Bridge Technologies B.V

Anti-Money Laundering and Combating the Financing of Terrorism Compliance Manual

Version 1.1

June 2025

Contents

1 Introduction

This manual is for the use of the management and employees BRIDGE TECHNOLOGIES B.V. (“BT”) as a guide to their Anti-Money Laundering and Counter- Terrorist Financing (“AML/CFT”) responsibilities. BT a company registered in Curacao.

In particular, this manual contains information which all members of staff need to be aware of in order to prevent the business being used to launder the proceeds of crime or for terrorist financingand any activity that facilitates money laundering or the funding of terrorist or criminal activities andto comply with all applicable requirements and regulations.

For the purposes of this policy a customer is an individual who has entered a business relationship and who has signed an ongoing service agreement with BT.

The remote gambling sector has been assessed by MONEYVAL, which published their findings in the Fifth Round Mutual Evaluation Report in July 2019. The report on behalf of the Financial Intelligence Analysis Unit (FIAU) and the Curacao Gaming Commission (CGC) identified the gambling sector as being higher inherent and residual risk for money laundering and terrorist financing relative to other gambling sectors. The risk assessment conducted during 2018, with initial results specific to the gaming sector published in October 2018.

BT is made up of multiple casino websites/brands. In light of this, this risk assessment document assesses the core money laundering and terrorist financing risks holistically across the BT network focusing on the four risk areas inherent in the gaming sector broken down as:

- Customer Risk;
- Product Service and Transaction Risk;
- Interface Risk;
- Geographical Risk;
- Nature and Behaviour Risk
- Reputation Risk

BT has a trained nominated officer/MLRO in place - anti-money laundering (AML) and terrorist financing risk (TFR) matters are regularly considered by BT senior management and potential AML/TFR cases are always escalated by the MLRO (or relevant staff member) accordingly.

Analysis of money laundering and terrorist financing vulnerabilities has been carried out by the Central Fraud team (CF team) in conjunction with the Compliance team. Each vulnerability is supported by evidence, intelligence and data. It also takes into consideration the CGC risk assessment.

The vulnerabilities identified are a point in time. Therefore, the CF team together with the Compliance team will add to the risk assessment emerging or new vulnerabilities on an annual basis, or sooner as required.

As set out in BT’s AML/CTF Policy, it follows a risk-based approach and employs systems and controls to prevent ML/TF activity in the following areas:

- Customer Verification;
- Customer Due Diligence;
- Ongoing Customer Monitoring;

- Reporting;
- Record Keeping; and
- Staff Due Diligence and Training.

Risk Assessment Methodology

This risk assessment considers the risks associated with customer activity, payments, geography, products and employee risk. Each risk identified is subject to mitigation, monitoring and documented control and review. In assessing each risk, the probability and impact are considered to calculate a total risk score to be assigned to each risk.

Risk probability – this is the likelihood of an identified Money Laundering (**ML**)/Terrorist Financing (**TF**) risk materialising.

Risk impact – this is the expected damage to BT should an identified ML/TF risk materialise. The impact of all risks is not identical; some may have a greater impact than others. In line with GAMLG industry guidance, the following factors have been considered when determining the impact of an identified risk:

- Facilitation of criminal conduct;
- Risk of regulatory fines/licence review and legal prosecution; and
- Reputational damage.

Each risk is given a severity of risk impact rating using a scale of 1-5. These are categorised as:

1 Insignificant
2 Minor
3 Moderate
4 Major
5 Severe

Each risk is also given a probability rating of 1-5 as follows:

1 Remote
2 Unlikely
3 Possible
4 Likely
5 Extremely likely

Multiplying both the risk probability and risk impact provides a total risk score for each risk identified. This enables BT to accurately assess the AML risks to ensure appropriate controls are in place to mitigate them. The control score is the risk score after the mitigation has been applied to the risk, thus reducing that risk score to an acceptable level.

Customer risk

Nature of risk	Risk score	
False documentation used to bypass controls.	Probability	1
	Impact	4
	Total	4
Mitigation of risk (Controls)	**Control Score**	
Where customers cannot be electronically verified, documentation is requested and uploaded to Shufti Pro for automated validation. Documents which fail the automated verification process are brought to the attention of the CF team, and are then subject to scrutiny of the trained CF team. Face ID can be requested through the Shufti Pro service, where the documents may raise concerns.	Probability	1
	Impact	2
	Total	2

Nature of risk	Risk score	
Customers may attempt to withdraw deposits following minimal play or following low risk activity on games where there is a high return to player percentage in an attempt to launder money and have it appear in the financial system as gambling winnings.	Probability	4
	Impact	4
	Total	16
Mitigation of risk (Controls)	**Control Score**	
The CF team have monitoring in place designed to assess this risk. All large withdrawals and high aggregate or individual deposits are reviewed for unusual activity, such as minimal play, and appropriate action taken.	Probability	2
	Impact	3
	Total	6

Nature of risk	Risk score	
A casino account could assist the disguise of funds destined to be used to support terrorism.	Probability	1
	Impact	4
	Total	4
Mitigation of risk (Controls)	**Control Score**	
Monitoring by the CF team takes place, but the amounts involved may be small and may come from legitimate sources. Open-source searches may reveal links (e.g. address) to known terrorist suspects. Open-source checks on username may also reveal identity of potential terrorist as advised by UK Metropolitan Police Counter Terrorism Unit. In addition, transactional IP monitoring in place to highlight any IP's coming from high-risk countries e.g. Iraq.	Probability	1
	Impact	2
	Total	2

Nature of risk	Risk score	
Abnormal activity – frequency and size of transaction.	Probability	4
	Impact	4
	Total	16
Mitigation of risk (Controls)	**Control Score**	
Where size or frequency of deposit or withdrawal behaviour is abnormal either as assessed against the customer base overall or against the previous pattern of an individual customer will prompt further consideration and may result in a request to the customer for documentation to prove source of wealth/funds.	Probability	2
	Impact	3
	Total	6

Nature of risk	Risk score	
Customers displaying behaviours which may indicate problem gambling behaviour could also be linked to ML.	Probability	4
	Impact	5
	Total	20
Mitigation of risk (Controls)	**Control Score**	
Staff are trained to consider abnormal transactional behaviour in the light of both social responsibility and AML. The Customer Intelligence and Responsible Gambling Review Committee considers this dual aspect of each account referred to it.	Probability	2
	Impact	3
	Total	6

Product, Service & Transaction Risk

Nature of risk	Risk score	
The use of multiple deposit methods may indicate the use of criminal funds.	Probability	4
	Impact	4
	Total	16
Mitigation of risk (Controls)	**Control Score**	
The CF team monitors this risk using Adyen and EPG reporting tools. In addition to using the detection tool, the CF team have a built-in mechanism to prevent more than three payment methods being used in a 24-hour period. Furthermore, the CF team review reports every 24 hours for customers using multiple deposit methods. In the event multiple payment methods are used, a review of the customer's account is undertaken.	Probability	2
	Impact	2
	Total	4

Nature of risk	Risk score	
A customer who wishes to withdraw funds using a different payment method to that used for deposit may be attempting to move criminal funds.	Probability	4
	Impact	4
	Total	16
Mitigation of risk (Controls)	**Control Score**	
BT operate a closed loop system, meaning withdrawals are processed to their depositing method. Where this is not possible, account activity is reviewed for potential concerns on a risk-based approach before sending to the chosen withdrawal method. Documents to evidence ownership of the outgoing method may be requested where appropriate.	Probability	2
	Impact	3
	Total	6

Nature of risk	Risk score	
Products offered to deposit	Probability	3
	Impact	3
	Total	9
Mitigation of risk (Controls)	**Control Score**	
Ten payment providers offer deposit options and service players under our CGC licence. These are: 1. CleanPay 2. ApcoPay 3. Ezeebill 4. Gumball Pay 5. PayNetEasy 6. Inpay 7. DNS 8. Alphapo	Probability	2
	Impact	3
	Total	6

All of the providers are EU, EEA or FCA regulated. None of the e-wallets listed, accept direct cash deposits. Pre-Paid Cards, E-wallets and vouchers are monitored by the CF team on a daily basis and all depositors > 1000EUR may have further due diligence performed.		

Nature of risk	**Risk score**	
Corporate card usage may facilitate the unauthorised use of company funds	Probability	4
	Impact	5
	Total	20
Mitigation of risk (Controls)	**Control Score**	
The use of corporate cards is automatically blocked using the Adyen product and the transaction will not be successful.	Probability	1
	Impact	1
	Total	1

Nature of risk	**Risk score**	
Customers may use stolen cards or the cards of 3rd party relatives/friends.	Probability	3
	Impact	4
	Total	12

Mitigation of risk (Controls)	Control Score	
3D secure authentication must be used for all cards. As a policy, third party cards are not permitted. If third party cards are used, the player is monitored by the CF team on a daily basis. The third-party card will also be banned from further use. If a third-party card is used more than twice, the customer is then banned from the network. A monitoring report is created every 24 hours which includes a detection of stolen cards.	Probability Impact Total	2 3 6

Nature of risk	Risk score	
Customers may use a gambling account as a “safe” place to deposit criminal money for a prolonged period of time.	Probability Impact Total	3 3 9
Mitigation of risk (Controls)	**Control Score**	
The CF team monitors large balances on a weekly basis.	Probability Impact Total	1 3 3

Nature of risk	Risk score	
The use of digital/cryptocurrencies presents a higher risk for the movement of criminal funds.	Probability Impact Total	4 5 20

Nature of risk	Risk score	
Card deposits declined by a customer’s bank may indicate the use of a card which does not belong to the customer.	Probability Impact Total	3 3 9
Mitigation of risk (Controls)	**Control Score**	
It is recognised that we, as is the case with other operators, cannot completely mitigate such risk. However, the CF team review multiple declines (for whatever reason) along with multiple card usage (as discussed above). In addition, multiple card deposit declines for higher-risk customers are reviewed by the Responsible Gambling and Customer Intelligence Review Committee during weekly meetings.	Probability	2

Declined card deposits also form part of BT's RG matrix.		

Nature of risk	**Risk score**	
The operation of multiple brands may mean that an individual is able to open several accounts and avoid relevant thresholds for ML/TF by breaking down large amounts into small separate transactions.	Probability	4
	Impact	4
	Total	16
Mitigation of risk (Controls)	**Control Score**	
Only one account may be operated by an individual with a single brand. Details are automatically checked on registration and duplicates cannot be opened. Any and all unusual customer activity will prompt review of customer behaviour across all brands accounts (if they hold another account/s). When an account reaches the thresholds set out in the verification policy, the CI team will check for and consider customer activity on other brands.	Probability	2
	Impact	3
	Total	6
Nature of risk	**Risk score**	
Employees may potentially pose a ML/TF threat by colluding to allow play, product or payment manipulation.	Probability	2
	Impact	3
	Total	6
Mitigation of risk (Controls)	**Control Score**	
Employee background checks Reference checks are undertaken for new employees. Police checks for Senior members of staff. Back-office systems access permissions Role based access permissions Test account policy BT has a policy of not allowing employees to create real personal accounts for the purpose of betting with any BT website. Should an employee require the creation of a test account required for testing purposes, then any request must be forwarded to Head of Testing for approval. All test accounts are subject to strict rules including ensuring that no payment method can be withdrawn to. Furthermore, accounts that are marked as test cannot be	Probability	2
	Impact	3

unmarked. There is no risk of test accounts being used on peer to peer so as poker as they are not provided	Total	6

Nature of risk	**Risk score**	
Employees may not be aware of how to escalate when they observe unusual activity that may constitute ML/TF activity.	Probability	3
	Impact	4
	Total	12
Mitigation of risk (Controls)	**Control Score**	
All employees receive annual ML/TF training. As part of this, the process for escalation is clearly described. Employees are informed of the Internal SAR reporting process including where to locate reporting forms. The MLRO will then assess whether the information provided constitutes a reportable event to the relevant authorities via the SAR reporting process.	Probability	2
	Impact	3
	Total	6

Nature of risk	**Risk score**	
Bingo is a new product being added to the BT product offering and could be launched without a Risk assessment	Probability	2
	Impact	4
	Total	8
Mitigation of risk (Controls)	**Control Score**	
	Probability	1

All new products are subject to a Risk Assessment prior to launch the new Bingo will be scrutinised by the Risk Assessment Committee in line with BT procedures with new product types. However, the bingo product does not allow customers to change the outcome of the result, meaning there is no possibility of hedging the bet placed; as such, the Bingo product falls into the Low-risk category as stipulated by the Implementing procedures Part 2.	Impact Total	2 2

Interface Risk

Customers who have deposited more than 2000 Eur (or currency equivalent) in rolling 180 day period and who are not 1+1 verified may be able to withdraw in breach of AML Regulations.	Probability	4
	Impact	4
	Total	16
Mitigation of risk (Controls)	**Control Score**	
The withdrawal block is applied automatically once the threshold is reached.	Probability	1
	Impact	3
	Total	3

Nature of risk	**Risk score**	
Customer not physically present for identification and physical ID documents not received.	Probability	4
	Impact	4
	Total	16
Mitigation of risk (Controls)	**Control Score**	
Account opening requires sufficient customer information (full name, date of birth, address) to seek verification from third party electronic screening once the 2k Eur threshold is reached, followed by manual review of documents where necessary. Deposit/withdrawal restrictions and, ultimately, account suspension is applied for those customers who cannot be fully verified.	Probability	2

Geographic Risk

Nature of risk	**Risk score**	
Mismatches between payment origins and declared residential address may indicate a customer is not who they claim to be.	Probability	3
	Impact	3
	Total	9
Mitigation of risk (Controls)	**Control Score**	
The Adyen product highlights mismatches between player location and card issuing country and currency so that appropriate action can be taken by the CF team.	Probability	2
	Impact	2
	Total	4

Nature of risk	**Risk score**	
Certain geographic locations have a higher ML/TF risk profile as identified by Transparency International and FATF reports.	Probability	4
	Impact	4
	Total	16
Mitigation of risk (Controls)	**Control Score**	
	Probability	3

Potential customers from high-risk jurisdictions are prevented from registering and certain payment methods may be blocked.	Impact	3
	Total	9

Nature of risk	**Risk score**	
Account activity from outside the registered jurisdiction (from IP address) may suggest the customer is not who they claim to be.	Probability	3
	Impact	3
	Total	9
Mitigation of risk (Controls)	**Control Score**	
Country mismatches are monitored by the CF team on a daily risk sensitive basis.	Probability	1
	Impact	2
	Total	2

Nature & Behaviour

Nature of risk	**Risk score**	
A customer who decides to change his personal details such as name or address may pose an increased ML/TF risk as the person may not be able to provide up to date information to BT. Outdated information increases the risk of not being able to perform accurate ongoing monitoring activities such as PEPs and Sanctions checks or enhanced customer due diligence checks.	Probability	2
	Impact	2
	Total	4
Mitigation of risk (Controls)	**Control Score**	
It is not possible for a customer to update account information without contacting BT. For any changes to their Name or Address, the customer must provide appropriate documentation for verification purposes. When a customer's documentation expire, updated documents are sought to ensure the customers information is updated regularly.	Probability	1
	Impact	2
	Total	2

Nature of risk	**Risk score**	
A customer may be reluctant to provide documentation or other information without a legitimate reason for doing so	Probability	4
	Impact	2
	Total	8
Mitigation of risk (Controls)	**Control Score**	
All customers are reminded that information provided it treated in the strictest confidential manner. Customers who do not provide requested documents will be suspended and not re-opened until such time documents are provided and verified.	Probability	2
	Impact	2
	Total	4

Nature of risk	**Risk score**	
An iSAR escalated to the MLRO may involve a family member or	Probability	3
	Impact	3

close associate causing a conflict of interest due to personal, professional or economic ties.	Total	9
Mitigation of risk (Controls)	**Control Score**	
Should the MLRO receive any reports on individual's or entities known to them, either in a personal or professional capacity; the MLRO will inform the CLCO, Director of Compliance and the DMLRO. In the same capacity, should the DMLRO in the absence of the MLRO receive any reports on individual's or entities known to them, either in a personal or professional capacity; the DMLRO will inform the CLCO, Director of Compliance and the MLRO. The investigation and any subsequent submission to the authorities will be carried out by the impartial party, the CLCO and Director of Compliance will be kept informed of the decision.	Probability Impact Total	3 2 6

Reputation Risk

Nature of risk	**Risk score**	
Customers appearing on Sanctions/PEPs lists using BT to clean criminally derived funds.	Probability	4
	Impact	5
	Total	20
Mitigation of risk (Controls)	**Control Score**	
	Probability	2
	Impact	3

Customers are checked against third party supplier sanctions

intervals (see PEPs/Sanctions policy document). Any account identified as being held by an individual on the sanctions list is suspended. PEPs matches are evaluated, and appropriate action taken as approved by senior management.	Total	6

Nature of risk	**Risk score**	
Customers who have been verified may nevertheless be linked to criminality and using the proceeds of crime to gamble.	Probability	3
	Impact	3
	Total	9
Mitigation of risk (Controls)	**Control Score**	
Adverse media reports and other open source information is used to provide additional background on customers who are judged to present increased risk.	Probability	2
	Impact	3
	Total	6

Nature of risk	**Risk score**	
The FIAU now stipulates that a subject person should consider the nature of the crime; an assault or a one-off shoplifting incident would not necessarily give cause for reporting, such as a fraud or theft from a company would. Time since the offence is also a factor we should consider.	Probability	3
	Impact	3
	Total	9
Mitigation of risk (Controls)	**Control Score**	
BT review all adverse media reports on a case-by-case basis. Consideration is given to the offence, time since the offence, and gravity of the offence.	Probability	2
	Impact	2
	Total	4

2 Regulatory Context

2.1 Money Laundering and Terrorist Financing

Money laundering is generally defined as engaging in acts designed to conceal or disguise the trueorigins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Money laundering often occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveller's cheques, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

One of the key differences between money laundering and terrorist financing is that terrorist financing does not necessarily involve the proceeds of crime but can come from legitimate sourcessuch as charitable donations or personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

3 Policy Statement

It is the policy of BT to actively prevent the services of the firm being used to facilitate financial crime, money laundering and terrorist financing.

Strict compliance with all applicable regulations will also protect the senior management and staff of the firm, as individuals, from the risks of breaches of the law, regulations, and supervisory requirements, and to preserve the reputation of the BT against the damage that could be caused by being implicated in money laundering and terrorist financing activities.

To achieve these objectives, it is the policy of this firm that:

- every staff member shall meet their personal obligations as appropriate to their role and responsibilities;
- commercial considerations cannot take precedence over BT's anti-money laundering commitment
- the company shall appoint a Money Laundering Reporting Officer/Nominated Officer/Compliance Officer ("MLRO"), and a deputy to cover in their absence, and they shall be afforded every assistance and cooperation by all members of staff in carrying out their duties and responsibilities. The deputy will be the Director Chief Executive Officer (CEO).

BT will strictly comply with all applicable AML/CFT rules and regulations with specific emphasis on:

- a culture of compliance to be adopted and promulgated throughout the firm towards the prevention of financial crime;

- a commitment to ensuring that customer's identities will be satisfactorily verified at required thresholds;
- a commitment to "knowing its customer" appropriately - both at acceptance and throughout the business relationship - through taking appropriate steps to verify the customer's identity and monitoring their use of BT services;
- a commitment to ensuring that staff are trained and made aware of the law and their obligations under it, and to establishing procedures to implement these requirements; and
- recognition of the importance of staff promptly reporting their suspicions internally:

At the heart of our policies, procedures and controls, and consistent with FATF Recommendation 1, is the risk-based approach. The risk-based approach means that we focus our resources on the areas of greatest risk.

Our policies, procedures and internal controls are designed to ensure compliance with all applicable anti-money laundering and anti-terrorist financing regulations and regulatory guidelines and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

4 Roles and Responsibilities

4.1 Senior Management

Senior Management are responsible for the overall compliance policy of BT and ensuring adequate resources are provided for the proper training of staff and the implementing of risk systems. This includes computer software to assist in oversight. Senior management will receive and consider the monthly compliance reports sent by the MLRO and authorise changes based on the recommendations if required. Assistance may be given to the MLRO in the preparation and/or updates of the AML manual.

Senior Management consists of the Board of Directors, the Executive Management Committee and the MLRO.

4.2 The Nominated Officer/Money Laundering Reporting Officer/ Compliance Officer

Responsible for receiving internal disclosures and making reports to the Curacao Gaming Commission. First point of contact for all compliance issues from staff. Prepares monthly report for consideration of senior management and conducts risk assessments of compliance systems. Undertakes regular random analysis of transactions including assessment of documentary evidence provided by customers. Assists in making any necessary amendments to AML manual in line with risk assessment. Ensures everyone is periodically informed of any changes in anti- money laundering or anti-terrorist financing legislation, policies and procedures, as well as current developments and changes in money laundering or terrorist activity financing schemes particular to their jobs. Reviews, customer identification information to ensure that all the necessary information has been obtained. Establishes and implement the risk scoring matrix following regulatory guidance and for review and approval by Senior Management.

4.3 Staff

Responsible for knowing the AML Compliance Manual and understanding responsibilities. Ensure company procedures are adhered to and obtaining all documentary evidence as outlined within the manual. Ensure that all suspicious and unusual activity is reported to the MLRO.

5 The Compliance Programme

5.1 The Money Laundering Reporting Officer/ Compliance Officer (MLRO)

BT has appointed a MLRO with full responsibility for BT's anti-money laundering compliance.

The MLRO:

- will monitor the day-to-day operation of BT's AML/CFT policies and respond to any reasonable request made by the NFIU, law enforcement and/or the Curacao Gaming Commission
- has the authority to act independently in carrying out their responsibilities, which any appropriate law enforcement agencies, in order that any suspicious activity may be reported to the right quarter as soon as is practicable.
- has the authority and the resources necessary to discharge their responsibilities effectively.
- is from a senior level and has direct access to senior management and the board of directors.
- may choose to delegate certain duties to other employees, but wherever such a delegation is made, the MLRO retains ultimate responsibility for the implementation of the compliance regime.
- at least annually, the MLRO will issue a report (the MLRO Report) to the senior management of BT on the operation and effectiveness of the money laundering controls. This report will cover improvements, remedial programmes, the outcome of any internal audit reviews of the AML/CFT processes, and other relevant items.

5.2 Compliance Policies and Procedures

BT has policies and procedures to assess the risks related to money laundering and terrorist financing. These policies and procedures are:

- written and maintained by the MLRO under the supervision of senior management
- approved by senior management
- communicated, understood and adhered to by everyone dealing with customers or their transactions, including those who work in the areas relating to customer identification, record keeping, and reportable transactions, who need enough information to process and complete a transaction properly as well as to ascertain the identity of customers and keep records as required.
- policies and procedures which incorporate the reporting, record keeping, customer identification, risk assessment and risk mitigation requirements applicable.

Although directors and senior officers may not be involved in day-to-day compliance, they

need to understand the statutory duties placed upon them, their staff and BT itself.

5.3 The Risk-Based Approach

In money laundering and terrorist financing, a risk-based approach covers the following:

- the risk assessment of customer relationships and business activities;
- the risk mitigation to implement controls to handle identified risks;
- keeping customer identification, beneficial ownership and business relationship information up to date; and
- the ongoing monitoring of business relationships and transactions.

Existing regulatory obligations, such as for customer identification, are a minimum baseline requirement. Where enhanced due diligence is appropriate, a principle of the risk-based approach is to focus resources where they are most needed to manage risks within our tolerance level.

5.4 Risk Mitigation

Risk mitigation is implementing controls to limit the potential money laundering and terrorist financing risks identified in the risk assessment so as to stay within the risk tolerance level. When the risk assessment determines that risk is high for money laundering or terrorist financing, then we will develop risk mitigation strategies and apply them.

5.5 In all situations, risk mitigation controls and measures include:

- focussing on operations (products and services, customers and business relationships, geographic locations, and any other relevant factors) that are more vulnerable to abuse by money launderers and criminals;
- informing senior management of compliance initiatives, identified compliance deficiencies, corrective action taken, and suspicious transaction reports filed;
- providing for program continuity despite changes in management, employees or structure;
- focussing on meeting all regulatory record keeping and reporting requirements, recommendations for anti-money laundering and anti-terrorist financing compliance and providing for timely updates in response to changes in requirements;
- enabling the timely identification of reportable transactions and ensure accurate filing of required reports;
- incorporating anti-money laundering and anti-terrorist financing compliance into job descriptions and performance evaluations of appropriate personnel; and
- providing for adequate supervision and training of employees that handle currency transactions, complete reports, monitor for suspicious transactions, or engage in any other activity that forms part of the anti-money laundering and anti-terrorist financing program.
- increasing awareness of high-risk situations within all business lines;
- increasing the frequency of ongoing monitoring of transactions or business relationships;
- escalating the approval of the establishment of an account or relationship even if not otherwise required to do so;
- increasing the levels of ongoing controls and reviews of relationships;
- requesting high-risk customers provide additional, documented information regarding

controls they have implemented to safeguard their operations from abuse by money launderers and terrorists;

- verifying the identity of customers by reference to reliable, independent source documents, data or information;
- preventing any transaction with a potential customer until identification and account opening information has been obtained;
- implementing an appropriate process to approve all relationships identified as high-risk as part of the customer acceptance process or declining to do business with potential customers because they exceed BT's risk tolerance level;
- implementing a process to exit from an existing high-risk relationship which management sees as exceeding BT's risk tolerance level.

5.6 Risk Assessment

BT is required to and will analyse potential threats and vulnerabilities to money laundering and terrorist financing to which the business may be exposed to in a risk assessment.

The risk assessment will document and consider the following:

- Products, services and delivery channels
- Geographic locations and areas of operation
- Customers

The risk assessment may identify high-risk situations for which risk mitigation controls and monitoring may be required. The risk assessment is not static and will change over time.

When a customer is identified as high-risk, they are subject to more frequent ongoing monitoring and updating of customer identification information, as well as any other appropriate enhanced measures.

BT shall perform an initial risk assessment at the beginning of a new customer relationship and for existing customers on an ongoing basis.

5.6.1 Client and Business Risk

5.6.2 Products, Services and Delivery Channels

BT will identify products and services or combinations of them that may pose an elevated risk of money laundering or terrorist financing. For example, products and services that support the movement and conversion of assets into, through and out of the financial system pose a high risk. Certain services have also been identified by financial regulators, governmental authorities or other credible sources as being potentially high-risk for money laundering or terrorist financing.

- wire transactions;
- transactions involving third parties;
- non-face-to-face business relationships.

5.6.2.1 Geographic Locations and Areas of Operation

Certain geographic locations potentially pose an elevated risk for money laundering and terrorist financing. These have been described by the FATF and by other resources such as Transparency International.

Clients from, or identified as linked to these countries will be regarded as high risk:

- any country subject to sanctions, embargoes, or similar measures;
- any country to have designated terrorist organisations operating within their country;
- any country known to be a tax haven, source of narcotics or other significant criminal activity;
- any country identified by the Financial Action Task Force (FATF) as non-cooperative in the fight against money laundering or terrorist financing or subject to a FATF statement;
- any country identified by credible sources as lacking appropriate money laundering or terrorist financing laws and regulations, or as having significant levels of corruption.

BT does not do business with or provide services to anyone in any country belonging to a list of select countries subject to comprehensive international sanctions (the “Sanctions List”).

5.6.2.2 Customer Relationships

The risk assessment requires to know your customers (“KYC”). This is not limited to identification or record keeping, but it is also about understanding the customers – including their activities, transaction patterns, and how they operate.

Examples of the factors that will be considered are:

- how long we have known the customer and had a business relationship;
- customers wanting to carry out large transactions;
- customers with regulatory or enforcement issues;
- customers with multiple online complaints;
- customers whose identification is difficult to verify;
- customers whose who are politically exposed.

A tiered approach is applied to identification and risk assessment of customers, both at the start ofthe relationship and on an on-going basis.

- If a player has not reached the monetary value threshold of deposits or withdrawals as provisioned under the relevant procedures of the Curacao Gaming Commission, the risk assessment to be carried out at this early stage will be based on the information obtained at registration such as the jurisdiction of residence of the player and on information obtained from searches and screening carried out on the player.
- Once the monetary value threshold is met, the player will be re-assessed. During this re-assessment BT obtains comprehensive information in relation to the purpose and intended nature of the business relationship for each player (this is further defined in the BT KYC Policy and Procedure). The collected information is factored into the customer risk assessment. Furthermore, the information obtained on the customer’s deposit method and game play between registration and the reaching of the threshold is also reflected in the re-assessment of the customer.

Each customer is risk-rated as either posing a low, medium or high risk of money laundering and/or terrorist financing. The rating given at the beginning of the business relationship may be adjusted after the re-assessment and may change over time. The level of customer due diligence will vary depending on the risk rating of the customer at the beginning of the relationship and as it changes. For all high-risk players, enhanced due diligence (“EDD”) is applied right away.

5.6.3 Regulatory risk

Regulatory risk means not meeting our obligations under applicable legislation. Examples of breaches of regulatory obligations include:

- customer identification not done properly;
- failure to train staff adequately;
- not having an anti-money laundering and anti-terrorist financing (AML/CFT) program;
- failure to report suspicious transactions;
- not having an MLRO;
- failing to keep complete customer records.

5.6.4 Risk Matrix

For ongoing monitoring, all customers are classified with a risk tier. The risk tier can be offset by alower risk factor in certain circumstances:

- Customers will initially be risk ranked according to the following:
    - Products and services they use
    - Their geographic location
    - The payment types they use
- The MLRO will define high risk customer types, geographic locations and payment types and risk thresholds following regulatory guidance and will report the risk rules to Senior Management for approval
- High risk status due to being a Politically Exposed Person (“PEP”) cannot be offset if the connected person is still a PEP
- Higher and moderate risk customers can be classified moderate or lower (one tier down) if the geographic location is LOW risk
- Higher and moderate risk merchants can be classified moderate or lower (one tier down) if they have been a customer for over five years and if no issues were identified during that time.
- The ongoing monitoring may give rise to factors which will allow an amendment of the risk tier of a customer
- Some customers may be prohibited from using BT products and services (for reasons that include but are not limited to age restrictions and self-exclusions). Restricted status cannot be offset, but for clarity, a “restricted” customer is not necessarily a high-risk customer.
- High risk status applies to PEPs, non-face-to-face relationships, certain geographic locations and certain types of payment
- Moderate risk status applies to certain geographic locations.
- Generally, countries which are EEA members and FATF members, will be classified as of low geographic risk, as will countries which are usually regarded as being “equivalent jurisdictions”
- The MLRO will include in their annual report to Senior Management the relative customers and volumes in each risk tier. There will be an annual review of the risk scoring by Senior Management and the MLRO to determine ongoing risk policy as part of the annual AML/CFT Risk Assessment

5.7 Compliance Training

BT has a training program for all relevant employees and other individuals who act on behalf of the Company. The goal of this training is to make sure that those who have contact with customers, who see customer transaction activity or who handle funds in any way understand the reporting, customer identification and record keeping requirements.

All new employees of BT are required to complete anti-money laundering and terrorist financing compliance training within their first three months of employment, and for customer-facing staff training is delivered prior to dealing with customers.

Training is currently conducted through a customised course. The training program is delivered electronically (via a learning management system). The training program is reviewed and updated by the MLRO to reflect requirements as they change. The compliance training includes a test which everyone must pass in order to consider their training complete.

To ensure employee training is kept up to date, all existing employees will receive follow up training on new and existing AML and regulatory requirements on a regular basis (at least within one year of their last training). If the online training test results show that a staff member does not understanding the training material, BT will ensure that the staff member receives specialised one-on-one training to understand the material.

An employee log of assigned and completed training materials is kept by the MLRO and the Human Resources department for administrative purposes. Retention of these records is for a period of five years.

Compliance training is adjusted in accordance to the employee's role within the company. The MLRO will review functions and arrange to provide suitable and customised training.

Our training will include at a minimum:

- an understanding of the reporting, customer identification and record keeping requirements as well as penalties for not meeting those requirements;
- making all employees aware of the internal policies and procedures for deterring and detecting money laundering and terrorist financing that are associated with their jobs;
- delivering to employees and suppliers a clear understanding of their responsibilities under these policies and procedures;
- all those who have contact with customers, who see customer transaction activity, who handle cash or funds in any way or who are responsible for implementing or overseeing the compliance regime must understand the reporting, customer identification and record keeping requirements.
- making all employees aware of how BT is vulnerable to abuse by criminals laundering the proceeds of crime or by terrorists financing their activities;
- making all employees and agents aware that they cannot disclose that they have made a suspicious transaction report, or disclose the contents of such a report, with the intent to prejudice a criminal investigation, whether it has started or not;
- that all employees and agents understanding that no criminal or civil proceedings may be brought against them for making a report in good faith;
- background information on money laundering so everyone who needs to can understand what money laundering is, why criminals choose to launder money and how the process usually works;
- details of what terrorist financing is and how that process usually works.

The MLRO is responsible for ensuring that everyone is informed of changes in anti-money laundering or anti-terrorist financing legislation, policies and procedures, and current developments in money laundering or terrorist activity financing schemes particularly relevant to their jobs.

Certain employees, such as those in compliance, customer services and operations, require types of specialised additional training which will be provided either through external services or internally. The training program is reviewed and updated to reflect changes in requirements.

6 Client Identification and Due Diligence

BT is required to obtain information to identify customers, to verify the customers' identity information, to obtain information on the purpose and intended nature of the business relationship and to monitor such business relationships on an ongoing basis. BT is also required:

- to be satisfied that the customers are who they say they are;
- to determine whether customers are acting on behalf of others; and
- to understand the circumstances of customers in order to protect BT from being used for fraud, money laundering or any other criminal activity

6.1 Customer Acceptance and Approval

BT enters into business relationships with private individuals. When accepting new customers, the company first ensures that:

- The customer is over 18 years of age and above the age at which gambling or gaming activities are legal in the jurisdiction that applies to customer; and
- Gambling is not illegal in the territory where the customer resides

Any duplicate accounts that may be opened by a customer are identified by the system using the customer identity details and those accounts are marked accordingly and linked together. Duplicate accounts may be closed by BT if problematic activity is identified.

6.2 Customer Identification

Client Identification is intended to confirm the existence and identify the individual with which BT has a business relationship and obtain supporting identity information. This includes measures to:

- Confirm the existence of the individual through identification documents;
- Conduct due diligence into the identity of the customer including:
    - cross-referencing customer names against government watch lists;
    - determining whether the customers are politically exposed persons;
    - determining whether any third parties are involved;
    - reviewing relevant publicly available information on the customer (e.g. adverse media, social media);
    - reviewing their background, reputation;
- Keep records of all information and documents obtained.

6.3 Identifying Information for Customers

This section sets out the standard identification requirements for individuals who have entered into a business relationship with BT. This outline is likely to be sufficient for most situations. If, however, the customer is assessed as presenting a higher money laundering or terrorist financing risk, in line with our identified risk matrix, then BT requires additional identity information to be provided and increase the level or verification accordingly.

Where the result of the standard verification check gives rise to concern or uncertainty over identity, the number of matches that will be required to be reasonably satisfied as to the individual's identity will increase. Any concerns must be reported to the MLRO.

If a customer is unable to produce a primary ID, the reasons for this should be noted and they may not be able to maintain an account.

All documentary evidence must be recent.

- Passports and drivers' licenses should be valid and not expired
- Utility bills should be dated within the last 3 months

In terms of beneficial ownership, we will ask every customer whether they are acting in their owncapacity or on behalf of another person. If they are acting for another person then we will requiredetails of such.

Sources of evidence

Proof of Identity - Acceptable photo identity:

- Valid passport; or
- Valid photo card driving licence (full or provisional); or
- National identity card.

Proof of Identity - Acceptable non-photo evidence of identity:

Documents issued by a government department, incorporating the person's name and residential address or their date of birth. e.g. (for proof of address or date of birth):

- Instrument of a court appointment (such as a grant of probate, bankruptcy); or
- Current tax identification number and/ or statement; or
- Current (within the last 3 months) bank statements, or credit/debit card statements issued by a regulated financial sector firm; or
- a recent (last available) utility bill (gas, water, electricity, telephone); it must be a bill or statement of account (not correspondence); statements printed off the internet are not acceptable on their own (a secondary check will be required such as a reference to a telephone directory including an online telephone directory); or
- Valid photo card driving licence (full or provisional); or
- A solicitor's letter confirming recent house purchase or land previous address.

When accepting evidence of identity from a customer, it is important that we make sufficient checks on the evidence provided to satisfy us of the customer's identity, and that we keep a record of the checks made. This will be done by the MLRO or under the supervision of the MLRO.

Usual checks on photo ID may include:

- Likeness against the customer
- Does the date of birth on the evidence match the apparent age of the customer?
- Is the ID valid?
- Is the spelling of names the same as other documents provided by the customer?

Checks on secondary evidence of ID may include:

- Do the addresses match the address given on the photo ID?
- Does the name of the customer match with the name on the photo ID?

Identity Verification Triggers

Verification of the identity of the customer occurs either when the customer has reached the monetary value threshold as provisioned under the relevant laws and regulations, or if the player is considered to be a high-risk player upon registration. The main trigger for Identity Verification is considered a single transaction (or smaller, linked transactions) that reach or exceed the monetary value threshold either at deposit or withdrawal stage. For example, transactions will be considered as linked when they are carried out by the same customer during a single period of being logged on to the BT's website or if they are carried out in 48 hours.

In all cases, the customer will receive a notification to upload identity verification documents listed above. Each document that is provided by customers to BT is checked manually by dedicated staff.

Further events that may trigger Identity Verification processes:

- When a customer requests a withdrawal to a different account than one that was used to make a deposit (e.g. due to the fact that certain payment service providers do not support incoming payments or other reasons). In these cases, the withdrawal requests will be immediately deducted from the customer's account, however, will not be processed until the customer's identity has been verified to ensure that the funds are going to the right person;
- When a customer makes multiple deposits within a short timeframe (five or more deposits in one hour);
- Staff identifies suspicious deposit patterns and or several payment cards are used (three or more different payment methods used within one week);
- Registration country and IP do not match – In such cases, the player account may not be blocked, and the player may still make deposits and play games, however, no withdrawal will be allowed until verification has been carried out;
- When a deposit exceeds 250EUR or currency equivalent.

Copies will be kept as evidence.

Additional Documents

Additional documents may be requested from customers to substantiate their activities or to betterunderstand their patters:

- Proof of Bank Account – This may be a screenshot or copy of the bank statement stating the customer's name and IBAN and the name of the bank (for instances when a customer requests a withdrawal to be deposited to a bank account);
- Proof of Payment Card – This may be a photo or copy of the front side of the card in

question or a bank statement that will include both the card details and the name of the customer (for instances when suspicious deposit patters are identified) –

    - To protect the customer's card data, BT informs them that they mayobfuscate some of the card details, however, the customer's name, as well as thefirst and last four digits of the card number must be visible.

- Bank Statements and Payslips – These may be requested from customers displaying potentially problematic gambling patterns and when external information available on the customer does not validate the amounts being gambled. In such cases BT would ask its higher volume customers for documents which would support the funds being spent on gambling.

Mitigation of Impersonation Risk

Various additional customer identity checks are permitted on a risk-based approach. These checks may include:

- Requiring the first payment to be carried out through an account in the customer's name with an EU/EEA regulated credit institution or one from an equivalent jurisdiction;
- Verifying additional aspects of the customer's identity, or of their electronic 'footprint';
- Telephone contact with the customer prior to opening the account on a home or business number which has been verified (electronically or otherwise) or a call to the customer before further transactions are permitted, using it to verify additional aspects of personal identity information that have been previously provided during the setting up of the account;

Keeping Information Up-to-Date

Once the identity of a customer has been confirmed, it does not have to be confirmed again. However, if there is any doubt about the information held, then that identification will be obtained again, including the identification of the customer.

BT may review the customer documentation and then update it as appropriate. Any changes to identification such as a change of name of the customer would require new documents to be obtained.

6.4 Politically Exposed Person Determination

At account opening BT will determine whether a customer relationship involves a Politically Exposed Person ("PEP").

If the customer is determined to be a, PEP the account will be referred to senior management prior to entering into an ongoing relationship with the account applicant.

A self-disclosure question about being a PEP is included during customer sign up, however, regardless of the selected answer, BT will screen all prospective customers (and existing customers) on an ongoing basis utilizing a third-party service provider which utilizes a credible source of commercially or publicly available information.

Confirmed PEPs will be ranked as high risk, subject to Enhanced Due Diligence ("EDD"), and no account will be opened or large transaction proceed without the express authority of the MLRO.

PEPs are defined as "an individual who is or has, at any time in the preceding year, been entrusted with prominent public functions and an immediate family member, or a known close associate, of such a person". This definition applies to those holding such a position within the EU or EEA. However, it is recognised that PEPs operating in certain countries (which are

associated with political stability, low levels of corruption, fair and free elections and other factors) pose a lower risk than other PEPs in which cases BT may take less intrusive steps to establish source of funds and can exercise oversight at a less senior level.

PEP status itself does not, incriminate individuals or entities. It does, however, put the customer, or the beneficial owner, into a higher risk category. PEPs do not automatically lose "high risk" status if they are no longer holding public office. BT will apply a risk-based approach to determine whether a former PEP should still be classified as high risk.

Regulatory guidance suggest that public functions exercised at levels lower than national should normally not be considered prominent. However, when their political exposure is comparable to that of similar positions at national level, for example, a senior official at state level in a federal system, firms should consider, on a risk-based approach, whether persons exercising those public functions should be considered as PEPs. Prominent public functions include:

- heads of state, heads of government, ministers and deputy or assistant ministers;
- members of parliaments;
- members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances;
- members of courts of auditors or of the boards of central banks;
- ambassadors, charges d'affaires and high-ranking officers in the armed forces; and (other than in respect of relevant positions at Community and international level)
- members of the administrative, management or supervisory boards of State-owned enterprises,
- members of the governing bodies of political parties; and
- directors, deputy directors and members of the board or equivalent function of an international organisation.

These categories do not include middle-ranking or more junior officials.

Immediate family members include:

- a spouse;
- a partner (including a person who is considered by his national law as equivalent to a spouse);
- children and their spouses or partners; and parents.
- Persons known to be close associates include:
- any individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a person who is a PEP; and
- any individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a person who is a PEP.

When deciding whether a person is a known close associate of a PEP, the firm will need only have regard to any information which is in their possession, or which is publicly known.

BT will have:

- appropriate risk-based procedures to determine whether a customer is a PEP;

- obtain appropriate senior management approval for establishing a business relationship with such a customer;
- take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship; and
- conduct enhanced ongoing monitoring of the business relationship.

7 Record Keeping

BT will keep records of customer due diligence and transactions.

7.1 The Client Account File

During business BT creates Client Account Files for all customers with whom it has an ongoing service agreement. The Client Account File consists of:

- the initial registration information, i.e. customer's name, address and other personal data;
- all documents used for identification of the customer including copies of individual identification documents;
- customer transaction data (including, but not limited to deposits, withdrawals, actions when gambling, etc.);
- internal memoranda and correspondence, which includes any memo, note, email, message or similar communication that is created or received, in the normal course of business, about the services provided to the customer;

7.2 Other Records to be Kept

7.2.1 Politically Exposed Person Records

Once a PEP transaction has been reviewed by senior management a record will be kept of:

- the office or position of the individual who is a PEP;
- the source of the funds (wealth and income), if known, that were used for the transaction;
- the date it was determined the individual to be a PEP;
- the name of the member of senior management who reviewed the transaction; and
- the date the transaction was reviewed.

BT will keep records of all customer business relationships for [5] years after the end of the relationship (the closing of the account).

This includes all customer identification information, documentary evidence of identity, risk-rating classifications and ongoing monitoring records.

7.2.2 Transaction Records

Records of transactions will be kept for ten years after the transaction.

7.2.3 MLRO Reports

All MLRO reports to senior management will be kept indefinitely.

7.2.4 Training Records

The company maintains records of all AML, Compliance and Responsible Gaming training undertaken by staff, the date it was provided and the results of any tests if applicable. These records will be kept for five years following the end of employment with the company.

7.2.5 Suspicious Activity Report Records

All SARs submitted including correspondence with NFIU (or any other government agency) will be kept for an unlimited period of time.

Internal reports of suspicions will be kept for five years.

7.3 How Should Records Be Kept?

They can be kept in electronic and paper format.

7.4 How Long Must Records Be Kept?

Unless otherwise specified all records will be kept for a minimum of fve years after the transaction or when they were created, or in the case of customer information records, until five years after the account has closed and the business relationship terminated.

These records include applications that were declined, and cancelled applications unless the application was cancelled before it was considered by the account approval process.

8 Ongoing Monitoring and Enhanced Due Diligence

BT will implement a risk-based approach to identify potential high risks of money laundering and terrorist financing and develop strategies to mitigate them.

8.1 Ongoing Monitoring Obligations:

Ongoing monitoring means monitoring customer relationships on a periodic basis, keeping a record of the measures taken to monitor the relationship and the information obtained, keeping a record of the purpose and intended nature of the business relationship and reviewing and updating this information periodically. The risk assessment of the customer determines how frequently we will monitor each business relationship and how frequently that business relationship information is to be kept up to date. All customer relationships need ongoing monitoring but high-risk customers will be monitored more frequently.

Ongoing monitoring of each business relationship is intended to:

- detect suspicious activity that must be reported;
- keep customer identification up to date;
- reassess the level of risk associated with the customer's transactions and activities;
- determine whether the transactions or activities are consistent with the information previously obtained about the customer, including the risk assessment;
- understand customer’s activities over time so that any changes can be measured to detect high risk

Monitoring high-risk situations may include measures such as:

- reviewing transactions based on an approved schedule that involves management sign- off;
- developing reports or performing more frequent review of reports that list high-risk

transactions, flagging activities or changes in activities from expectations and elevating concerns as necessary;

- setting business limits or parameters regarding accounts or transactions that would trigger early warning signals and require mandatory review;
- reviewing transactions more frequently against suspicious transaction indicators relevant to the relationship.

Where ongoing monitoring finds that a business relationship is high risk, then the risk assessment will treat that customer as high risk. This means more frequent monitoring of the business relationship with that customer, updating their customer identification information more frequently, and adopting any other appropriate enhanced monitoring measures (as listed below).

The frequency of monitoring will vary depending on the risk assessment of the customer but the ongoing monitoring obligation is to monitor all business relationships.

The current scheduled frequency of review (monitoring the business relationship and updating customer identification information) is that high-risk customers will be reviewed annually, moderate risk customers will be reviewed within two years and low-risk customers will be reviewed within three years.

8.2 Enhanced Due Diligence

Where the risks of money laundering or terrorist financing are higher, the customer will be classified as high risk and BT will conduct enhanced customer due diligence (“EDD”) measures, consistent with the risks identified. A non-exhaustive list of enhanced measures that will be taken to mitigate the risk in cases of high-risk business relationships is listed below:

- obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.);
- updating more frequently the identification documents of the customer;
- obtaining information on the source of funds or source of wealth of the customer;
- obtaining the approval of senior management to enter into or maintain the business relationship;
- identifying patterns of transactions that need further examination;
- requiring the first payment to be carried out through an account in the customer's name with EU regulated credit institution or one from an equivalent jurisdiction;
- increased and more frequent monitoring of transactions;
- establishing more stringent thresholds for ascertaining identification;
- gathering additional documents, data or information; or taking additional steps to verify the documents obtained;
- establishing transaction limits customised to the nature, scale and complexity of the customer;
- increasing internal controls of high-risk business relationships;
- obtaining the approval of senior management at the transaction level for products and services that are new for that customer;
- obtaining regular credit reports.

8.3 Transaction Monitoring

There are certain automated controls in place to monitor customer activities, for example:

- First time deposits;
- Cash-out alerts for cash-outs greater than EUR1,000 (or currency equivalent)
- Activity alerts when customer pays to, or stakes EUR1,000 during any period of 24 hours;
- Credit Card BIN alerts (when Credit Card country differs from player account country/IP);

In addition, all cash-out requests are processed manually by the Payments Team and are reviewed on a daily basis. Every request undergoes security checks before approval in order to determine that the origin of the funds/wins is compliant with the Curacao Gaming Commission's Policy and the terms and conditions of the Company.

9 Suspicious Activities

Any member of BT can report suspicious activities to the MLRO, as BT's Nominated Officer. A suspicious activity is one where it is known, or suspected, there are reasonably grounds to know or suspect that a person is engaged in, or attempting, money laundering or terrorist financing.

9.1 Grounds for Knowledge or Suspicion

Having knowledge means knowing something to be true. Knowledge can be inferred from the surrounding circumstances; so, for example, a failure to ask obvious questions may imply knowledge. The knowledge must, however, have come to BT during the course of business, or from a disclosure (to the MLRO).

Suspicion is more subjective and falls short of proof based on firm evidence. Suspicion is more than speculation and is based on some foundation.

An unusual transaction is not necessarily suspicious. Unusual patterns of gambling, including the spending of particularly large amounts of money in relation to the customer's profile, should receive attention, but unusual behaviour should not necessarily lead to grounds for knowledge or suspicion of money laundering, or the making of a report to the NFIU. The MLRO is required to assess all of the circumstances and, in some cases, it may be helpful to ask the customer or others more questions. The choice depends on what is already known about the customer and the transaction, and how easy it is to make enquiries.

Members of staff who consider a transaction or activity to be suspicious, would not necessarily be expected to know or to establish the exact nature of any underlying criminal offence, or that the particular funds or property were those arising from a crime, money laundering or terrorist financing. "Reasonable grounds to know or suspect" introduces an objective test of suspicion. The test is likely to be met when there are facts or circumstances, known to the member of staff, from which a reasonable person (in a payments firm) would have inferred knowledge, or formed the suspicion, that another person was engaged in money laundering or terrorist financing.

A defence of failing to meet the test of suspicion, would be for staff to demonstrate that they took reasonable steps to know the customer and the rationale for the transaction, activity or instruction.

9.2 How to Make a Suspicious Activity Report

Any member of staff, who is suspicious that a transaction may involve money laundering or who becomes aware during the course of their work that someone else is involved in money laundering, must make a disclosure to the MLRO using the BT Suspicious Transaction Report form.

Once completed, the form should be printed off. The member of staff making the report must sign and date the form before giving it to the MLRO. The MLRO will take note of the date and time of report receipt.

Upon receipt of the form by the MLRO, they will then decide what is to be done as a result of the report, e.g., whether the matter must be reported to the Curacao Gaming Commission or not, or further enquiries made and record its decision and the reason for it in the customer files. The member of staff concerned must be informed of the decision and the reasons for it.

If the matter is to be referred to the Curacao Gaming Commission, the MLRO or a subordinate will complete the Curacao Gaming Commission report form and discussing with the reporting member of staff how matters with the customer are to be conducted from that stage. The Curacao Gaming Commission STR report form must be signed off by the MLRO or the CEO. Same process holds for any reports made to the Curacao Gaming Commission.

BT must not proceed with a transaction whilst we await consent from Curacao Gaming Commission. Curacao Gaming Commission is given 7 working days (not including weekends or bank holidays) to consider the report.

If we hear nothing then we may continue with the transaction but not inform the customer about the report. Curacao Gaming Commission may give consent to proceed earlier than this time limit. They may also refuse consent in which case they have a further 31 calendar days (including weekends or bank holidays) to further consider the report. After this they must either begin proceedings or allow the transaction to continue.

The MLRO will submit a softcopy version of the report to the NFIU. Any paper file for each matter will be kept by the MLRO. The MLRO shall also file an incident report with the Curacao Gaming Commission.

There must be no record on the customer file or on the computer system which refers in any way to suspicious activity reporting, money laundering, etc., to avoid the risk of tipping off. It is a criminal offence to inform a customer that a SAR has been submitted, or to inform them of an investigation into their affairs.

All records of SARs will be kept in the central reporting file, which is kept by the MLRO.

9.3 How to Identify Suspicious Activity

Transactions may give reasonable grounds to suspect that they are related to money laundering or terrorist activity financing regardless of the sum of money involved. There is no monetary threshold for making a SAR. Suspicious transactions may involve several factors that on their own seem insignificant, but together raise suspicion that the transaction is related to the commission or attempted commission of a money laundering or terrorist activity financing offence, or both. As a general guide, a transaction may be connected to money laundering or terrorist activity financing when we think that it (or a group of transactions) raises questions or gives rise to discomfort, apprehension or mistrust.

BT will examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent

economic or lawful purpose.

The context in which the transaction occurs or is attempted is a significant factor in assessing suspicion and this will vary from one customer to another.

Transactions will be evaluated in terms of what seems appropriate and is within normal practices in business and based on our knowledge of the customer. The fact that transactions do not appear to be in keeping with normal industry practices may be a relevant factor.

Reasonable evaluation of relevant factors, including the knowledge of the customer's business, financial history, background and behaviour is the basis of assessing suspicion. Behaviour is suspicious, not people. We have listed below some indicators to help with this assessment.

9.4 Indicators of Suspicious Transactions

Certain products, services, activities or channels may pose a higher risk of misuse for money laundering. Listed below are several anti-money laundering risk indicators or “red flags” that might be grounds for suspicion. The list is not exhaustive and not conclusive but will be used as a guide for inquiry and follow-up, alongside other material.

A single indicator does not necessarily indicate reasonable grounds to suspect money laundering or terrorist financing activity. However, if several indicators are present during one or a series of transactions, then we will take a closer look at other factors before deciding whether the transaction must be reported.

In the case of a transaction aborted in the belief that the property is owned or controlled by or on behalf of a terrorist or a terrorist group, then there must be a terrorist property report. If there are reasonable grounds to suspect that the transaction is related to an attempted commission of a terrorist activity financing or money laundering offence, then a suspicious transaction report about the attempted transaction is also required.

Becoming aware of certain indicators could trigger reasonable grounds to suspect that one or more transactions from the past (that had not previously seemed suspicious) were related to money laundering or terrorist financing.

9.4.1 Application and Identification

- Information mismatch from application
- Application information/address/customer differs from initial registration
- Inability to provide government issued identification details
- Change of address to high-fraud area or to problematic jurisdiction, shortly after the application
- Lack of reliable third party and/or governmental verification of individual
- The address indicated (or corroborated) is identified as mail drop or other high-risk address, as opposed to a physical street address
- Transaction volume, deposits, and cash-outs are inconsistent

9.4.2 Account Settlement

- Large, cross-border wire transfer payments
- Settlements/partial settlements from unrelated third parties
- Excessive/ongoing large credit refunds

9.4.3 Transaction and Customer Monitoring

- Stakes wagered by a customer become unusually high or out of the ordinary and the customer is believed to be spending beyond his or her known means. This requires some knowledge of the customer but, nevertheless, there may be circumstances that appear unusual and raise the suspicion that he is using money obtained unlawfully.
    - It may be that the customer lives in low-cost accommodation with no known source of income but nonetheless is spending money well above his or her apparent means.
    - There is no set amount which dictates when a SAR should be made and much will depend on what is known, or suspected, about the customer.
- A customer exhibits unusual gambling patterns with an almost guaranteed return or very little financial risk.
    - It is accepted that some customers prefer to gamble in this way but, in some instances, the actions may raise suspicion because they are different from the customer's normal gambling practices.
- Money is deposited by a customer or held over a period and withdrawn by the customer without being used for gambling.
    - For instance, suspicions should be raised by any large amounts deposited in gaming machines or gambling accounts that are then cashed or withdrawn after very little game play or gambling.
- A customer regularly gambles large amounts of money and appears to find a level of losses acceptable.
    - In this instance, the customer may be spending the proceeds of crime and sees the losses as an acceptable consequence of the process of laundering those proceeds.
- A customers spend increases over a period of time, thereby masking high spend and potential money laundering.
- A customer spends little, but often, and his annual aggregate spend is high and out of kilter with his expected spend.
- A customer displays gambling patterns where spend is high but the risk is low, for example gambling on red and black in roulette. The customer could be laundering money in a way that guarantees minimal loss.
- Instances of high spend by customers that lead to significant commercial risk for the operator may also indicate suspicious activity.

Indicators to help establish suspicion that a transaction may be related to a terrorist activity financing offence mostly resemble those relating to money laundering, although there are some differences. For example, amounts relating to terrorist financing generally may be smaller.

9.5 Financial Sanctions

It is the policy of BT to verify the identity of all customers, and to check that they are not the subject of sanctions or other statutory measures prohibiting the Company from providing its services. The member of staff conducting verification of identity will complete the process by checking that the customer is not the subject of sanctions or other statutory measures, using

the screening methods set out by the MLRO. These include the direct questions to the prospective customer, screening of all new customers against sanctions and other databases (via direct reference to an official list or using a commercially available product), and ongoing screening of all customer names (via ongoing subscription to commercially available products and automatic uploads).

9.6 Adverse Media

Along with Sanctions and PEP databases, third-party providers offer a service that screens individuals for adverse media. BT uses such a service to identify if a customer has been identified by the media as having links to financial crime, terrorist financing and/or other criminal activity. These individuals, once confirmed to be one and the same in both media and among the BT customers, would only be allowed to continue using BT services after a close review by the MLRO and/or senior management.

10 Anti-Bribery and Whistleblowing

As an extension to the AML/CFT efforts, BT also employs Anti-Bribery and Whistleblowing Policies and Procedures. These are standalone documents that are available to all employees and are part of their onboarding package.

11 Employee Background Checks

BT is committed to establish and maintain procedures which enable it to be satisfied as to the integrity of all new staff members and by extension their likeliness to follow the BT policies and procedures. To meet this requirement, the Human Resource Department is responsible for undertaking all of the checks listed in relation to new members of staff and for retaining the appropriate records:

- Obtain and confirm references, if required;
- Confirm their employment history and the qualifications they have;
- Request a recent police conduct certificate; and
- Request details of any regulatory action taken against them.

Appendix 1 – Glossary of Abbreviations

Abbreviations used in this document:

AML Anti-money laundering

CFT Combating the financing of terrorism

FATF Financial Action Task Force, an intergovernmental body whose purpose is to develop and promote broad AML/CFT standards, both at national and international levels

MLR Money Laundering Regulations MLRO Money Laundering Reporting Officer PSD Payment Services Directive

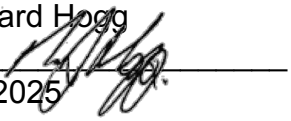
SAR Suspicious Activity Report

STR Suspicious Transaction Report

Version	Date	Author	Description
1.0	01/06/2025	Melissa Hardie	First Policy
1.1	01/06/2025	Richard Hogg	Reviewed, Policy No Change

Document Sign Off

Role	Name	Date	Note
Director	Richard Hogg	01/06/2025	

Bridge Technologies B.V
Title: Director
Name: Richard Hogg
Signature: 
Date 01/06/2025