of unusual transactions which required closer investigations;
- f. Records of frozen accounts;
- g. Schedule of the training provided to the SA Technology N.V.'s personnel regarding money laundering, terrorist financing and proliferation of weapons;
- h. The assessment report on the SA Technology N.V.'s policies and procedures on money laundering, terrorist financing and financing of proliferation by the internal audit department or an external auditor;
- i. The customer's files including customer risk assessment, CDD, customer acceptance and transaction information.

Annex 1 Definitions

Close associates' means:

- Natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person;
- Natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

Family members include the following:

- The spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;
- The children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person;
- The parents of a politically exposed person;

NOIS

National Ordinance on Identification of Clients when rendering Services

NORUT

National Ordinance on the Reporting of Unusual Transactions

Politically Exposed Persons (PEPs)

Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country and the direct family members or close associates of such persons. Examples are:

Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

Source of Funds

Refers to how the funds for a particular transaction were obtained by the customers, like personal savings, pension release, property sales, share sales and dividends, gifts, compensation from legal rulings.

Source of Wealth

Source of wealth is the origin of all the money a person has accumulated over their lifetime, like employment income, inheritances, investments, business ownership interests.

(Ultimate) beneficial ownership (UBO)

Refers to the natural person(s) who ultimately own(s) or control(s) a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person.

Date: November 29, 2024