FINANCREDITS BNK

PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

Glossary

- **AML:** 'Anti-Money Laundering', which generally refers to the policies, procedures and actions undertaken within a financial organisation to prevent it from being used (whether knowingly or unwittingly) as a vehicle for money laundering (a term which, in this document, also includes the financing of terrorism, bribery and corruption).
- **AMLCO:** an employee of FINANCREDITS BNK appointed by the Board of Directors of FINANCREDITS BNK, who assumes the role of compliance officer in the fight against money laundering. The AMLCO is independent and is responsible for the supervision and enforcement of anti-money laundering legislation, as well as FINANCREDITS BNK's procedures
- **Authorised Person:** a company ('Authorised Company') regulated in the conduct of its business by FINCEN or by equivalent regulators in a third country, or an authorised market institution.
- **Beneficial owner:** a natural person who:
    1. ultimately controls (either directly or indirectly) a customer;
    2. in relation to a customer that is a legal person or an arrangement, exercises (either directly or indirectly) ultimate effective control over the person or arrangement, or over the management of that person or arrangement;
    3. is the ultimate owner of the Customer or has an interest in the Customer, whether by legal title or as a beneficial owner (whether directly or indirectly);
    4. in whose name or for whose benefit a Transaction is being carried out;
    5. whose instructions the signatories to an account or any intermediary giving instructions to such signatories are, at that time, customarily acting upon.
    6. A person not covered by paragraphs (a) or (b) above is not a Beneficial Owner under paragraphs (c) or (d) if, taking into account a risk-based assessment of the Customer, the holding is small (less than 10% +1 of the voting rights and/or economic interests, as required in the specific case) and, given the circumstances, does not present any money laundering risk or such risk is negligible.
    7. In paragraphs (a) to (e), the reference to a 'Client' includes a client account, the client's assets and the legal person or underlying arrangements constituting or comprising the client, the client account or the client's assets.
- **Board of Directors:** the Board of Directors.
- **CDD**: Customer Due Diligence, i.e. the procedures carried out to verify the identity, source of wealth and financial profile of the customer in order to prevent the use of the financial institution for money laundering, terrorist financing, bribery or corruption.
- **Client:**
    1. a person in respect of whom, in relation to a business relationship between that person and the Company, there is a firm intention or commitment on the part of each party to establish a contractual relationship, or there is a firm commitment on the part of each party to carry out a Transaction, in relation to a product or service provided by the Company;
    2. a client of an Authorised Firm;
    3. in relation to a single-family office, a member of the single family;
    4. a person with whom the Company is establishing or has established a business relationship.

- **Employees**: the Board of Directors, all operational staff, any employee who has contact with clients, and any other employee who may encounter money laundering situations in the course of their duties. This also includes all persons providing services (from the front office to the back office) under agreements.
- **FATF**: the Financial Action Task Force, i.e. the intergovernmental body whose objective is the development and promotion of international standards to combat money laundering and terrorist financing.
- **FATF Recommendations**: the publication entitled 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation', as published and periodically amended by the FATF.
- **FINCEN:** an office of the US Department of the Treasury that protects the financial system against illicit activities. It combats money laundering and terrorist financing by analysing financial transactions. Its mandate is to facilitate the detection, prevention and deterrence of money laundering and the financing of terrorist activities, whilst ensuring the protection of personal information under its control.
- **IER**: Internal Evaluation Report.
- **ISR**: Internal Suspicion Report.
- **Act:** Means:
- Proceeds of Crime (Money Laundering) and Terrorist Financing Act (and its periodic amendments);
- the anti-money laundering rules and guidelines issued by FINCEN;
- ministerial directives and transaction restrictions.
- **Customer:** A customer of FINANCREDITS BNK who uses the Service that enables businesses to accept payments in multiple forms.
- **ML**: Money laundering.
- **Payment instrument**: any personalised device and/or set of procedures agreed between the payment service user and the payment service provider, and used by the payment service user to initiate a payment order.
- **Payment order**: Any instruction from a payer or payee to their payment service provider requesting the execution of a payment transaction.
- **Payment transaction**: An act initiated by the payer or the payee, consisting of depositing, transferring or withdrawing funds, irrespective of any underlying obligation between the payer and the payee.
- **PEP**: Politically exposed person; a natural person (and, where relevant, their family members or associates) who is resident in the United States or in other countries and who has been or is currently entrusted with a prominent public function, as well as their immediate family members or persons known to be associates of such persons. The term 'politically exposed persons' includes, amongst others, the following natural persons who have been entrusted, or were previously entrusted, with the performance of prominent public functions at home or abroad:
- Heads of State, Heads of Government, ministers and deputy ministers or secretaries of state;
- Members of parliament;
- Members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to appeal, except in exceptional circumstances;
- Members of courts of auditors or the governing councils of central banks;
- Ambassadors and high-ranking officers of the armed forces; and
- Members of the administrative, management or supervisory bodies of state-owned enterprises;

Notes/Additional information:

- It is at the discretion of the Anti-Money Laundering Committee (in consultation with the Board of Directors) to extend the list of positions that a politically exposed person may hold (for example, to include mayors)
- Where a person has ceased to hold a prominent public office for a period of at least one year, the Company shall not be obliged to regard them as politically exposed.
- None of the categories set out above for PEPs shall be interpreted as covering middle-ranking or junior officials.
- Immediate family members of PEPs include the following:
    1. The spouse or any partner considered by national law to be equivalent to a spouse;
    2. Children and their spouses or partners, or persons with whom they have been cohabiting for at least one year; and
    3. Parents.
- Persons known to be close associates include the following:
    1. Any natural person known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relationship with a PEP;
    2. Any natural person who is the sole beneficial owner of a legal entity or legal arrangement known to have been established for the de facto benefit of a PEP.
- **SAR:** Suspicious Activity Report; a report (including a suspicious transaction) filed with FINCEN.
- **Source of wealth**: refers to the means by which the Client's total assets or net worth are acquired, have been acquired or accumulated.
- **TF**: Terrorist financing.
- **Transaction**: a request made to FINANCREDITS BNK whereby a customer transfers money from a corresponding bank in an approved country and then requests a SEPA/SWIFT transfer to another designated account for the payment of services

1. INTRODUCTION

Money laundering ('ML') is the process by which criminals attempt to conceal or disguise the true origin and ownership of the proceeds of their criminal activities, thereby avoiding prosecution, conviction and the confiscation of criminal funds. If carried out successfully, money laundering enables criminals to evade prosecution, retain control over the proceeds of crime and continue their criminal activities. For the purposes of this Policy, money laundering also includes terrorist financing, bribery and corruption.

Regulations issued by each supervisory authority (for persons carrying out financial or other activities: 'regulated persons') with the aim of establishing the specific policy, procedures and internal controls that all regulated persons must implement for the effective prevention of money laundering and terrorist financing, in order to achieve full compliance with the requirements of the Act.

The company is obliged to comply with the provisions set out in the Act. Furthermore, the company has an ultimate obligation to cooperate and report suspicions and other matters relating to money laundering, terrorist financing, bribery and corruption to FINTRAC.

2. OBJECTIVE

In accordance with the legal framework established by FINCEN, money services businesses authorised and regulated by FINCEN are required to establish, implement and maintain anti-money laundering and 'Know Your Customer' ('KYC') policies and procedures. Therefore, the purpose of this Procedure is: (i) to set out the principles and details of the anti-money laundering ('AML') and customer due diligence ('CDD') approach in force at FINANCREDITS BNK; and (ii) to ensure that the Company complies with them and with all relevant legislative requirements.

In this regard, the company's anti-money laundering (AML) and 'Know Your Customer' (KYC) policies and procedures have been drawn up in accordance with these legal requirements. This procedure has been drawn up to guide all company employees, as well as any service providers with whom the company collaborates, on all the policies, procedures, systems and mechanisms that the company must implement to achieve its regulatory compliance objectives. It also provides a clear understanding of what they and the Company must and must not do to comply with the law, and how to recognise and report any suspicious activity that may be taking place. This Procedure applies to all FINANCREDITS BNK Employees (whether permanent or temporary).

The Compliance Department, in particular the AMLCO, is responsible for maintaining this procedure. It will be reviewed at least every 12 months, or whenever necessary to adapt to any changes in legislation. When it is republished, changes will be highlighted so that staff are aware of the amendments.

3. LEGAL FRAMEWORK

Under the terms of its operating licence, FINANCREDITS BNK must have adequate organisational mechanisms in place to prevent its misuse for the purposes of money laundering, terrorist financing, bribery and corruption. The legal requirements for payment institutions (PIs) have been established by FINCEN and are determined by the following laws and regulations:

1) Law on the Proceeds of Crime (Money Laundering) and the Financing of Terrorism
1) Regulations on the Reporting of Suspicious Transactions Related to Proceeds of Crime (Money Laundering) and Terrorist Financing;
2) The Regulations on Proceeds of Crime (Money Laundering) and Terrorist Financing;
3) Regulations on the Reporting of Cross-Border Movements of Cash and Monetary Instruments;
4) Regulations on the Registration of Proceeds of Crime (Money Laundering) and Terrorist Financing;
5) The Regulations on Administrative Monetary Penalties relating to Proceeds of Crime (Money Laundering) and Terrorist Financing;

6) The FINCEN Interpretation Policy. FINCEN engages with stakeholders in various ways to raise awareness and ensure consistent internal and external communication regarding regulatory compliance requirements. These measures include:

a. The publication of various guidance documents on the FINCEN website, including:
b. FINCEN Interpretation Notes
c. FINCEN Policy Interpretations
d. FINCEN guidelines; and
e. FINCEN guidance on the risk-based approach

4. Offences relating to money laundering and terrorist financing

4.1. Definition of money laundering

Money laundering is understood to mean any act intended to conceal the nature, source and location of proceeds derived from criminal activities through a series of transactions. The offender has the following three (3) objectives:

i. concealing the true ownership and origin of the proceeds of crime;
ii. to retain control over such proceeds; and
iii. to alter the form of such proceeds

Money laundering can take many forms, ranging from highly complex processes to the simplest of mechanisms. It can be carried out using an almost infinite number of methods spanning a wide range of financial services and products. Historically, money launderers have preferred to misuse the financial system—as one of many channels employed—to carry out their money laundering activities. Traditionally, a successful money laundering operation typically consists of three stages in the order of placement, layering and integration. However, it is important to understand that not all money laundering activities involve such a sophisticated process.

Placement: this is the actual disposal of the proceeds of crime so that their link to criminal activity is not discovered. When the proceeds are in cash, the first step is to introduce the funds into the financial system. Some examples of this include:

- Smurfing: cash from illegal sources is divided amongst 'deposit specialists' or 'smurfs', who make multiple deposits into multiple accounts (often using various aliases) at any number of financial institutions;
- Structuring: transactions are split into separate amounts below USD 10,000/ EUR 10,000 to circumvent the transaction reporting requirements established by law;
- Physically transporting cash between jurisdictions;
- Depositing cash into the account of a professional intermediary;
- Various ways of disposing of the cash, for example, by purchasing expensive items, contracting costly services, or acquiring tradable assets in one-off transactions;
- The use of the financial system, as it allows large sums of money to be transferred instantly, both locally and to offshore jurisdictions. This rapid transfer of funds to and between foreign jurisdictions makes it difficult to investigate transactions and trace their origin. In the context of money laundering, this technique involves transferring money through payment systems that do not require funds to be sent via formal bank accounts;
- Gambling is a common placement technique used to launder money, which involves feeding illeg s into slot machines or online casinos and withdrawing it as gambling winnings. Funds that appear to be winnings can easily be used to justify unusual spikes in income.

Layering: this is how the criminal separates themselves and the money from the original source. Layers of transactions are created with the intention of obscuring the audit trail. It is hoped that, having remained in the financial system for a period of time, the money will eventually acquire an appearance of legitimacy. Examples include:

- Rapid movement of funds between depositary institutions and jurisdictions;
- Cash withdrawals to third parties without any rational or justifiable commercial reason;
- Movement of cash through a network of legitimate businesses and shell companies across various jurisdictions;
- Resale of goods and assets;
- Lawyers, accountants and other professionals may be used as intermediaries between the illegal funds and the offender; such transactions may involve the use of shell companies, false records and complex documentary trails;
- Transfers of funds to and from domestic and offshore bank accounts held by fictitious individuals and companies.

Integration: this involves putting the money to actual use. If the layering has been successful, the criminal can deploy the proceeds within the economy as apparently legitimate funds. At this stage, of course, a transaction is unlikely to appear necessarily suspicious. Some examples include:

- Credit and debit cards are efficient ways for money launderers to integrate illegal money into the financial system. By maintaining an account in an offshore jurisdiction through which payments are made, criminals limit the financial trail leading back to their country of residence;
- Fictitious transactions;
- 'Business recycling' is a common integration technique in which illegal funds are mixed with the cash flow of an apparently legitimate business.

Certain factors will indicate that a transaction may form part of a money laundering scheme. In general, it is to be expected that most potentially suspicious transactions will come to our attention as part of the triage or stratification process. It is essential that all employees remain particularly alert to circumstances that may appear suspicious. It is therefore crucial to have a clear understanding of the principles governing what constitutes a suspicious transaction. Examples of certain behaviours and transactions that will be considered suspicious include:

- An unusual transaction in the course of normal financial activity;
- Any unusually linked transaction;
- Any unusual method of settlement;
- A customer who refuses to provide the required KYC documents.

Whilst the money remains in the system, it is relatively safe. It is only when it is moved that the money launderer becomes vulnerable. The money will be moved to a large extent.

4.2. Scheduled offences

The Act applies to specified offences, which include money laundering offences and predicate offences.

4.3. Money laundering offences

Any person who knows, or at the relevant time ought to have known, that any property constitutes the proceeds of an underlying offence is guilty of an offence if they carry out any of the following acts:

i. Converts, transfers or withdraws such property with the intention of concealing or disguising its illicit origin, or of assisting in any way a person involved in the commission of the predicate offence to carry out any of the above actions, or acts in any other way to evade the legal consequences of their actions;

ii. Conceals or disguises the true nature, origin, location, disposition, movement or rights relating to the property or ownership of such property;
iii. Acquiring, possessing or using such property;
iv. Participating in, associating with, cooperating in, conspiring to commit, or attempting to commit, and aiding, abetting or providing guidance or advice for the commission of any of the offences mentioned above;
v. Providing information in connection with investigations into money laundering offences with the aim of enabling the person who derived a benefit from the commission of an underlying offence to retain the proceeds or control of the proceeds derived from the commission of the offence.

4.4. Underlying offences

Underlying offences are described as:

1. All criminal offences punishable by a term of imprisonment exceeding one year, as a result of which proceeds have been obtained that may constitute the subject matter of a money laundering offence as defined in the relevant section of the Act;
2. Terrorist financing offences, as specified in the relevant Terrorist Financing (Ratification and Other Provisions) Acts, as well as the raising of funds for the financing of persons or organisations associated with terrorism;
3. Drug trafficking offences, as specified in the relevant section of the Act; and
4. Tax evasion.

Note:
- It shall not matter whether the offence in question falls within the jurisdiction of the courts of the United States

or not.
- The perpetrators of an underlying offence may also commit a money laundering offence.
- The knowledge, intent or purpose required as elements of the offences may be inferred from objective and factual circumstances.

4.5. Other offences: failure to report

It is an offence for any person, including employees of the Company, who, in the course of their commercial, professional, business or employment activities, has knowledge or reasonable suspicion that another person is involved in money laundering (ML) or terrorist financing (TF) activities, to fail to report such knowledge or suspicion to FINCEN as soon as reasonably possible after becoming aware of the information. Failure to comply with the reporting obligation in these circumstances may result in the penalty described in section 4.5 below.

4.6. Offences relating to the disclosure of information

Any person who: (i) discloses information or other relevant material concerning knowledge or suspicions of money laundering or terrorist financing that has been submitted to FINCEN; or (ii) discloses information that may hinder or prejudice the questioning and investigation being conducted in respect of the prescribed offences or the identification of proceeds, knowing or suspecting that such questioning and investigation are taking place, is guilty of an offence. The penalty for 'whistleblowing' is explained in section 4.5 below.

4.7. Penalties for non-compliance

The objective of FINCEN's Administrative Monetary Sanctions (AMS) programme is to encourage future compliance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the Act) and its regulations, as well as to promote a change in behaviour. The AMS programme supports FINCEN's mandate by providing a measured and proportionate response to specific instances of non-compliance. FINCEN is committed to working with Reporting Entities (REs) to help them comply with the regulations. AMPs are not automatically imposed in response to non-compliance, as other compliance measures are typically taken to change behaviour before a penalty is considered. The purpose of this policy is to provide a framework for determining an AMP and to summarise the principles and guidelines FINCEN uses when imposing an AMP.

5. Key elements of the anti-money laundering programme

The key elements of the firm's anti-money laundering policy, systems and controls include the following:

5.1. Risk-based approach

- Identify the ML/TF risks faced by the Company, as well as those presented by each customer, and then adopt the necessary, risk-based approach to eliminate or manage them.
- Carry out the appropriate level of CDD (Customer Due Diligence) with regard to its customers, taking into account the risks arising in each case, rather than following a 'rules-based' approach. An essential part of this is documenting knowledge of the customer, their sources of wealth and funds, by completing the onboarding process in accordance with the limit established in the regulations that each customer will maintain with FINANCREDITS BNK.
- Ensure that higher-risk business relationships, including those involving a politically exposed person ('PEP'), are only accepted with the explicit approval of the Board of Directors and an understanding of the potentially higher risks they entail.

5.2. Staff awareness and training

- To ensure that staff are aware of the money laundering and terrorist financing risks faced by the company, their obligations and responsibilities under applicable laws and regulations, the company's procedures for carrying out customer due diligence, and how to recognise and report suspicious activities.

5.3. Customer due diligence

- Not only verifying the identity of FINANCREDITS BNK's customers (and their beneficial owners, where relevant), but also understanding the source of their funds and their flow.
- Take into account international sanctions regimes, as well as governmental, regulatory and international determinations regarding blacklisted countries and individuals, to check and verify that FINANCREDITS BNK's customers are not subject to them.

5.4. Prohibited business

- FINANCREDITS BNK will not maintain business relationships with persons whose beneficial owners cannot be identified, nor with representatives (or holders of bearer shares) acting on behalf of persons whose identity has not been disclosed to the company.
- FINANCREDITS BNK will not establish a business relationship unless customer due diligence has been completed.

- FINANCREDITS BNK will not establish a business relationship with any Customer operating or domiciled/residing in a prohibited country (Appendix 7).
- FINANCREDITS BNK will not establish a business relationship with any Client operating in prohibited sectors (e.g. adult content, unregulated binary options trading, etc.) (Appendix 8).

5.5. Reliance on third parties

FINANCREDITS BNK may engage third parties to collect and provide the documentation or information necessary for due diligence purposes. In such cases, the company shall require such third parties to:

- make available to FINANCREDITS BNK any evidence, information and identification documents that said third party has received when applying due diligence controls in accordance with its legal obligations;
- provide copies of such evidence, information and identification documents obtained by the third party for the purpose of establishing the identity of the customer and the beneficial owner (who is a natural person), within 24 hours in the event that:
- the Company is required to respond to any regulatory enquiry; or
- in compliance with a court order, without FINANCREDITS BNK being obliged to disclose to the third party the reason for the enquiry or the details thereof;
- notify FINANCREDITS BNK in the event that the Customer modifies any details of the initial information provided;
- notify FINANCREDITS BNK should the Customer cease to use its services.

5.6. Ongoing due diligence and monitoring of customer activity

- Maintain up-to-date information on the Company's Clients and verify any significant changes.
- Monitor the customer's activities and transactions throughout the entire relationship to detect any signs of suspicious behaviour that may require further investigation.

5.7. Customer Deposits

- The company will receive funds via any of the following methods:
- Bank transfer from credit institutions within the United States (or an equivalent third country)
- Bank transfer from Alternative Payment Methods ('APMs') with which the Company has already established a business relationship (i.e. which have undergone the CDD process)
- Bank transfer from other PIs or EMIs within the United States (or an equivalent third country) with which the Company has already established a business relationship (i.e. which have undergone the CDD process)
- The Company will not accept funds from any institution located in a country classified by the AMLCO as 'high risk'. In its assessment, the AMLCO will consult reports issued by the CA, the EU, the UN, the US, the FATF or any other relevant and reliable source.

5.8. Payments from clients

Company clients:

- The client's bank account must be in the name of the person (natural or legal) who holds the contract with the Company. The following exception is permitted: where the account is held in the name of a company that is related to the Client under company law and in relation to the Client's ownership; proof of the relationship must be provided via extracts from the commercial register and/or other certified official documents.
- The Company refuses to establish a correspondent banking relationship with shell banks. Furthermore, it refrains from establishing relationships with foreign correspondent financial institutions that allow their accounts to be used by shell banks.

5.9. Reliance on third parties

FINANCREDITS BNK may engage third parties to collect and provide the documentation or information necessary for due diligence purposes. In such cases, the company shall require such third parties to:

- make available to FINANCREDITS BNK any evidence, information and identification documents that said third party has received when applying due diligence controls in accordance with its legal obligations;
- provide copies of such evidence, information and identification documents obtained by the third party for the purpose of establishing the identity of the customer and the beneficial owner (who is a natural person), within 24 hours in the event that:
- the Company is required to respond to any regulatory enquiry; or
- in compliance with a court order, without FINANCREDITS BNK being obliged to disclose to the third party the reason for the enquiry or the details thereof;
- notify FINANCREDITS BNK in the event that the Customer modifies any details of the initial information provided;
- notify FINANCREDITS BNK should the Customer cease to use its services.

5.10. Ongoing due diligence and monitoring of customer activity

- Maintain up-to-date information on the Company's Customers and verify any significant changes.
- Monitor the client's activities and transactions throughout the entire relationship to detect signs of suspicious behaviour that may require further analysis.

5.11. Customer deposits

- The company will receive funds via any of the following methods:
- Bank transfer from credit institutions within the United States (or an equivalent third country)
- Bank transfer from Alternative Payment Methods ('APMs') with which the Company has already established a business relationship (i.e. which have undergone the CDD process)
- Bank transfer from other PIs or EMIs within the United States (or an equivalent third country) with which the Company has already established a business relationship (i.e. which have undergone the CDD process)
- The Company will not accept funds from any institution located in a country classified by the AMLCO as 'high risk'. In its assessment, the AMLCO will consult reports issued by the CA, the EU, the UN, the US, the FATF or any other relevant and reliable source.

5.12. Payments from clients

Company clients:

- The client's bank account must be in the name of the person (natural or legal) who holds the contract with the Company. The following exception is permitted: where the account is held in the name of a company that is related to the Client under company law and in relation to the Client's ownership; proof of the relationship must be provided via extracts from the commercial register and/or other certified official documents.
- The Company refuses to establish a correspondent banking relationship with shell banks. Furthermore, it refrains from establishing relationships with foreign correspondent financial institutions that allow their accounts to be used by shell banks.

The Client is required to provide the following:

- Bank details form signed by the company's authorised representative.
- Certified copy of the authorised signatory's passport or identity document.
- A voided cheque or bank statement showing the bank details, or a lawyer's approval on the bank details form (one of the three options).

Verified by the Compliance Department:

- The bank details provided correspond to the person (natural or legal) contracted with the company and the acquiring bank.
- The bank details must be signed by the company's authorised representative (signatures will be compared with those on contracts or the passport).
- The voided cheque or bank statement matches the signed bank details forms.
- The account reconciliation procedures mentioned above apply to the following:
- new customers
- existing customers adding additional currencies; and
- existing customers who change their bank details; customers must also explain the reason for changing their bank account

5.13.Ongoing due diligence and monitoring of client activity

- Maintain up-to-date information on the Company's clients and verify any significant changes.
- Monitor customer activities and transactions throughout the relationship to detect signs of suspicious behaviour that may require further analysis.

5.14.Customer deposits

- The company will receive funds via any of the following methods:
- Bank transfer from credit institutions within the United States (or an equivalent third country)
- Bank transfer via Alternative Payment Methods ('APMs') with which the Company has already established a business relationship (i.e. which have undergone the KYC process)
- Bank transfer from other PIs or EMIs within the United States (or an equivalent third country) with which the Company has already established a business relationship (i.e. which have undergone the CDD process)
- The Company will not accept funds from any institution located in a country classified by the AMLCO as 'high risk'. In its assessment, the AMLCO will consult reports issued by the CA, the EU, the UN, the US, the FATF or any other relevant and reliable source.

5.15.Payments from clients

Company clients:

- The client's bank account must be in the name of the person (natural or legal) who holds the contract with the Company. The following exception is permitted: where the account is held in the name of a company that is related to the Client under company law and in relation to the Client's ownership; proof of the relationship must be provided via extracts from the commercial register and/or other certified official documents.
- The Company refuses to establish a correspondent banking relationship with shell banks. Furthermore, it refrains from establishing relationships with foreign correspondent financial institutions that allow their accounts to be used by shell banks.

The Client is required to provide the following:

- Bank details form signed by the company's authorised representative
- Certified copy of the authorised signatory's passport or identity document
- A voided cheque or bank statement showing the bank details, or a lawyer's approval on the bank details form (one of the three options).
- Verified by the Compliance Department:

1. The bank details provided correspond to the person (natural or legal) contracted with the company and the acquiring bank.
2. The bank details must be signed by the company's authorised representative (signatures will be compared with those on contracts or the passport).
3. The voided cheque or bank statement matches the signed bank details forms.

- The account reconciliation procedures mentioned above apply to the following:
- new customers
- existing customers adding additional currencies; and
- existing customers who change their bank details; customers must also explain the reason for changing their bank account.

Customers with closed accounts: FINANCREDITS BNK will release the balances six months after the closure of the processed account to the same bank account that was used prior to the closure of the processed account.

Minimum payment limits: The company applies a minimum payment limit with regard to the payment procedure. The minimum varies from client to client and as agreed with the client.

Payment frequency: Payments are made daily. Reserve payments are made monthly.

Suspension of payments/reserves: The company reserves the right to suspend payments in accordance with its internal policies and in accordance with the client's contract.

Reasons for suspension of payments:

- Bank details have been changed and the company has not been informed of this.
- Drastic changes in processing volume or any abnormal processing compared to the client's processing history.
- The client has ceased processing.
- Any other relevant issue raised by the Customer Service, Risk Management, Compliance and Finance departments
- The Company refuses to establish a correspondent banking relationship with fictitious banks. Furthermore, it refrains from establishing relationships with foreign correspondent financial institutions that allow their accounts to be used by fictitious banks.
- The Customer is required to provide the following:
- Bank details form signed by the company's authorised representative
- Certified copy of the authorised signatory's passport or identity document
- A voided cheque or bank statement showing the bank details, or a solicitor's approval on the bank details form (one of the three options).
- Verified by the Compliance Department:
- The bank details provided correspond to the person (natural or legal) contracted with the company and the acquiring bank.
- The bank details must be signed by the company's authorised representative (signatures will be compared with those on contracts or the passport).
- The voided cheque or bank statement matches the signed bank details forms.
- The account reconciliation procedures mentioned above apply to the following:
- new customers
- existing customers adding additional currencies; and
- existing customers who change their bank details; customers must also explain the reason for changing their bank account
- **Customers with closed accounts**: FINANCREDITS BNK will release the balances six months after the closure of the processed account to the same bank account that was used prior to the closure of the processed account.

- **Minimum payment limits**: The company applies a minimum payment limit with regard to the payment procedure. The minimum varies from customer to customer and as agreed with the customer.
- **Payment frequency**: Payments are made daily. Reserve payments are made monthly.
- **Suspension of payments/reserves**: The company reserves the right to suspend payments in accordance with its internal policies and in accordance with the client's contract.
- **Reasons for suspension of payments**:
- Bank details have been changed and the company has not been informed of this.
- Drastic changes in processing volume or any abnormal processing compared to the client's processing history.
- The client has ceased processing.
- Any other relevant issue raised by the Customer Service, Risk Management, Compliance and Finance departments.

5.16. Bribery and corruption

Corruption is the abuse of a public or private position for personal gain. The person benefiting may be a public official, but could also be a relative, friend or business associate of that person.
Bribery is the offering or acceptance of a gift, loan, payment or other reward to or from a person (in government or business) as an incentive to do something that is illegal, improper or a breach of trust.
Some examples of improper payments include:

- Payment to a government official to win a public tender;
- Excessive hospitality towards a potential client with the specific aim of winning a contract;
- Gifts directly related to the award of a banking mandate. Fundamental principles:
- FINANCREDITS BNK does not tolerate bribery or corruption by its staff or agents under any circumstances;
- Any suspicion of corrupt conduct must be reported to the Compliance Department, which will refer the matter to senior management;
- Senior management will treat any indication of corruption or bribery as a serious disciplinary matter, which will be thoroughly investigated and may result in disciplinary action, up to and including dismissal. The company will report relevant information to the regulatory authorities or law enforcement agencies. All departments undertake to identify the specific risks of bribery and corruption in our business and to report them to the Compliance Department accordingly.
- Employees must comply with the company's Code of Conduct at all times. Third parties acting on behalf of the company must be encouraged to follow the same standards. Contracts entered into with such third parties must include clauses reflecting a commitment not to engage in corrupt practices.
- Employees are required to report any indication of suspected bribery and/or corruption to the AMLCO. This applies to suspicions of bribery/corruption by company employees, our agents and suppliers, or our customers.
- The Compliance Department is responsible for:
    i. periodically assessing the risks of bribery and corruption across the company;
    ii. confirming that appropriate systems and controls are in place to mitigate this risk and demonstrating that these controls operate effectively; and
    iii. ensuring that employees are properly trained and informed about the risks of corruption and bribery, as well as any effective means of addressing such risks.

6. Powers of the Regulatory Authority (FINCEN) and sanctions

6.1. Powers of the regulator

The Act requires all persons carrying out financial or other activities to establish and maintain specific policies and procedures to protect their business and the financial system, in general, against its use for the purposes of money laundering or terrorist financing. Essentially, these procedures are designed to achieve two objectives. Firstly, to facilitate the recognition and detection of suspicious transactions. Secondly, to ensure, through the strict application of the 'know your customer' principle and the maintenance of adequate record-keeping procedures, that, should a customer become the subject of an investigation, the business can provide its part of the audit trail.

Any person carrying out financial or other activities is required to implement adequate and appropriate systems and procedures in relation to the following:

i. Customer identification and customer due diligence;
ii. Record-keeping;
iii. Internal reporting and reporting to FINCEN;
iv. Internal control, risk assessment and risk management to prevent money laundering and terrorist financing;
v. Detailed examination of each transaction which, by its nature, may be considered likely to be related to money laundering or terrorist financing offences and, in particular, of complex transactions or those of an unusually high value, as well as any other unusual pattern of transactions lacking an apparent economic purpose or a visible lawful purpose;
vi. Informing its employees regarding:
    a. the systems and procedures;
    b. obligations under anti-money laundering legislation;
vii. Ongoing training of its employees in the recognition and handling of transactions and activities that may be related to money laundering or terrorist financing.

6.2. Sanctions

The regulatory authority may impose any or all of the following measures in the event that a regulated firm fails to comply with the provisions of the Act:

- Require the regulated firm to take measures within a specified timeframe to rectify the situation and comply with the regulations.
- Amend, suspend or revoke the operating licence; require the dismissal or removal of any consultant, director or officer, including the compliance officer (CO), the internal auditor or the anti-money laundering officer (AMLCO), should the breach be due to their negligence, fault or deliberate omission. Furthermore, impose the regulatory fines protocol for the prevention of money laundering and terrorist financing.

7. Provisions and responsibilities of senior management

7.1. Responsibilities of the Board of Directors

The law requires the Board of Directors of FINANCREDITS BNK to:

- Determine, record and approve the general principles of the company's policy regarding the prevention of money laundering and terrorist financing, and communicate these to senior management and the CO.
- Appoint a Compliance Officer (CO) and an Anti-Money Laundering Compliance Officer (AMLCO) (and a deputy AMLCO) and, where necessary, one or mor y deputy AMLCOs.
- Define the roles and responsibilities of the Anti-Money Laundering Officer (AMLCO) and the deputy officers.
- Approve the AML Policy and the risk management framework.

- Ensure that all requirements of the Act are met.
- Ensure that adequate, effective and sufficient systems and controls are in place.
- Ensure that the AMLCO is notified immediately of unusual or suspicious transactions and other matters of significance.
- Provide the AMLCO with full and timely access to all data and information relating to customer identity, transaction documents and other relevant records and information held by the company so that they can perform their role effectively.
- Provide the AMLCO with adequate resources to enable them to perform their role effectively.
- Ensure that the Anti-Money Laundering Officer (AMLCO) has full autonomy in the process of assessing Suspicious Transaction Reports (STRs) and unrestricted access to the information necessary to carry out this process.
- Ensure that all employees are aware of the person assigned the role of AMLCO, as well as any other person to whom they must report any transaction or activity of which they are aware or suspect may be related to money laundering and terrorist financing.
- Establish a clear and rapid chain of communication for reporting suspicious transactions to the AMLCO.
- Review and approve the AMLCO's Annual Report.

The Board's responsibilities are set out as follows:

i. Periodically review the company's policies and ensure that they comply with applicable legislation in force;
ii. To establish the company's strategy, based on the annual budgets, plan the approach and ensure the continuity of the company's operations;
iii. Meet frequently to ensure that operational and strategic matters are discussed and to provide guidance to the executive directors and senior management. Board meetings shall be held once a quarter at the Company's offices, and two Directors must attend, either in person or by proxy, in order to constitute a quorum. In addition to the Directors and the Company Secretary, senior management, external auditors and legal advisers may attend the meeting, as well as any other member of the Company's staff who receives an invitation from the Board;
iv. Ensure that matters relating to internal audit, compliance and risk management are reviewed at least once a year and provide guidance to the heads of the relevant departments on future actions and the policies to be followed;
v. Address any issues raised by the regulator and define the measures to be taken should corrective action be required.

7.2. Responsibilities of Senior Management

Senior Management, executive directors and members of management who are directly responsible for:

- Establishing the risk management strategies to be followed by the Company.
- Ensuring that the company complies with applicable rules and regulations.
- Addressing and resolving day-to-day operational issues.

Senior Management is responsible for ensuring that the Company complies with its legal obligations and reviews the effectiveness of the policies and procedures followed by the Company in relation to the provision of its authorised payment services.

Specifically, the following actions are carried out:

- Senior Management receives regularly updated information, at least once a year, on the activities of the Company's Internal Audit, Compliance and Risk Management functions.

- Senior Management reviews the activities of each of the Company's departments to address any identified deficiencies.
- Senior Management presents matters requiring discussion and resolution to the Board of Directors.
- The AML Policy is reviewed and assessed annually by the Company's management: the Chief Executive Officer, the Chief Financial Officer and the Compliance Manager. The AML Policy is updated in accordance with financial legislation, the acquiring bank's regulations and internal policy.
- The company has a Regulatory Compliance department with extensive experience, whose objective is to ensure that all the company's clients comply with both the company's high standards and the acquiring bank's requirements.
- It represents the Board of Directors' strategy, makes decisions through leadership and management, and is responsible for the implementation of the strategic plan.
- To provide information to the Board of Directors on the major projects the company plans to undertake.
- Review the policy and procedures the company will implement and establish the strategy the company will follow, subject to the approval of the Board of Directors.
- Advise the Board of Directors as appropriate.
- Oversee the company's day-to-day operations and submit any requested reports to the Board of Directors for review, resolution or approval where necessary.
- To be responsible for the reorganisation of the company's business, where necessary.
- Ensure that the company maintains and implements an adequate internal control mechanism.
- Ensure that the company complies with its legal obligations to the Central Bank.
- Periodically assess whether the company's policies and procedures comply with the relevant legislation issued by FINCEN.
- Ensure that the conditions included in subcontracting agreements with relevant service providers or individuals are met at all times.
- Determine the access privileges of relevant users within the company (as applicable).
- Ensure that the company has sufficient resources and expertise to carry out its operations.
- Responsible for the Company's Substitution Policy.
- Take all measures deemed appropriate to remedy any weaknesses and/or deficiencies identified in the AMLCO's Annual Report.

7.3. Appointment of the AMLCO

The Anti-Money Laundering Compliance Officer (AMLCO) and their deputy are appointed by the Board of Directors. Where deemed necessary due to the volume or geographical scope of the services or activities, AMLCO assistants may be appointed, either by geographical district or otherwise, to support the AMLCO. They are responsible for the implementation and supervision of the company's compliance with this Procedure, as well as with the Act and regulations.

The company shall immediately notify FINCEN of the names and titles of the persons it designates as the AMLCO, Deputy AMLCO and AMLCO Assistants. The AMLCO and Deputy AMLCO must deal with FINCEN in an open and cooperative manner, and must adequately disclose any information that FINCEN might reasonably expect to receive.

The AMLCO and the Deputy AMLCO shall have direct access to the Board of Directors, as well as timely and unrestricted access to all information necessary for the performance of their duties. The AMLCO and the Deputy AMLCO have sufficient seniority and independence within the company to act on their own initiative and perform their duties effectively, objectively and independently, and are fully authorised by the Board of Directors to do so.

All employees must cooperate fully with the AMLCO and the Deputy AMLCO in the performance of their duties.

7.4. Responsibilities of the AMLCO

At a minimum, the AMLCO's duties include the following:

- Development of measures, procedures and controls: the AMLCO develops the anti-money laundering policy and the relevant measures, procedures and controls for the prevention of money laundering and terrorist financing, and describes and assigns the powers and limits of responsibility of each department involved.
- Customer acceptance policy, risk management and compliance, and procedures.

As part of this function, the AMLCO:

1. Develops and establishes the customer acceptance policy, which is submitted via the company's senior management to the Board of Directors for consideration and approval;
2. Prepares the risk management and compliance procedures relating to money laundering and terrorist financing. The AMLCO shall review and assess the relevant Procedure on a regular basis and update it where deficiencies are identified or where it is necessary to adapt the procedures to ensure effective risk mitigation. Any updates to the Procedure must also be approved by Senior Management. The AMLCO must also maintain a Procedure relating to all its functions.

- Supervision: supervises and assesses the correct and effective application of the policy, practices, measures, procedures and controls designed to detect any risk of non-compliance by the company with legal requirements. The AMLCO implements appropriate oversight mechanisms (e.g. on-site visits to different departments of the Company) that will provide all the information necessary to assess the level of compliance of the Company's departments and employees with the procedures and controls in place. Should it identify deficiencies in the application of the required practices, measures, procedures and controls, it provides appropriate guidance for the adoption of corrective measures and, where necessary, reports to the Board of Directors via Senior Management.

Random review of account opening documents obtained from the Company's existing customers to ensure compliance with the Company's procedures and legal requirements.

- Internal reporting procedures (reporting to FINCEN): the AMLCO:

7.5. Appointment of the AMLCO

The Anti-Money Laundering Compliance Officer (AMLCO) and their deputy are appointed by the Board of Directors. Where deemed necessary due to the volume or geographical scope of the services or activities, AMLCO assistants may be appointed, either by geographical district or otherwise, to support the AMLCO. They are responsible for implementing and overseeing the company's compliance with this Procedure, as well as with the Act and regulations.

The company shall immediately notify FINCEN of the names and positions of the persons it designates as the AMLCO, Deputy AMLCO and AMLCO Assistants. The AMLCO and Deputy AMLCO must deal with FINCEN in an open and cooperative manner, and must adequately disclose any information that FINCEN might reasonably expect to receive.

The AMLCO and the Deputy AMLCO have direct access to the Board of Directors, as well as timely and unrestricted access to all information necessary for the performance of their duties. The AMLCO and the Deputy AMLCO have sufficient seniority and independence within the company to act on their own initiative and perform their duties effectively, objectively and independently, and are fully authorised by the Board of Directors to do so.

All employees must cooperate fully with the AMLCO and the Deputy AMLCO in the performance of their duties.

7.6. Responsibilities of the AMLCO

At a minimum, the AMLCO's duties include the following:

- Development of measures, procedures and controls: the AMLCO develops the anti-money laundering policy and the relevant measures, procedures and controls for the prevention of money laundering and terrorist financing, and describes and assigns the powers and limits of

responsibility of each department involved.

- Customer acceptance policy, risk management and compliance, and procedures.

As part of this function, the AMLCO:

- Develops and establishes the customer acceptance policy, which is submitted via the company's senior management to the Board of Directors for consideration and approval;
- Prepares the risk management and compliance procedures relating to money laundering and terrorist financing. The AMLCO shall review and assess the relevant Procedure on a regular basis and update it where deficiencies are identified or where it is necessary to adapt the procedures to ensure effective risk mitigation. Any updates to the Procedure must also be approved by Senior Management. The AMLCO must also maintain a Procedure relating to all its functions.
- Supervision: supervises and evaluates the correct and effective application of the policy, practices, measures, procedures and controls designed to detect any risk of non-compliance by the company with legal requirements. The AMLCO implements appropriate oversight mechanisms (e.g. on-site visits to different departments of the Company) that will provide all the information necessary to assess the level of compliance of the Company's departments and employees with the procedures and controls in place. Should it identify deficiencies in the application of the required practices, measures, procedures and controls, it provides appropriate guidance for the adoption of corrective measures and, where necessary, reports to the Board of Directors via Senior Management.
- Random review of account opening documents obtained from the Company's existing customers to ensure compliance with the Company's procedures and legal requirements.
- Internal reporting procedures (reporting to FINCEN): the AMLCO:

    1. receives information from company employees that is considered to constitute knowledge of or suspicion regarding money laundering (ML) or terrorist financing (TF) activities, or that could be related to such activities. The information is received via a written report using the Internal Suspicion Report ('ISR') (Appendix 1);
    2. assesses and reviews the information received and analyses the circumstances of the case with the reporting officer and, where appropriate, with the reporting officer's superiors. The assessment of the information received is documented in the Internal Evaluation Report ('IER') (Appendix 2);
    3. If, following the assessment, the AMLCO decides to notify FINCEN, it does so by submitting a report via the 'FINCEN electronic reporting system', the portal maintained by FINCEN (Appendix 3). Following the submission of the CO's report to FINCEN, the accounts involved and any other related accounts are closely monitored by the AMLCO officer;
    4. If, following the assessment, the AMLCO decides not to notify FINCEN, it must explain in detail the reasons for that decision in the Internal Evaluation Report;
    5. Acts as the first point of contact with FINCEN at the start of and during an investigation resulting from the submission of a report to FINCEN;
    6. Maintains a record containing statistical information (e.g., district and branch/unit managing the customer's account(s), date of submission of the internal report, date of assessment, date of notification to FINCEN) in relation to SARs and the AMLCO's reports to FINCEN.

- Preparation of a client list: ensures the preparation and maintenance of client lists classified according to a risk-based approach (low, normal, high risk) containing, amongst other things:
    1. The names of the clients;
    2. Their account number (customer ID);
    3. The date the business relationship began;
    4. The branches holding the account;

5. Keeps a record of all potential customers whom the company has rejected;
6. Ensures that records are updated for all new or existing customers, in light of any additional information obtained.

Furthermore, ensures that these lists are updated with all new or existing customers, in light of any additional information obtained.

Furthermore, the AMLCO is responsible for maintaining in its records potential customers with whom it has not been permitted to establish a business relationship.

- Preparation of a list of third parties: the AMLCO must maintain a record containing all details and information (name, business address, activities, regulator, start date of the business relationship, last assessment date, next assessment date and assessment rating) regarding third parties with whom the PI has a business relationship.
- Identification, recording and assessment of risks and updating of procedures – The AMLCO:
    1. Identifies, records and assesses, at least once a year, all risks arising from existing and new customers, as well as from new payment instruments and services, and updates and modifies the systems and procedures applied by the company for the effective management of the aforementioned risks;
    2. Ensures that appropriate measures and procedures are in place to minimise risks.
- Training – The AMLCO:
    1. Provides advice and guidance to the Company's employees on matters relating to money laundering and terrorist financing;
    2. Identifies the departments and employees within the Company that require the most training and education in order to prevent money laundering and the financing of terrorism, and organises appropriate training sessions;
    3. Develops and implements an annual staff training programme, and assesses the suitability of the education and training provided;
    4. Maintains complete records of all seminars and other training activities provided to employees.
- AMLCO Annual Report: the annual report, prepared by the AMLCO, is an important tool for assessing the company's level of compliance with its obligations. The annual report is prepared and submitted for approval to the Board of Directors within two months of the end of each calendar year, and must be submitted to the Board of Directors via PI's Senior Management.
- Additional duties of the AMLCO:
    1. Respond to all requests and enquiries from FINCEN, provide all requested information and cooperate fully with FINCEN;
    2. The AMLCO and deputy AMLCOs acquire the knowledge and skills necessary to implement adequate internal procedures to recognise, prevent and report transactions/activities suspected of being associated with money laundering or terrorist financing;
    3. Assess the suitability of the measures and procedures applied by a third party on whom the company relies for customer identification and due diligence, or which requests the opening of 'customer accounts';
    4. Reports to the Company's Senior Management, through regular periodic reports (in addition to the Annual Report), on the management of risks associated with money laundering and terrorist financing;
    5. Obtains and utilises country assessment reports on money laundering issued by the Financial Action Task Force (FATF) and the regional international bodies established and operating in accordance with FATF principles (the International Monetary Fund and the World Bank);
    6. Collaborates and exchanges information with other Anti-Money Laundering Officers (AMLCOs) of affiliated companies, where appropriate;
    7. Compiles or advises on corrective measures in response to the Central Bank's findings.

8. It assesses the findings of the Internal Audit Unit to adopt corrective measures aimed at the prevention and suppression of money laundering and terrorist financing.

7.7. The Internal Audit Department

FINANCREDITS BNK shall commission periodic reviews and assessments of the effectiveness of its anti-money laundering policies, procedures, systems and controls, as well as compliance with them, and shall specifically cover the following:

i. sample checks on compliance with the company's CDD provisions;
ii. an analysis of all notifications made to the AMLCO to highlight any areas where procedures or training need to be improved; and
iii. a review of the nature and frequency of dialogue between the Board of Directors and the AMLCO.

Such reviews shall be carried out by the internal audit function at least once a year. The internal auditor's conclusions and observations shall be presented, in the form of a written report, to the Board of Directors, which shall decide on the measures to be taken to ensure the rectification of any weaknesses and/or deficiencies that have been detected.

The Chief Compliance Officer (CCO) and the Anti-Money Laundering Compliance Officer (AMLCO) must submit the minutes of the Board of Directors' decision referred to above and the internal auditor's report to FINTRAC within twenty days of the date of the relevant meeting, and no later than three months after the end of each calendar year.

7.8. The Internal Audit Department

FINANCREDITS BNK shall commission periodic reviews and assessments of the effectiveness of its anti-money laundering policies, procedures, systems and controls, as well as compliance therewith, and shall specifically cover the following:

i. sample checks on compliance with the company's CDD provisions;
ii. an analysis of all notifications made to the AMLCO to highlight any areas where procedures or training need to be improved; and
iii. a review of the nature and frequency of dialogue between the Board of Directors and the AMLCO.
iv. Such reviews shall be carried out by the internal audit function at least once a year. The internal auditor's conclusions and observations shall be submitted, in the form of a written report, to the Board of Directors, which shall decide on the measures to be taken to ensure the rectification of any weaknesses and/or deficiencies that have been detected.
v. The Chief Compliance Officer (CCO) and the Anti-Money Laundering Compliance Officer (AMLCO) must submit the minutes of the Board of Directors' decision referred to above and the internal auditor's report to FINTRAC within twenty days of the date of the relevant meeting, and no later than three months after the end of each calendar year.

7.8. Annual Anti-Money Laundering Report

The Annual Report, following its approval by the Board of Directors, is sent to FINCEN together with the minutes of the meeting at which the report was discussed and approved. The minutes include the measures decided upon to rectify any weaknesses and/or deficiencies identified in the annual report and the timeframe for implementing such measures. These minutes and the annual report are sent to FINCEN within twenty days of the date of the relevant meeting, and no later than three months after the end of the calendar year.

The Board of Directors reviews and approves the Annual Report. The company's senior management shall then take all measures it deems appropriate in the circumstances to remedy any weaknesses and/or deficiencies identified in the Annual Report. The AMLCO must also keep senior management informed of any potential diversification of the identified risks.

The Annual Report covers, at a minimum, the following:

- Information on the measures adopted and/or procedures introduced to comply with amendments and/or new provisions of the Act that have occurred during the financial year under review.
- Information on the number of inspections and reviews carried out by the AMLCO and the Internal Audit Unit, reporting on significant deficiencies and weaknesses identified in the policy, practices, measures, procedures and controls that the Company applies for the prevention of money laundering and terrorist financing. In this regard, the report describes the services affected, the severity of the deficiencies and weaknesses, the risk implications, and the measures taken and/or recommendations made to rectify the situation.
- The number of internal reports of suspected money laundering submitted by company employees to the Anti-Money Laundering Committee (AMLCO), broken down by district, department and branch, as well as any comments or observations in this regard.
- The number of suspicious reports submitted by the AMLCO to FINCEN, with information or details on the main grounds for suspicion and highlights of any particular trends.
- The number of suspicious transactions identified by the AMLCO but not submitted to FINCEN.
- Information, details or observations regarding communication with employees on the prevention of money laundering and terrorist financing.
- Information on updates to the policy, measures, practices, procedures and controls applied by the firm in relation to high-risk customers, as well as the number and country of origin of high-risk customers with whom a business relationship has been established or an occasional transaction has been carried out, broken down by category and country of residence or establishment.
- Information on updates to the systems and procedures implemented by the Company for the ongoing monitoring of client accounts and transactions, together with a description of its main operations and any weaknesses identified.
- Information on the training courses/seminars attended by the AMLCO, the deputy AMLCOs and the alternate AMLCO, as well as any other educational material received.
- Information on training and any educational materials provided to staff during the year, reporting, the number of courses/seminars organised, their duration, the number and position of employees who attended, the names and qualifications of the instructors , and specifying whether the courses/seminars were delivered internally or by an external organisation or consultants.
- Results of the assessment of the suitability and effectiveness of staff training.
- Information on the recommended training programme for the coming year.
- Information on the structure and staffing of the AMLCO department, as well as recommendations and timelines for their implementation, regarding any additional staff and technical resources that may be necessary to strengthen anti-money laundering and counter-terrorist financing measures and procedures.
- The AMLCO includes in the annual report a copy of the risk assessment report for the current year, as approved by the Board of Directors.
- Details regarding third parties with whom the company collaborates.

7.9. Notification to FINCEN

The company shall notify FINCEN in writing as soon as possible if:

- it receives a request for information from a regulator or agency responsible for combating money laundering or terrorist financing in connection with investigations into possible cases of money laundering or terrorist financing;
- it becomes aware of, or has reasonable grounds to believe, that a case of money laundering has occurred or may have occurred in or through its business;
- it becomes aware of any matter relating to money laundering or sanctions affecting the company that may have negative consequences for the company's reputation;
- is aware of any significant breach of any section or provision of the Act and regulations.

FINCEN has the power to request that the Company provide information and documents relating to the beneficial owners of legal and natural persons or the existence and details of a business relationship, as well as account balances and information on suspicious transactions or other assets or activities, without the need to obtain a court order. The same applies to requests submitted to FINCEN by the competent authorities of other countries.

AMLCO guarantees that, in the event of an investigation into suspicious activities by FINCEN, it will be able to provide the following information without delay:

i. the identity of the account holder or holders;
ii. the identity of the beneficial owners of the account;
iii. the identity of the persons authorised to manage the account;
iv. details of the volume of funds or the level of transactions passing through the account;
v. linked accounts; and
vi. in relation to specific transactions:
    1. the source of the funds;
    2. the type and amount of currency involved in the transaction;
    3. the manner in which the funds were deposited or withdrawn (e.g. cash, cheques, bank transfers);
    4. the identity of the person who gave the instruction for the transaction;
    5. the destination of the funds;
    6. the form of the instructions and authorisation given; and
    7. the type and identification number of any account involved in the transaction.

8. The risk-based approach

8.1. Summary

FINANCREDITS BNK adopts an anti-money laundering (AML) approach that is proportionate to the risks to which it is exposed as a result of the nature of its business, its customers, products, services and any other matter relevant in the context of money laundering, and ensures that such risk-based assessments are:

i. objective and proportionate to the risks;
ii. based on reasonable grounds;
iii. are properly documented; and
iv. reviewed and updated at appropriate intervals. The company's 'risk-based approach' involves:

- Enterprise risk assessments: periodic assessments of RESEC's activities that enable the Board of Directors to understand the money laundering (ML) and terrorist financing (TF) risks faced by the company, evaluate FINANCREDITS BNK's vulnerabilities to such risks, and take all reasonable measures to eliminate or manage them.
- Customer risk assessments: assessments of the money laundering (ML) and terrorist financing (TF) risks posed by each of the company's customers; an essential part of this is documenting customer knowledge, which is carried out through a risk scoring assessment.
- Risk mitigation: through customer due diligence and ongoing monitoring that is proportionate to the risks that have been assessed.

The application of a 'risk-based approach' enables the Board of Directors and Senior Management to differentiate between customers in a manner that aligns with the risk profile of their particular business. Furthermore, it enables the Board of Directors and Senior Management to apply their own approach in formulating policies, procedures and controls in response to the company's particular circumstances and characteristics. Finally, this method promotes the prioritisation of the company's efforts and actions in response to the likelihood of money laundering or terrorist financing occurring through the

use of the services it provides.

8.2. Business Risk Assessment

The AMLCO and the risk manager are responsible for identifying, recording and assessing all potential risks. A 'risk-based approach' involves the identification, recording and assessment of the risks that need to be managed. The firm shall assess, at least once a year, the money laundering and terrorist financing risks to which its business is exposed, taking into account the nature, scope and complexity of its activities and, to the extent relevant, any vulnerabilities related to:

- the geographical spread of operations;
- the nature and profile of customers, and the products and services used;
- the channel, method and practice of the services provided;
- the volume, size and complexity of transactions;
- the degree of risk associated with each service sector;
- the country of origin and destination of customer funds;
- deviations from the expected level of transactions;
- the nature of commercial transactions;
- non-face-to-face customers;
- a complex ownership structure involving legal entities;
- companies with bearer shares in their shareholding structure;
- companies incorporated in offshore centres;
- politically exposed persons;
- the Client's refusal to disclose the ultimate beneficial owners (UBOs) of a legal entity; and
- the use of new or developing technologies for both new and existing products.

FINANCREDITS BNK will ensure that any risk identified in the business risk assessment is taken into account in its day-to-day operations, including in relation to: (i) the development of new products/services; (ii) the acquisition of new Clients; and (iii) changes to its business profile.

FINANCREDITS BNK will use the information obtained from its periodic business risk assessments to develop and maintain its policies, procedures, systems and controls, in order to ensure that they adequately mitigate the identified risks, assess their effectiveness and contribute to the allocation and prioritisation of resources dedicated to anti-money laundering, as well as to the conduct of customer risk assessments.

8.3. Customer risk assessment

Before carrying out CDD on a new customer, the company will conduct a risk score assessment and assign the customer a risk rating commensurate with the customer's money laundering risk. The AMLCO draws up and maintains a list of customer categories (low, medium or high risk), which contains, amongst other details, customer names, account numbers and the start date of the business relationship. These lists are updated without delay to include all new or existing customers identified by the Company.

When conducting a customer risk assessment, the Company:

i. identify the customer or customers and any beneficial owner;
ii. obtain information on the purpose and intended nature of the business relationship;
iii. take into account:
    a. the nature of the Customer, its ownership and control structure, and its beneficial ownership, if any (i.e. its legal structure, activity or profession, location of the Customer's business and commercial rationale for its business model, expected turnover)
    b. the nature of the Customer's business relationship with the Company (i.e. how the Customer is introduced to the Company; the Customer's country of origin, residence, nationality, place of incorporation or place of business; the volume of transactions; the duration of the business relationship)

c. the relevant risk associated with the products and services (i.e. types of transactions, types of products/services)

iv. taking into account the results of the business risk assessment

Following a review of the risk assessment, the Firm will assign each Client a risk rating of 'high', 'medium' or 'low'. Please note that Clients with similar characteristics may be assigned different risk ratings, taking into account the product or service in question and any other factors relevant to the Client's risk assessment. The Client's risk assessment shall be fully documented, reviewed and approved by the AMLCO and filed in the Client's record. All 'high' risk business relationships and any business relationship involving a PEP or bearer shares must be approved by the Company's Risk Committee.

The firm will periodically review each client's risk rating to ensure it remains up to date in light of current AML risks

8.4. Low-risk clients

This category includes the following Clients:

- Credit or financial institutions subject to the Act;
- Credit or financial institutions located in a country outside the United States with requirements equivalent to those established by the Act and which are subject to supervision for compliance with such requirements;
- Publicly traded companies whose securities are admitted to trading on a regulated market in the United States
- in a third country subject to disclosure requirements consistent with EU legislation;
- National public authorities in the US and countries within the European Economic Area;
- A pension scheme or similar arrangement providing retirement benefits to employees, where contributions are made by deduction from wages and the scheme rules do not permit the transfer of members' rights under the scheme;
- Customers with a low risk score;
- In the above cases, the Company must gather sufficient information to determine whether the Customer meets the requirements to be classified as a low-risk Customer and to carry out the simplified customer identification and due diligence procedure (see section 9.2. for further information).
- Public authorities or public bodies in the US or the countries of the European Economic Area must meet all of the following criteria to be considered low-risk:
- They have been entrusted with public functions;
- Their identity is public, transparent and verifiable;
- Their activities, as well as their accounting practices, are transparent;

8.5. Medium-risk customers

This category includes the following customers:

- Public companies listed on stock exchanges in countries that do not adequately implement the FATF Recommendations;
- Private companies not classified as high-risk; and
- Any other customer who does not fall into the high-risk or low-risk categories.
- The following documents must be obtained for corporate customers (see section 8.5.2. for further information):
- Certificate of incorporation;
- Certificate of registered office;
- Certificate of directors and secretary;
- Certificate of registered shareholders;

- Memorandum and Articles of Association;
- Legal ownership structure leading to the ultimate beneficial owners (UBOs), signed by the UBO or the person exercising ultimate control over the legal entity or the person with ultimate responsibility for decision-making and managing the client's operations;
- Resolution of the board of directors appointing the person who will open and manage the legal entity's account;
- Identification of the persons exercising ultimate control over the legal entity's activities and assets. The firm verifies the identity of the natural persons exercising ultimate control, even if such persons hold no direct or indirect interest, or if their interest is less than 10% plus one share, in the ordinary share capital or voting rights of the legal entity;
- A recent bank statement showing the details of the bank account in the customer's name to verify the bank details provided;
- Certificate of good standing (optional);
- In the case of regulated companies, the relevant licence is required; and
- Valid identification documents for the directors, the beneficial owner and the authorised signatories.

8.6. High-risk customers

This category includes the following clients:

- Accounts held in the name of companies whose shares are bearer shares;
- Trust accounts;
- Customer accounts held in the name of a third party;
- Accounts held by politically exposed persons;
- Accounts held by persons who do not meet the definition of a politically exposed person (PEP), but whose prominence or influence poses a high risk of corruption;
- Online betting and gambling;
- Customers who do not wish to provide information on the ultimate beneficial owners of a legal entity;
- Non-face-to-face customers;
- Businesses whose commercial relationship is conducted under unusual circumstances (for example, a significant and unexplained geographical distance between the business and the customer);
- Businesses that handle large amounts of cash;
- Charities and foundations, as well as Islamic foundations; and
- Any other customer whom the Risk and Compliance departments determine should be classified as such.

8.7. Politically exposed persons

Politically exposed persons ('PEPs') are natural persons who have been or are currently entrusted with prominent public functions in Canada or any other country, as well as their immediate family members or persons known to be close associates of such persons.

FINCEN considers that:

i. Whilst 'PEP' status does not in itself incriminate the person in question or any entity with which they are associated, it places the Client, or the Beneficial Owner, in a higher-risk category;
ii. In general, a foreign PEP presents a higher risk of money laundering because there is a greater risk that such a person, if engaged in money laundering, would attempt to place their money abroad, where the Customer is less likely to be recognised as a PEP and where it would be more difficult for law enforcement agencies in their home jurisdiction to seize or freeze their criminally derived assets;

iii. After leaving office, a PEP may continue to pose a higher risk of money laundering if that person continues to exert political influence or otherwise poses a risk of corruption;
iv. Politically exposed persons (PEPs) are considered high-risk from the perspective of anti-money laundering; Therefore, any relationship between FINANCREDITS BNK and a PEP must always be approved by an executive director, preferably by the managing director or deputy managing director and the director, whether the PEP already has a business relationship with FINANCREDITS BNK or is joining the company for the first time. To enable executive directors to make an informed decision regarding the continuation of a relationship with an existing PEP or the onboarding of a new PEP as a customer, the following information must be gathered to create a profile of the PEP as part of enhanced due diligence:
    1. Jurisdiction;
    2. Business profile;
    3. Products offered or requested by the PEP;
    4. Source of funds and assets; and
    5. Information available from public sources;

It should be noted that, under this Policy, domestic PEPs are subject to the same enhanced due diligence and the aforementioned procedures as foreign PEPs.

9. Classification of customer types

9.1. Accounts held by natural persons ('Customers'/'Users')

To create your account profile, the following information must be collected:
- Purpose and reason for requesting the establishment of a business relationship;
- Expected monthly turnover;
- Nature of the transactions;
- Expected source of incoming funds;
- Expected destination of outgoing transfers/payments (target market);
- Approximate volume of previous payment transactions (processing history), where applicable;
- Clear description of the main commercial/professional activities/operations;
- The customer's profession and other occupations, including the name of the employer/business organisation;
- Real name(s) as appearing on the official identity document or passport;
- Current full permanent address, including postcode;
- Telephone numbers (landline and mobile) and fax number;
- Email address, if available;
- Date and place of birth;
- Nationality;
- Signature.

The Company will request an identity card or passport from individuals as proof of identity. Proof of residence must include a utility bill (e.g. electricity, water) or proof of home insurance or council tax and/or a bank statement.

Furthermore, in the event of any doubt regarding the authenticity of any document (passport, identity card or proof of address), the Company will request verification of identity from the Home Office, the embassy or consulate of the issuing country, or a reputable credit institution or reliable financial institution located in the customer's country of residence.

The Company will verify precisely whether the customer holds or has held public office (PEP), has been included on the relevant list of persons subject to financial sanctions and/or poses a risk to the business because they have been flagged by additional searches carried out by AMLCO.

Alternative identity verification where certified documents cannot be provided or it is unreasonable to expect a customer (natural persons) to provide them.
The company has recognised that clients may face considerable difficulties in obtaining certified documentation, both from a financial and practical standpoint, and has also noted that a significant number of clients prefer alternative service providers that do not impose such requirements. Consequently, without prejudice to the certification requirements and taking into account the potential risks, the following alternative measures shall apply in such cases:

For proof of identity
In cases where the Company has difficulty obtaining the above, taking into account all potential risks, the Company will obtain copies of identification documentation, which will be verified through a third-party source.

This alternative process shall NOT apply to High-Risk Clients or to Clients classified as Low or Medium Risk where the transaction volume of their account exceeds $50,000 USD in any calendar year.

For proof of residence
- By using an established and maintained regulatory or government database; or
- Post (such communication must be sent by registered post) – (i) The Company will send an official letter to the Client's address containing a validation code, which the Client must provide to the Company in order to verify the address provided by the Client; (ii) The Company may also conduct a telephone interview with the Client, during which the Client must confirm the validation code in order to verify their identity and place of residence.

The company shall notify FINCEN if, at the start of the business relationship or during the course of it, it is established that a customer appears on the lists of persons subject to restrictive measures as provided for by law.

9.2. Accounts of legal entities (companies, 'Clients')

Before establishing a business relationship, steps must be taken through a company search and/or other business enquiries to ensure that the applicant company has not been, and is not in the process of being: dissolved, struck off the register, wound up or liquidated. Furthermore, if changes subsequently occur in the company's structure or ownership, or if suspicions arise due to a change in the pattern of payments through a company account, additional checks must be carried out.

The following documents (originals or certified copies) must be obtained for corporate entities (customer incorporation):

- Certificate of incorporation;
- Certificate of registered office;
- Memorandum and Articles of Association;
- Certificate of directors and secretary;
- Certificate of registered shareholders (in the case of private legal entities);
- Certificate of good standing (for companies incorporated more than one year prior to the date of application to become a client);
- In the case of regulated companies, the relevant licence is required;

- Resolution of the Board of Directors to open an account and grant authority to those who will operate it (certified by the secretary of the legal entity);
- Where registered shareholders act as representatives of the beneficial owners, a copy of the deed or trust agreement entered into between the representative shareholder and the beneficial owner, pursuant to which it has been agreed that the shares shall be registered in the name of the representative shareholder on behalf of the beneficial owner;
- Legal ownership structure certified by the UBO or the person exercising ultimate control over the legal entity or the person with ultimate responsibility for decision-making and managing the Client's operations;
- Identification of the persons exercising ultimate control over the activities and assets of the legal entity (including where such persons hold no direct or indirect interest, or where their interest is less than 10% plus one share of the ordinary share capital or voting rights of the legal entity);
- Where deemed necessary to better understand the activities, sources and uses of the funds or assets, the Company will obtain copies of the latest audited financial statements (if available) and/or copies of the latest management accounts;
- A recent bank statement showing the details of the bank account in the client's name to verify the bank details provided (please note that the bank details must correspond to the company or its parent company);
- Declaration of the company's ultimate beneficial owners (if different from the shareholders) (optional);
- Certified copy (recent, no more than 6 months old) of a bank statement, utility bill or local authority tax bill, to verify the address of the head office (optional);
- Various public information materials, annual reports, press releases, website materials;
- As an additional due diligence measure, the company may conduct a search and obtain information from the relevant commercial register or other sources, such as credit rating agencies or background check providers;
- Adequate documentation and sufficient information to fully understand the control structure and management of business activities, as well as the nature of the services and activities provided by the client;
- The identity of directors, partners, beneficial owners and other persons authorised to manage the account is verified. The verification of the identity of these persons must be carried out in accordance with the procedures for verifying the identity of natural persons;

Note:
If the shareholders or directors are legal entities (as opposed to natural persons), the firm obtains the following identification documents right up to the ultimate beneficial owner:

1. Certificate of shareholders
2. Certificate of directors
3. Information on these persons provided by background check providers
4. In the case of legal entities incorporated outside Canada, the firm requests and obtains documents similar to those mentioned above.

Alternative identity verification where certified documents cannot reasonably be provided for a customer (sections 12.2, 12.3 and 12.4)

The Company has recognised that Clients may face substantial difficulties in obtaining certified documentation, both from a financial and practical perspective, and has also identified a substantial risk to the business due to such Clients preferring alternative service providers that do not impose such requirements. Consequently, without prejudice to the certification requirements and taking into account the potential risks, the following alternative measures shall apply in such cases:

a. KYC for directors/shareholders:

- WorldCheck: this shall apply to all natural persons where the customer is a legal entity, including the shareholders of the legal entity, authorised persons and the beneficial owner(s);
- Obtain the documentation provided by the official Companies Register of the client's relevant jurisdiction and verify the documentation obtained by the client.

b. Company documentation:

- The company must obtain the documentation provided by the official Commercial Register of the relevant jurisdiction of the client and verify the documentation obtained by the client;
- WorldCheck: this will be carried out on all natural persons where the client is a legal entity, including the shareholders of the legal entity, authorised persons and the beneficial owner(s);

9.3. Accounting for unincorporated businesses, partnerships and other legal entities without legal personality

In the case of unincorporated businesses, partnerships and other entities without legal personality:

- The identity of directors, partners, beneficial owners and other persons authorised to manage the account is verified. The verification of the identity of these persons must be carried out in accordance with the procedures for verifying the identity of natural persons;
- In the case of companies, the original or a certified copy of the company's registration certificate is obtained;
- Proof of the address of the company's registered office is obtained;
- The nature and scope of its activities are determined;
- The formal partnership agreement (if any);
- A power of attorney from the company authorising the opening of the account and confirming the authority of a specific person who will be responsible for its operation;
- All information necessary to create the company's financial profile (as for legal entities).

9.4. Front men, agents or third parties

The Company takes reasonable steps to obtain the appropriate documents, data or information in order to establish and verify the identity of:

- The representative or agent of the third party;
- Any third party on whose behalf the representative or agent is acting.
- In addition, the Company obtains a copy of the authorisation agreement entered into between the parties concerned.

9.5. Third party

The term 'third party' refers to a credit or financial institution, auditors, independent legal professionals, persons providing fiduciary and corporate services to third parties, accountants or tax advisers (but not money transfer companies or foreign exchange operators) who:

1. Are subject to compulsory professional registration recognised by law.
2. Are subject to supervision regarding compliance with the requirements of the Act
3. The third parties referred to above must: Be subject to mandatory professional registration recognised by law; and Be subject to supervision regarding compliance with the requirements of the Act.

Third-party assessment

The Company obtains data and information in order to verify that the third party is subject to professional registration in accordance with the applicable legislation of its country of incorporation and/or operation, as well as to supervision for the purposes of compliance with anti-money laundering and counter-terrorist financing measures. Where the third party in question is an accountant, an independent legal professional or a provider of fiduciary and corporate services, the Company, prior to accepting the customer identification data verified by that third party, applies the following additional measures and procedures:

a. It analyses and assesses the systems and procedures applied by the third party for the prevention of money laundering and terrorist financing.
b. As a result of the above assessment, it is verified that the third party implements customer identification and due diligence systems and procedures that are in line with the requirements of the Act and FINCEN's regulations and guidelines.
c. It maintains a separate file for each third party, in which it stores the aforementioned assessment report and other relevant information (e.g. identification data, minutes of meetings, evidence of the data and information).
d. Collaboration with the third party commences, and acceptance of the customer identification data verified by the third party is subject to the approval of the compliance officer.
e. A copy of the policies and procedures that the third party undertakes to apply is received.
f. Details of the third party's Anti-Money Laundering Compliance Officer (AMLCO).
g. The compliance officer maintains a list containing the (name, business address, activities, regulator, start date of the business relationship) of the third parties with whom the payment institution has a business relationship.
h. The AMLCO shall ensure that the business relationship the company maintains with such third parties is assessed annually and that records are kept containing the details of the
i. Third Parties (i.e. name, address, sector of activity, regulatory authority, start date of the business relationship, date of the last assessment, next assessment, assessment rating) with whom the company has established a business relationship.

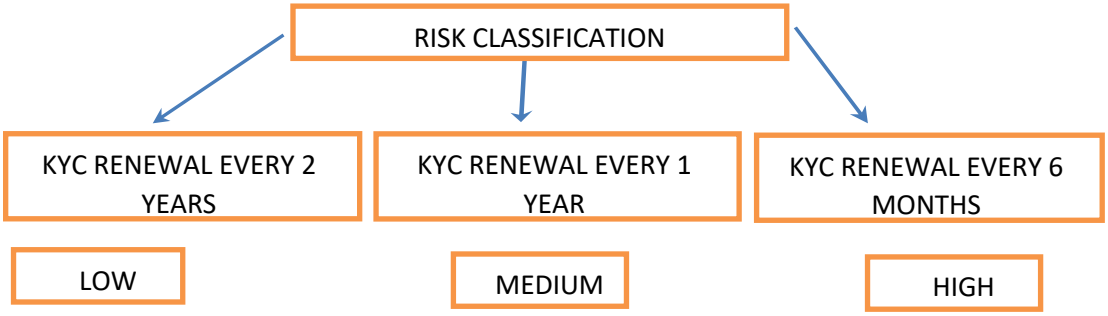
Use of third parties for customer identification and due diligence purposes

The Company may use third parties to apply the requirements for:

a. Identifying the customer and verifying their identity.
b. Identifying the beneficial owner and verifying their identity.
c. Obtaining information on the purpose and intended nature of the business relationship with regard to customer identification procedures and customer due diligence measures. It should be noted that the ultimate responsibility for complying with the above requirements rests with the company.
d. The Company must obtain copies of customers' identification documentation from third parties, taking into account the level of risk associated with each customer, the business relationship, the product or the transaction involving the following third parties:
e. Credit institutions or financial organisations subject to the Act and operating in Canada, the US or a country within the European Economic Area, or in another country with anti-money laundering requirements similar to those in Canada.
f. Any third party carrying out financial activities and operating in a country outside the EEA that applies the same requirements as those set out in the Act.

9.6. CDD update / periodic review

In accordance with its Procedure, FINANCREDITS BNK carries out periodic KYC reviews on all its Customers. The diagram below illustrates the periodic KYC review process.
The frequency of the periodic KYC review depends on the customer's risk level, as indicated below:



In addition to the above, the Compliance department will also review an account outside the specific review date when an account-related event or incident has alerted the company to potential adverse information (also known as a 'trigger event').
Passports and ID documents will be monitored and flagged to indicate expiry dates. Expired passports or ID documents will be requested shortly before the expiry date via system alerts.

9.7. Prohibited Clients

- The Company shall not enter into a business relationship with a Client who is a Legal Person if the Client's ownership or control arrangements prevent the Company — taking into account the specific risk circumstances and risk assessment — from identifying one or more of the Client's beneficial owners.
- The Company shall not open or maintain anonymous accounts, accounts in the name of fictitious persons, or accounts in the name of third parties which are in the name of one person but are controlled or held for the benefit of another person whose identity has not been disclosed to the Company.
- The Company maintains a list of prohibited countries as described in Appendix 7.
- The Company maintains a list of prohibited industries as described in Appendix 8.
- The Company shall not establish any business relationship with a fictitious bank.

10. Customer Due Diligence

Customer due diligence ('CDD') is the process of:

- verifying the identity of the customer and any beneficial owner based on original documents, or on data or information issued by or obtained from a reliable and independent source;
- understanding the source of funds and the source of the customer's wealth, for example, by consulting published accounts or a customer questionnaire; and
- to carry out ongoing customer due diligence in relation to the business relationship with the Customer.
- For the purposes of this section of the Procedure, the term 'Customer' includes any of the following:
- a customer of the company's products or services, and custody;
- a business partner, such as an execution broker or a supplier.
- The level of CDD to be carried out (both initially and during the business relationship) must be determined based on the client's risk rating assigned in the client risk assessment.
- At a minimum, the customer identification process must establish:
- That FINANCREDITS BNK is dealing with a real natural or legal person (i.e. that the Customer physically exists);

- That the customer is that entity (i.e., to avoid the risk of identity theft);
- That the entity has identifiable owners and controllers and its representatives can be located at the address provided;
- The nature of the normal business activities the entity expects to carry out;
- The legitimacy of the source of its assets and its business activities; and
- When carrying out these checks, FINANCREDITS BNK must determine that the customer is engaged in legitimate activities and has legitimate sources of assets.

10.1.Application of customer due diligence

The company will apply customer identification procedures and due diligence measures in respect of customers in the following cases:

- When establishing a business relationship;
- Where there is a suspicion of money laundering or terrorist financing, regardless of the transaction amount;
- Where there are doubts regarding the accuracy or suitability of the customer identification details previously provided;
- When an inactive account is reactivated;
- When there is a change in the customer's risk classification (i.e. from a low-risk customer to a medium- or high-risk customer); and
- When adverse information about a customer is identified.
- The Company applies each of the due diligence measures and customer identification procedures mentioned above, but may determine the scope of such measures on a risk-sensitive basis, depending on the type of customer, the business relationship, the product or the transaction. The Company must be able to demonstrate to the Competent Supervisory Authorities ('CBA') that the scope of the measures is appropriate in view of the risks posed by the use of its services for the purposes of money laundering and terrorist financing.

10.2. Simplified due diligence

The Company may apply simplified customer identification and due diligence procedures to low-risk customers. Please note that this is not an automatic exemption and is only applied once the customer has undergone the appropriate risk assessment, which has not resulted in high-risk findings. This applies to customers who are:

- Regulated financial institutions or collective investment undertakings, or subsidiaries or branches of such entities domiciled in the EU or the US;
- Regulated financial institutions or collective investment undertakings domiciled in, or subsidiaries or branches of such entities domiciled in, approved countries;
- Listed companies whose securities (other than debt securities or securities representing underlying securities, i.e. ADRs and GDRs) are admitted to trading on a regulated stock market, as well as subsidiaries or branches of such entities;
- Public and government departments, agencies and authorities of the US and EU Member States, or legal entities controlled (50% + 1) by the US and EU Member States;
- Supranational organisations, for example, the IMF, the World Bank, the EBRD, the UN, etc.
- The company's policy is to collect sufficient information to assess a customer as low risk. Simplified CDD must be proportionate to the identified money laundering risks and may include any of the following elements:
- verifying the identity of the customer and the beneficial owner after the business relationship has been established;

- reducing the frequency of customer identification updates or, where appropriate, not carrying them out;
- deciding not to verify the identity of the beneficial owner;
- deciding not to verify an identification document beyond requesting a copy;
- collecting information on the pattern and level of transactions expected from a customer in order to determine which are unusual or suspicious;
- verify a customer's financial profile:
- The purpose and reason for requesting the establishment of a business relationship;
- The customer's expected turnover;
- The nature of the transactions;
- The intended source of incoming funds and the destination of outgoing funds;
- The customer's assets and annual income; and
- A description of the main business or professional activities.
- not to inquire into the source of the funds or the source of the customer's assets;
- reduce the level of ongoing monitoring of transactions, based on a reasonable monetary threshold or the nature of the transaction;
- not to collect specific information or apply specific measures to understand the purpose and intended nature of the business relationship, but to infer such purpose and nature from the type of transactions or the established business relationship.

Although the risks may be low for all such Clients, the Company will not adopt a one-size-fits-all approach for all its low-risk Clients and will carry out CDD that is proportionate to the risks identified on a case-by-case basis. For example, where the risks of money laundering (ML) or terrorist financing (TF) are very low, the Company may simply identify the Customer and verify such information only to the extent commercially necessary, whilst in the case of a complex Transaction, more comprehensive simplified CDD may be required.

The Company may reasonably reduce the frequency of updates to the Customer's identification or omit them where ML or TF risks are low and the service provided to the Customer does not present a realistic opportunity for ML/TF.

10.3.Enhanced due diligence

If the Client has been assigned a 'High' risk rating following the Client risk assessment, the Company must carry out enhanced CDD. All higher-risk clients must be approved by the AMLCO or the Deputy AMLCO and by the CEO/MD.

Enhanced due diligence is carried out when the business relationships to be established:

i. are linked to a politically exposed person;
ii. are linked to non-face-to-face clients;
iii. relate to a customer who is a legal person with bearer shares in circulation or with the capacity to issue bearer shares in accordance with its memorandum and articles of association, or to subsidiaries of such legal persons;
iv. relate to online betting or gambling;
v. relate to a legal entity or unregulated trust domiciled in a high-risk jurisdiction listed in Appendix 7;
vi. relate to a fund domiciled in a high-risk jurisdiction listed in Appendix 7, or are managed by a fund manager and administered by a fund administrator not regulated in the US, the EU or an approved country;
vii. any other instance where there is a suspicion of money laundering.

Enhanced CDD involves, to the extent necessary as determined on a case-by-case basis, the following:

- obtaining and verifying additional information:
  i. identification details of the Customer and any Beneficial Owner;
  ii. information on the intended nature of the business relationship; and
  iii. information regarding the reasons for a transaction.
- updating the CDD information held by the Company regarding the Customer and any Beneficial Owner more regularly;
- verify information regarding the source of funds and the source of the Customer's wealth;
- increase the level and scope of monitoring of the business relationship, in order to determine whether the customer's transactions or activities appear unusual or suspicious;
- obtain approval from the chief executive, senior management or the board of directors to enter into a business relationship with the customer.
- Where appropriate, enhanced CDD measures may include:
- obtaining documentary evidence regarding the source or circumstances giving rise to the Client's funds and assets;
- gaining a better understanding of the client's business activity and structures, their use of the Company's products and services, as well as the nature and volume of business to be expected from the client;
- taking steps to ensure that the Customer's use of complex legal structures and/or the use of trusts and private investment vehicles serves a genuine and legitimate purpose, and to properly understand the chain of ownership, authority or control leading to the Beneficial Owner, the settlor and the beneficiaries, where applicable;
- to the extent that the assets belong to the Beneficial Owner and not to the Client, to enquire into the source of the funds and the source of the funds/assets of the Beneficial Owner;
- verify the source of the funds by obtaining independent corroborating evidence, such as, for example, deposit slips from a recognised bank (and the length of time such deposits have been held at that institution), dividend payments relating to a shareholding, bank statements, salary/bonus certificates, loan documentation and evidence of a transaction that gave rise to the payment into the account. A customer must be able to demonstrate and document how the funds in question are linked to a specific event that gave rise to the payment into the account or to the source of funds for a transaction;
- verify the source of wealth by obtaining independent corroborative evidence, such as, for example, share certificates, publicly accessible property records, bank or brokerage account statements, probate documents, audited accounts and financial statements, news reports from a reputable source and other similar evidence;
- request a report from an external provider to obtain further information about a customer or a transaction, or to investigate a customer or a beneficial owner in cases of very high risk. Such reports may be particularly useful where little or no information is publicly available about the person in question.

Accounts of 'politically exposed persons' (PEPs):

With regard to transactions or business relationships with politically exposed persons residing in the United States or in a third country, the following additional due diligence measures shall apply:

- The firm shall have appropriate risk-based procedures in place to determine whether the customer is a politically exposed person. These procedures may include, depending on the degree of risk:

1. The acquisition and implementation of a reliable commercial database on politically exposed persons.
2. Searching for and obtaining information from the customer themselves or from publicly available sources.
3. In the case of legal entities and legal arrangements, the firm shall also verify whether the beneficial owners, authorised signatories and persons authorised to act on behalf of such legal entities and arrangements are politically exposed persons.

- Obtaining the approval of the Chief Executive to establish business relationships with such customers. The decision is then referred to the AMLCO.
- If, after the establishment of a business relationship, the customer is or has become a PEP, then the Chief Executive grants approval to continue the business relationship, which is referred to the AMLCO. If a business relationship has been established with a natural or legal person and the Company subsequently identifies that the relevant natural persons are or have been PEPs, then approval must be obtained from senior management to continue the business relationship (or account). The AML systems must screen Clients (and their related natural persons) at least once a month to identify such cases.
- A competent officer of the company must prepare a brief report on the customer's profile, which shall be submitted to the company's senior manager, who in turn approves the establishment of the business relationship with that customer. However, the final decision to accept or reject a customer rests with the AMLCO.
- Before establishing a business relationship with a PEP, the firm must obtain appropriate documentation to verify not only their identity but also to assess their business reputation (e.g. third-party references).
- Carry out continuous and enhanced monitoring of the business relationship.
- Take appropriate measures to determine the source of wealth and the source of funds involved in the business relationship or payment transaction.
- The account will be subject to an annual review to determine whether it is permitted to continue operating. The competent officer in charge of the account must prepare a note summarising the results of the review. The note must be submitted for consideration and approval to the Company's Senior Management and filed in the client's personal file.

Note:

- With regard to the issue of corruption, the company will use the following sources: Transparency International's (TI) Corruption Perceptions Index (CPI) (www.transparency.org).
- With regard to the adequacy of the implementation of the FATF Recommendations, the Company will obtain information from:
- Country assessment reports produced by the FATF.
- Country assessment reports produced by other regional bodies operating in accordance with FATF principles or the International Monetary Fund, and will take additional precautions with regard to countries that do not meet the Financial Action Task Force (FATF) 40+9 requirements.

Non-face-to-face customers:

Where the customer has not been physically present (i.e. where the customer requests the establishment of a business relationship or an occasional transaction through a representative, an agent, by post, by telephone or via the internet) for identification purposes, the Company:

- Follow the established customer identification and due diligence procedures, as applied to customers with whom it has direct and personal contact, and obtain exactly the same information and identification documents.
- In addition, one or more of the following measures shall be applied:
- Obtain additional documents, data or information to verify the customer's identity.
- Take additional steps to verify or certify the documents provided, or request confirmatory certification from a credit or financial institution subject to the Act.
- Ensuring that the first payment for the transactions is made through an account opened in the customer's name at a credit institution operating in the US or a country within the European Economic Area.
- To comply with the above additional measures, one or more of the following documents will be obtained, at the discretion of AMLCO in each particular case:
- Direct confirmation of the prospective client's genuine name, address and signature by a bank operating in their country of origin.
- Obtaining a letter of reference from a third party (an independent and reliable source).
- Telephone contact with the customer at their home or office, prior to establishing a business relationship or an occasional transaction, via a telephone number that has been verified by a reliable and independent source.
- Contacting the customer by post at an address previously verified by the Company through independent and reliable sources.
- In the case of companies or other legal entities, the Company will take additional measures, if necessary, to ensure that they operate from the address of their head office and carry out legitimate business activities.
- Additional data and information, if necessary, to ensure a proper and complete understanding of their activities and source of wealth.
- For transactions via the internet, telephone, fax or other means where the customer is not present to verify the authenticity of their signature, that they are the true account holder or that they have been duly authorised to operate the account, the Company applies reliable methods, procedures and control mechanisms regarding access to such means, in order to ensure that the person is the true account holder or authorised signatory. (One-time password, one-time code, etc.)

Note: The above measures apply to both natural persons and legal entities.

Accounts in the name of companies whose shares are bearer shares:

The company may accept as clients those companies whose own shares or those of their parent companies (if any) have been issued to the bearer, applying, in addition to the procedures described above for legal entities,
all of the following additional due diligence measures:

- The Company requests copies of the bearer share certificate.
- The company receives the completed version of Appendix 5 or Appendix 6.
- The account is closely monitored throughout its operation. At least once a year, a review of the account's transactions and turnover is carried out and a note authorising the results of the review is prepared, which must be kept in the client's file.

- Where there is a change in the beneficial owners, the Company assesses whether or not to allow the

account to continue operating.

Online betting/gambling:

The company may establish a business relationship or carry out a one-off transaction on behalf of natural or legal persons engaged in online betting or gambling activities, provided that:

- Such persons hold a licence granted by a competent authority in the US, the European Economic Area or another third country that applies sufficient measures for the licensing and supervision of such businesses.
- In addition to the identification documents required for other corporate entities, the Company requires a copy of the licence granted to such persons by the competent supervisory or regulatory authority.
- The authenticity of such a licence will be verified directly with the supervisory or regulatory authority, or through other independent and reliable sources.
- The Company collects the necessary information to understand the control structure of clients and ensures that such clients implement adequate and appropriate systems and procedures for customer identification and due diligence to prevent money laundering and terrorist financing.
- Note: In all the cases mentioned above, the decision to establish a business relationship or to carry out an occasional transaction must always be approved by both the Anti-Money Laundering Committee (AMLCO) and an executive director.
- The account of such a client is subject to close monitoring and periodic reviews (at least once a year) in order to decide whether or not to allow the continuation of their business.

Companies with a trust in their shareholding structure:

When the company establishes a business relationship or carries out an occasional transaction with a client whose shareholding structure includes a trust, it must determine:

- The legal nature of the trust;
- The name and date of incorporation of the trust;
- The nature of the trust's activities;
- The purpose for which the trust was established;
- The origin and source of the funds, requesting the relevant extracts from the trust deed; and
- Any other relevant information regarding the trustees and verification of the identity of the settlor, the trustee and the beneficial owners, in accordance with the customer identification procedures described above.
- Note: All relevant data and information shall be recorded and retained in the customer's file.

Customers from countries that inadequately implement the FATF Recommendations:

The firm applies the following:

- It applies additional monitoring procedures and pays particular attention to business relationships and transactions with persons, including companies and financial institutions, from countries that do not apply or inadequately apply the above recommendations.
- Transactions with persons from such countries, for which there is no apparent economic purpose or visible lawful purpose, shall be subject to more detailed scrutiny in order to determine their background and economic, commercial or investment purposes. If the company is unable to ascertain the legitimacy of the transaction, it must file a suspicious transaction report via the AMLCO with FINCEN.

10.4. Authenticity of documents obtained

Ideally, documents should be inspected in their original form. Where this is not possible (for example, because the business has no physical contact with the customer), it must obtain a first-generation

photocopy certified as a true copy of the original document by a person of good standing, such as a qualified lawyer or notary, a chartered accountant, a bank manager, a police officer, an embassy or consular official, or a similar person (whose identity and objectivity can be demonstrated beyond reasonable doubt).
The certified photocopy must:

i. include a statement certifying that the photocopy is a true copy of the original document;
ii. state the date on which the photocopy was made and certified;
iii. state the name, occupation, business address and telephone number of the person who certified the photocopy.

Please note that the requirement for a 'first-generation' photocopy means that copies of photocopies are not accepted.
Furthermore, all customer identification documentation provided must be recent (where applicable). A document is considered recent when it is submitted to FINANCREDITS BNK within 6 months of the date of issue.

10.5. Language requirements

All customer identification documents collected during the KYC process must be in English. Customer identification documents collected directly from the customer (articles of association and statutes, certificate of incorporation, personal identification documents, etc.) are usually in the local language.
Where these documents cannot be provided in English, the best practice is:

i. Identify the document;
ii. Explain its purpose; and
iii. Please describe the specific content of the document in English (the key points, not a literal translation).

10.6. Certification requirements

Where specified in the KYC document request lists, customer identification documentation must be provided as a certified copy or in the form of an apostille. In all other cases, the originals must be provided.
A certified (true) copy means that the person certifying the copy of the document has seen the original document at the time of certification and is in a position to certify that the copy is a true and complete copy of the original document.

The Company recognises such certifications when they are carried out by reputable independent sources. Such sources include, by way of example, the client's bank operating in Canada or in an approved country, a lawyer or chartered accountant regulated by a professional body (membership number required/verified), a notary public, the embassy or consulate of the client's country of origin in the United States, the US embassy in the client's place of residence, the police or any similar authority. The company requires that the certification process include the certifier stating their name, title or role, signature, date and official stamp on the documents being certified. In all cases, the identity and impartiality of the person carrying out the certification must be demonstrated beyond reasonable doubt.

Where the list of documents required for KYC specifies that documents must be apostilled, this process requires that the documents be apostilled in accordance with the provisions of the Hague Convention. It is clarified that certification is very different from accreditation, which requires a reputable source to validate the content of the documentation. Within the KYC process, certified documentation is not expected to carry an accreditation.

10.7.Independent reputable sources

The independent reputable sources that may provide original documents or certify that the documents are true copies are as follows:

- A regulated financial institution in the United States or an authorised country, provided that the person holds a relevant position (compliance, legal, secretarial, operations);
- An independent solicitor, whose identity can be verified by the Client Onboarding Unit through publicly available sources (membership of a professional body or other standard existence checks);
- An independent audit firm, whose identity can be verified by the Account Management / Client Onboarding Unit through publicly available sources (membership of a professional body or other standard existence checks);
- A notary public;
- The embassy or consulate of the client's country of origin in the United States;
- The US embassy in the client's place of residence;
- The police or a similar authority;
- Any full-time employee of FINANCREDITS BNK;
- Regulated administrators in Canada or an approved country;
- Any officially authorised national or regional commercial register existing in the United States or in an authorised country.

10.8.Reliable sources

The company only recognises electronic information from reliable electronic sources. The following are considered reliable electronic sources of information:

- Online information from any officially authorised commercial register;
- Online information from any website of a regulator in the United States or an approved country;
- Websites of the client or its parent company confirming the nature of subsidiary or branch relationships;
- Annual reports, corporate governance reports and audited financial statements downloaded from clients' websites;
- Services from authorised providers, for example, Worldcheck, Webshield, LexisNexis, etc.
- Online information from recognised news agencies, for example, Bloomberg, Reuters, Factiva, FT.

10.9. Timing of customer due diligence

FINANCREDITS BNK will ensure that appropriate customer due diligence (CDD) is carried out, or has been carried out, when:

- it transfers existing customers to the company or acquires a portfolio of existing customers from a third party, including other affiliated companies;
- it intends to establish a business relationship with a new customer;
- it has doubts about the accuracy or suitability of the CDD documents, data or information it has obtained, for example, where there is a substantial change in the way the account is operated that is inconsistent with the customer's business profile, or where it appears that the customer is not the actual customer;

- suspects money laundering or terrorist financing;
- there is a change in the customer's risk rating, or where a change in the customer's circumstances warrants it.

Generally, CDD must be completed before any business relationship is formalised, for example, by signing a contract with the client or accepting the terms and conditions.

However, in exceptional circumstances, and subject to the approval of the AMLCO and the CEO/MD, CDD may be completed after that point if:

- the postponement of customer or beneficial owner verification is necessary to avoid disrupting the normal course of a business relationship in order to execute an urgent transaction, the non-execution of which would cause or could cause a financial loss to the customer due to price fluctuations or the loss of opportunities;
- there is a low risk of money laundering occurring and the firm can effectively manage any identified risk of this nature;
- the verification is completed as soon as reasonably practicable and, depending on the nature of the relationship with the customer, ideally within a period not exceeding 30 days.
- Where the Firm is unable to reasonably comply with the 30-day rule mentioned above, it must, before the end of the 30-day period, document the reason for its non-compliance, complete the verification as soon as possible and record the instance of non-compliance in its Annual Anti-Money Laundering Report. Please note that FINCEN may specify a timeframe within which the verification must be completed. If the CDD is not completed within this timeframe, FINCEN may order the Company to cease any business relationship with the Customer.
- In light of the above, the Company's policy is not to enter into a business relationship with any Customer until the CDD has been completed.

10.10. Failure to comply with the customer due diligence obligation

If, during the course of the business relationship, a Client fails to provide or refuses to provide, within a reasonable timeframe, the required data and verification information, the Company may terminate the business relationship and close all the client's accounts. It may also be appropriate for the Company not to carry out a Transaction until the CDD has been completed. Where it is not possible to carry out the CDD or a substantial part thereof, such as the identification and verification of a Beneficial Owner, the business relationship with that Customer shall not be established.

If FINANCREDITS BNK is unable to carry out or complete the CDD, it shall apply one or more of the following measures, as appropriate in the circumstances:

i. not open an account or provide a service;
ii. not otherwise establish a business relationship or carry out a transaction;
iii. without prejudice to the foregoing, terminate or suspend any existing business relationship with the Customer;
iv. assess whether the circumstances require the submission of a Suspicious Activity Report (SAR) to FINCEN.

In the case of a new customer, it may be appropriate to terminate the business relationship before a product or service is provided. However, in the case of an existing customer, whilst termination of the business relationship should not be ruled out, suspension may be more appropriate depending on the circumstances. In any event, the company must take care not to alert the customer.

FINANCREDITS BNK is not obliged to terminate or suspend any existing business relationship with a customer if:

- doing so would amount to 'alerting' the customer; or
- FINCEN instructs the company to act otherwise.

10.11. Prohibition on cooperating with or maintaining anonymous accounts

The Company is prohibited from opening or maintaining anonymous or numbered accounts, or accounts in the name of persons other than those appearing on official identity documents. The Company must pay particular attention to any threat or risk of money laundering or terrorist financing that may arise from products or transactions that facilitate anonymity, and must take measures, if necessary, to prevent their use in such activities.

10.12. Ongoing customer relationship monitoring

When carrying out ongoing CDD, FINANCREDITS BNK must focus on all customers, particularly those assigned a higher risk category, and using this risk-based approach:

i. monitor customers' transactions to ensure they are consistent with the firm's knowledge of the customer, their business and their risk rating;
ii. pay particular attention to any complex or unusually large transactions, or to unusual patterns of transactions that have no apparent or visible economic or legitimate purpose;
iii. investigate the background and purpose of transactions;
iv. periodically review the adequacy of the customer due diligence (CDD) information held on customers and beneficial owners to ensure that the information remains up to date, particularly in the case of customers with a higher risk rating;
v. periodically review the risk assessment of each customer to ensure that their risk rating remains appropriate in light of current money laundering risks.

When monitoring the customer relationship, FINANCREDITS BNK will carry out a periodic review to ensure that the customer's identity documentation, such as passport number and address and, in the case of a legal entity, its share register or list of partners, etc., is accurate and up to date.

In particular, such reviews shall be carried out when:

- FINANCREDITS BNK amends its CDD documentation requirements;
- an unusual transaction with the Customer is anticipated (including, where necessary, the source of funds) to ensure that transactions are consistent with the Customer's profile and business model;
- there is a substantial change in the Customer's legal status and circumstances, such as a change in:
- Directors/secretary;
- Registered shareholders and/or beneficial owners;
- registered office;
- Trustees;
- corporate name and/or trading name;
- Principal business partners and/or undertaking new significant business activities. The extent of ongoing CDD to be carried out will depend on the Customer's risk assessment.

To monitor customer transactions, FINANCREDITS BNK will use automated procedures or systems, or a combination of both, depending, amongst other things, on the size and nature of the company's business and the complexity and volume of the transactions.
FINANCREDITS BNK will also review its customers, their businesses and transactions against the UN Security Council sanctions lists and any other sanctions lists that may be relevant, both during this regular review process and at the time a new sanction is issued.

11. Monitoring and reporting of suspicious activities

11.1.Summary

FINANCREDITS BNK maintains:

1. policies, procedures, systems and controls designed to monitor and detect suspicious activities or transactions related to possible cases of money laundering or terrorist financing; and
2. an anti-money laundering training and awareness programme that enables employees to recognise when they have reasonable grounds to suspect that an act of money laundering or terrorist financing is taking place, as well as the means by which they should report such suspicions.

11.2. Examples of suspicious activities

Money laundering or terrorist financing operations can take many forms: there is no single set of circumstances or pattern of behaviour that allows them to be recognised. The key to recognising a suspicious activity is knowing enough about the customer and their expected normal activities to recognise when their activity is abnormal.

By way of example, circumstances that could give rise to reasonable grounds for suspicion at the customer onboarding stage might include those in which the customer:

- refuses, without a reasonable explanation, to provide the requested information; and/or
- makes extensive use of overseas accounts, companies or structures in circumstances where their financial needs do not justify such arrangements.
- Subsequently, during the course of a business relationship with a customer, circumstances that could give rise to reasonable grounds for suspicion might include:
- Transactions that do not correspond to the information provided during the onboarding phase, or ‘ ’ that lack an apparent purpose, have no obvious economic rationale, or are designed or structured to evade detection;
- Transactions requested by a person without a reasonable explanation, which fall outside the usual scope of the services normally requested or which are outside the company’s experience in relation to that particular customer;
- Transactions of a volume or pattern which, without a reasonable explanation, do not fit with previous experience or are deliberately structured to avoid detection;
- The customer uses the relationship for a single transaction or only for a very short period of time;
- The unnecessary channelling of funds through third-party accounts, if this comes to the Company’s attention;
- Unusual transactions without an apparent profit motive.

11.3. Obligation to carry out further investigations

- A transaction that appears unusual is not necessarily suspicious. Even clients with a stable and predictable transaction profile may periodically carry out transactions that are unusual for them. Clients may, for perfectly valid reasons, have an erratic pattern of transactions or account activity. Therefore, the unusual nature of a transaction is, in the first instance, merely a basis for further investigation, which in turn may require a judgement as to whether it is suspicious. A transaction or activity may not be suspicious at that time, but if suspicions arise later, a reporting obligation then arises.
- If you have reasonable grounds for suspicion, you must not ignore a potentially valid suspicion through wilful blindness, negligence (i.e. deliberately and recklessly failing to carry out appropriate enquiries) or by failing to properly assess the facts and information that are presented or available.

11.4. Obligation to report

Any employee who knows or suspects, or who has reasonable grounds to know or suspect, that a person is involved in money laundering has a personal obligation to submit a Suspicious Activity Report (SAR) to the Anti-Money Laundering Compliance Officer (AMLCO). This obligation applies even in situations where no business relationship has been established, if the circumstances were suspicious.

Knowledge refers to actual knowledge supported by tangible information or evidence; it implies concrete knowledge, such as that obtained when a person admits to being involved in a specific criminal activity, for example, tax evasion. Suspicion, on the other hand, is formed without concrete evidence or information to support it; it is based on objective reasoning. Suspicion must be more than mere speculation and must be based on some basis that a case of money laundering has occurred or is about

to occur. Bear in mind, however, that an employee who considers a transaction to be suspicious is not expected to know the exact nature of the offence or that the funds in question definitely originate from money laundering or terrorist financing.
The requirements mentioned above do not prevent an employee from consulting with their immediate supervisor or other employees to decide whether the circumstances warrant the submission of a Suspicious Transaction Report (STR) to the Anti-Money Laundering Compliance Officer (AMLCO). However, despite such consultation, the employee must decide for themselves whether the AMLCO should be notified and must not be prevented or discouraged from doing so if they know, suspect or have reasonable grounds to know or suspect that a person may be involved in money laundering.
Employees are also reminded that failure to comply with the obligation to file a Suspicious Activity Report (SAR) may result in disciplinary action by the company against the employee. Although all external Suspicious Activity Reports (SARs) must be filed solely by the Anti-Money Laundering Officer (AMLCO) or their deputy, the company's policy states that no action will be taken against any employee who discloses information relating to money laundering to FINCEN or any other relevant body involved in the prevention of money laundering, including FINCEN.

11.5. Reporting procedures

- Any knowledge, suspicion or reasonable grounds to know or suspect that a person is attempting to commit money laundering or terrorist financing must be reported to the AMLCO. This must cover not only suspicious transactions that have taken place, but also attempted suspicious transactions and any type of suspicious activity or behaviour, including the actions of customers or potential customers.
- Initially, the employee may report informally, by telephone or in person; however, they must subsequently submit an ISR, which must be dated and signed.
- The ISR provides documentary evidence that the employee has fulfilled their personal obligation to report suspicious circumstances and creates a permanent record of what those circumstances were.
- The compliance department encourages company employees to contact the company's AMLCO, either in person or by email, to report or discuss suspicious activities.

11.6. Investigation by the AMLCO

- Upon receiving an ISR, the AMLCO shall immediately:
- investigate and document the circumstances in relation to which the report was filed;
- determine whether, in accordance with the Act, a corresponding Suspicious Activity Report (SAR) must be filed with FINCEN and document that determination;
- if necessary, file an external Suspicious Activity Report (SAR) with FINCEN as soon as possible; and
- immediately notify FINCEN that such a report has been filed.
- If no external SAR is filed, the AMLCO must record their reasons for not doing so.

- Please note that the decision as to whether or not to file an external Suspicious Activity Report (SAR) rests solely with the Anti-Money Laundering Compliance Officer (AMLCO) and is not subject to the consent or approval of any other person.
- If the Firm knows or suspects that the funds subject to the report do not belong to a Client but to a third party, the AMLCO must include this fact, as well as details of the additional measures the Firm proposes to take in relation to the case, in the report.

11.7. Submission of reports to FINCEN

- In accordance with the relevant provisions of the law, any employee of a financial institution who knows or suspects that a transaction is related to money laundering or terrorist financing must report their suspicions to FINCEN via the compliance officer.
- All reports from the compliance officer (or AMLCO) must be submitted online.

- Following the submission of a SAR, the company may subsequently wish to terminate its relationship with the customer in question for risk prevention reasons. In such a case, and as required by the Act, the company acts with particular caution so as not to alert the customer in question that a suspicious activity report has been submitted to FINCEN. Therefore, close cooperation is maintained with FINCEN so as not to hinder ongoing investigations.
- Cooperation with FINCEN following the reporting of suspicious transactions or activities:
- Following the submission of the AMLCO's report to FINCEN, the accounts involved and any other related accounts will be closely monitored by the AMLCO. Following FINCEN's instructions, the AMLCO will thoroughly investigate all transactions on the accounts.
- The Company shall comply with all instructions issued by FINCEN. FINCEN may order the Company to refrain from executing or to delay the execution of a Client's transaction, without such action constituting a breach of any contractual or other obligation on the part of the Company and its Employees.
- The AMLCO shall act as the first point of contact with FINCEN, both at the outset and during an investigation.
- A large cash transaction report must be filed with FINCEN when a reporting entity receives $10,000 or more in cash in the course of a single transaction, or when it receives two or more cash amounts totalling $10,000 or more, made within 24 consecutive hours by or on behalf of the same person or entity.
- An electronic funds transfer report must be filed with FINCEN when transmitting instructions for the transfer of $10,000 or more out of or into the United States in a single transaction; or in two or more transactions totalling $10,000 or more made within 24 consecutive hours by or on behalf of the same person or entity, via any electronic, magnetic or optical device, telephone apparatus or computer.

11.8. Prohibition on 'tipping off'

- Informing any person that they are under scrutiny, or that a competent authority is investigating their possible involvement in suspicious activities related to money laundering, constitutes an offence under the Act. Employees must therefore be sensitive to these issues when considering CDD measures and take all reasonable precautions to avoid 'alerting' the person.
- Consequently, if the Company reasonably believes that the application of CDD measures will alert a Client or a potential client, it may choose not to proceed with that process and must file an external SAR instead.
- Persons carrying out financial or other activities are, in accordance with internal reporting procedures, obliged to avoid carrying out any transaction which they know or suspect may be related to money laundering or terrorist financing activities, before such suspicion is reported to FINCEN, as appropriate.

- However, if it is impossible to prevent the transaction from taking place, or if doing so could prejudice any investigation or prosecution of the persons for whose benefit the alleged money laundering or terrorist financing activities are being carried out, FINCEN shall be informed after the transaction in question has taken place.

12. Imposition of sanctions and other conclusions

12.1. Relevant rulings and sanctions

FINANCREDITS BNK must exercise due diligence to ensure that it does not provide services (or conduct business of any other kind) to any person involved in money laundering, terrorist financing, proliferation financing or the financing of weapons of mass destruction.
Therefore, FINANCREDITS BNK shall obtain and make appropriate use of the relevant resolutions or sanctions issued by:

• Official website of the United States Government;
• The Official Journal of the European Union;
• The US Department of the Treasury, Office of Foreign Assets Control (OFAC); and
• The United Nations Security Council.

FINANCREDITS BNK will immediately notify FINCEN as soon as it becomes aware that it is:

i. is carrying out or is about to carry out an activity;
ii. holding or about to hold money or other assets; or
iii. is carrying out or is about to carry out any other business, whether derived from or related to (i) or (ii) above, for or on behalf of a person in contravention of a relevant sanction or resolution issued by the Official Journal of the European Union, OFAC or the United Nations Security Council.

AMLCO shall ensure that any notification sent to FINCEN in accordance with the Act includes details of the activity in question and of the measures taken or which FINANCREDITS BNK proposes to take in respect of the matters specified in the notification.

12.2. Government, regulatory and international conclusions

FINANCREDITS BNK shall obtain and make appropriate use of (including conducting additional due diligence on, or refraining from carrying out a Transaction for or on behalf of, any person who is the subject of) any findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions issued by:

• the United States Government;
• the US Federal Reserve;
• FINCEN;
• the FATF;
• any other organisation or agency it deems appropriate (such as OFAC). In relation to:

1. measures taken to prevent money laundering, terrorist financing, proliferation financing or the financing of weapons of mass destruction in a specific country or jurisdiction, including any assessment of substantial deficiencies in the adoption of international standards by the relevant countries; and
2. the names of persons, groups, organisations or entities, or any other body suspected of money laundering, terrorist financing or the financing of weapons of mass destruction.

FINNACREDITS BNK will examine and pay particular attention to any transaction or business relationship with persons located in such countries or jurisdictions (including countries or jurisdictions that are no longer identified as deficient or that have been exempted from special scrutiny) and will ensure that it is aware of the background on which the assessments or specific recommendations have been made.

12.3. Obtaining and using sanctions and other findings

FINANCREDITS BNK will collect and make appropriate use of available national and international information (including conducting more thorough due diligence on any person subject to such information, or refraining from carrying out a transaction for or on behalf of such a person), including lists of suspects such as those provided by the Office of Foreign Assets Control (OFAC) of the US Department of the Treasury, , as well as information obtained from Dow Jones and other reliable sources, such as subscriber lists obtained directly from government agencies, to carry out initial and ongoing checks on its Clients and their Transactions.

The firm shall also maintain a list of prohibited and high-risk countries and jurisdictions (as set out in Appendix 7) referred to above and shall use World-Check and other appropriate sources to identify any person of the type mentioned in that list.

The sources mentioned above shall be consulted during the customer onboarding stage and, subsequently, as appropriate, as part of ongoing customer monitoring. If an apparent match is found, the AMLCO must be notified immediately to receive guidance on how to proceed.

In relation to the above, FINANCREDITS BNK will continue to pay particular attention to transactions with customers located in countries or jurisdictions that are no longer identified as deficient or that have been exempted from special scrutiny.

13. Training and awareness-raising on money laundering prevention

FINANCREDITS BNK's policy is to provide training on the prevention of money laundering to all relevant employees as soon as reasonably practicable after they join the company and, thereafter, at least once a year. Relevant employees include the Board of Directors, operational staff, any employee who has contact with customers, and any other employee who may encounter money laundering situations in the course of their duties.

The training programme aims to educate employees on the latest developments in the prevention of money laundering and terrorist financing, including the practical methods used for this purpose. It is structured differently for new employees, existing employees and the various departments of the company, in accordance with the services they provide. The AMLCO maintains a record of all training provided to employees.

The format, content and objectives of the AML training programme will be overseen by the AMLCO and will specifically address the key topics and objectives set out below.

13.1. Key topics and objectives

- AMLCO will ensure that FINANCREDITS BNK's AML training:
- is appropriately tailored to the company's activities, including its products, services, customers, distribution channels, business partners and the level and complexity of transactions;
- covers the Company's anti-money laundering policies, procedures, systems and controls;
- covers the types of activities that may constitute suspicious activities in the context of the business in which an employee is involved and which may justify the submission of a Suspicious Transaction Report (STR) to the Anti-Money Laundering Compliance Officer (AMLCO);
- recognise and manage transactions and activities, including how to gather and assess the information necessary to determine whether a person is involved in suspicious activities that may be related to money laundering or terrorist financing;
- understand the company's procedures for submitting an ISR to the AMLCO;
- be aware of the prevailing money laundering techniques, methods and trends relevant to the company's business;

- understand the roles and responsibilities of employees in the fight against money laundering, such as the identity and responsibilities of the AMLCO and the Deputy AMLCO;
- understand the findings, recommendations, guidance, directives, resolutions, sanctions, notices or other relevant conclusions issued by government, regulatory and international bodies.
- It is recommended that the training includes:
    i. the relevant anti-money laundering legislation in force in Canada;
    ii. the guidance policy issued by FINCEN in relation to anti-money laundering legislation; and
    iii. ministerial directives concerning the prevention of the use of the financial system for the legalisation of the proceeds of money laundering or terrorist financing.
- To achieve this objective, a copy of this procedure is distributed to all relevant employees
- All new employees will receive initial compliance training and will be informed about the AMLCO.

13.2. Employee obligations

- Employees may be held personally liable for failing to report information or suspicions relating to money laundering or terrorist financing.

- Employees must cooperate and report, without delay, anything that comes to their attention regarding transactions suspected of being related to money laundering or terrorist financing.
- Employees fulfil their legal obligation to report their suspicions regarding money laundering and terrorist financing by submitting the ISR to the AMLCO.

14. Systems in use

14.1. Continuous monitoring systems

This is a review to determine whether the amount of contingent risk exceeds the approved amount. In addition, the following must also be carried out:

- WorldCheck: This is carried out for existing customers and in the event of changes to: the company's structure, directors or shareholders, as well as at appropriate times. The company will subscribe to a new WorldCheck service, whereby, upon uploading client names, automatic alerts will be received from WorldCheck whenever a match is found. WorldCheck will verify and update its lists, including the OFAC list, on a daily basis.
- Annual website review procedure for all declared URLs:
- In accordance with the rules of the credit card associations;
- Content review.
- PCI DSS review: Where applicable, verification of current customers' PCI DSS documentation (SAQ, network scan and certificate).
- Keeping up to date with PCI DSS standards and regulations: Obtaining updated corporate documentation/identifiers: In accordance with changes to corporate structure; changes in directors/shareholders; additional activities/URLs of existing clients.

15. Record retention

The following client-related records must be retained for a period of five years:

- Proof of customer identification.
- Evidence and details of the business relationship or transactions, including accounting entries, relevant correspondence with customers and other persons with whom the company maintains a business relationship.
- The five-year period is calculated from the date of the transactions or the end of the business relationship. Details of all clients are recorded on a prescribed form which is kept in the client's file together with all other documents, as well as all internal records of meetings with the respective client. The form is updated periodically or whenever new information relevant to the client's financial profile arises:
- As regards the customer's account opening documentation, a copy or references to the required evidence are retained for at least five years after the business relationship with the customer in question has ended.
- In the case of business relationships and transactions, the supporting evidence and records, consisting of original documents or copies admissible in court proceedings under applicable national law, are retained for a period of at least five years following the completion of the transaction or the end of the business relationship.

15.1. Retention of document/data records

FINANCREDITS BNK shall retain sufficient information to maintain an audit trail, so that any transaction can be reconstructed and reviewed and, if necessary, evidence can be provided for criminal proceedings.

The company retains records of the following documents and data:

- Evidence of the customer's identity.
- Relevant evidence and details of all business relationships and transactions, including documents for recording transactions in the accounting books;

- Transaction amounts and currency;
- Relevant documents relating to correspondence with customers and other persons with whom they have a business relationship;
- An assessment of the systems and procedures applied by a third party relied upon by the Company for the purposes of customer identification and due diligence.
- The company guarantees that all the documents mentioned above will be made available to FINCEN and the competent supervisory authorities promptly and without delay, so that they may fulfil their legal obligations.

15.2. Retention period for documents/data

- The documents and data mentioned above are retained for a minimum period of five years, calculated from the execution of the transactions or the termination of the business relationship.
- Documents/data relevant to ongoing investigations are retained until FINCEN confirms that the investigation has been concluded and the case has been closed.

15.3.Format of records

- The retention of documents/data, with the exception of original documents or certified copies thereof which are retained in hard copy, may be carried out in other formats, provided that the Company is able to retrieve the relevant documents/data without undue delay and submit them to FINCEN or the competent authority upon request.
- All correspondence with customers, including relevant files, is stored in the company's email system and in secure folders.

15.4. Client transaction data

In relation to client transactions, the Company retains the following information:

- Executed/completed transactions: o Client name/code;
- Transaction reference identifier (unique identification code);
- Amount of the payment transaction;
- Amount of the payment transaction charges payable by the payee; and
- Value date and time of execution.
- Rejected payment orders:
- Customer name/code;
- Reference identifier (unique identification code) of the order;
- Amount of the payment order;
- Date and time of receipt of the payment order; and
- Reason for refusal or rejection.
- Relevant correspondence with customers:
- Emails/faxes or other correspondence with customers;
- Customer complaints; and
- Confirmations sent to customers.

16. Termination of the business relationship with Clients

The Company may terminate the business relationship with the Customer, or vice versa, at any time with 30 days' notice by written notification to the other party. Without prejudice to the foregoing, the Company may immediately suspend all or part of the services or terminate the business relationship, upon written notification (by fax, post or email), at the Company's sole discretion, if:

- The Customer breaches the 'Service Agreement' or the 'Terms and Conditions' or any other agreement to which the Customer and the Company are parties.
- The Company suspects or reasonably believes that the Customer is using the services in connection with unauthorised, dishonest or criminal activities, or fraud.

- The Customer is unable to pay its debts as they fall due or is declared bankrupt or insolvent, or has a receiver, a receiver, a provisional liquidator, a liquidator or an administrator in respect of any substantial part of their assets, or is subject to enforcement proceedings in respect of any of their assets, or if an application for winding-up is made and such application is not withdrawn, satisfied or dismissed within 30 days, or if the Customer suffers or is subject to any event, circumstance or procedure equivalent to those set out above in any other jurisdiction.
- The Company is required to do so by any regulatory authority or agency or pursuant to the applicable rules or laws.
- If anything occurs to the Client or comes to the Company's attention in relation to the Client, or arising from or incidental to the Client's business or the conduct of the Client's business (including business practices or individual activity), which the Company, in its sole discretion, considers: (i) disgraceful or capable of damaging the reputation of the Acquiring Banks, the APMs or the Company; (ii) detrimental to the business of the Acquiring Banks, the APMs or the Company; or (iii) likely to give rise to or resulting in fraud or any other criminal activity, or suspicion of fraud or any other criminal activity.
- Any circumstance, event or series of events in respect of which the Company has reasonable grounds to believe that they materially and adversely affect or may affect the Customer's ability to fulfil, in full and on time, one or more of its obligations, or its liabilities or potential liabilities under the 'Service Agreement' or the 'Commercial Terms'; such circumstances and events may include: (i) a substantial change in the goods and/or services supplied by the Client; (ii) substantial fluctuations, whether positive or negative, from month to month in the Client's transaction volumes or in the average value of transactions; (iii) the imposition of levies; (iv) a change of control in relation to the Client; (v) instructions from a regulatory authority which the Client does not comply with, is unable to comply with or is unwilling to comply with; and/or (vi) a substantial deterioration in the Client's earnings or financial or commercial position.
- In the event of expiry or termination for any reason of the agreement between the Company and the respective Acquiring Banks, the APMPs relating to the provision of the Services.
- In the event of the Client's death (where the Client is a natural person).

Appendices

Annex 1 – Internal Suspicion Report

INTERNAL REPORT OF SUSPICION OF MONEY LAUNDERING			
REPORTER			
Name:			
Tel.:			
Department:		Fax:	
Position:			
Email:			
Customer details			
Name:			
Address:			
Date of birth:			
Contact details/Telephone/Fax/Email:			
Occupation/Employer:			
Employer details:			
Passport number:			
Nationality:			
Country of residence:			
ID number:			
Other ID:			
Account details:			
Linked accounts:			
Products/services:			
Risk rating:			
Information/Suspicion			
Brief description of activities/transactions:			
Reason(s) for suspicion (provide as much detail as possible; use another sheet if necessary)			
Signature of the reporting person:		Date:	
For use by anti-money laundering officers			
Date received:		Time of receipt:	
		Notified to FINCEN	

Appendix 2 – Internal Assessment Report

INTERNAL ASSESSMENT REPORT OF THE ANTI-MONEY LAUNDERING COORDINATION UNIT

Reference:

Client:

Reporter:

Branch/Department:

INVESTIGATIONS CARRIED OUT (Brief description)

DOCUMENTS CONSULTED/ATTACHED

FINDING/DECISION

FILE REFERENCE:

MONEY LAUNDERING

SIGNATURE

DATE

Appendix 3 – Report to FINCEN.

The report will be prepared manually online via FINCEN's web application known as the 'FINCEN Electronic Reporting System'. FINANCREDITS BNK, the AMLCO, is registered on the system.

The system allows draft reports to be saved and offers other features to assist compliance officers in preparing the report. The system also allows relevant documents to be attached to the report. This option is more time-consuming, as all relevant fields must be completed manually within the system.

The alternative method for submitting reports involves using an XML file containing all the relevant information relating to that report. Once completed, the AMLCO will upload this file to the system. The method used will depend on the number of reports the company submits to FINCEN each year.

The AMLCO ensures that, in the event of an investigation into suspicious activity by FINCEN, it can provide the following information without delay:

i. the identity of the account holder(s);
ii. the identity of the account's beneficial owners;
iii. the identity of the persons authorised to manage the account;
iv. details of the volume of funds or the level of transactions passing through the account;
v. linked accounts; and
vi. in relation to specific transactions:

- the source of the funds;
- the type and amount of currency used in the transaction;
- the manner in which the funds were deposited or withdrawn (e.g. cash, cheques, bank transfers);
- the identity of the person who gave the instruction for the transaction;
- the destination of the funds;
- the form of the instructions and authorisation given; and
- the type and identification number of any account involved in the transaction

Appendix 4 – Examples of suspicious transactions and activities related to money laundering and terrorist financing

MONEY LAUNDERING

1. Transactions via bank accounts:

- The use of accounts in the name of trustees, nominees or client accounts for no apparent reason or in a manner inconsistent with the account holder's activities.
- Demanding the return of funds on the grounds that they were sent in error.
- Carrying out multiple transactions on the same day at the same bank branch, but with an apparent attempt to use different tellers.
- Any natural or legal person whose account shows virtually no normal personal or business banking activity, but which is used to receive or transfer large sums of money without an obvious purpose or connection to the account holder and/or their business (for example, a substantial increase in the volume of transactions in an account).
- Customers who appear to hold accounts at several banks within the same locality, particularly where the bank is aware of a regular process of consolidating such accounts prior to a request to transfer the funds.
- Accounts that receive significant periodic deposits and remain inactive at other times.
- Increased use of safe deposit boxes by private individuals. Use of sealed packages deposited and withdrawn.
- Company representatives who avoid contact with the branch.
- Customers who refuse to provide information which, under normal circumstances, would make them eligible for credit or other banking services that would be considered valuable.
- A large number of people making payments to the same account without a proper explanation.
- An account where several people have signing authority, but these people appear to have no relationship with one another (whether family or business).

2. Transactions relating to investments:

- Purchase of securities that the bank will hold in custody, where this does not appear appropriate given the customer's apparent circumstances.
- Requests from customers for investment management services (whether in foreign exchange or securities) where the source of the funds is unclear or does not match the customer's apparent circumstances.
- The purchase and sale of a security without a discernible purpose or in circumstances that appear unusual.

3. Electronic transfer/international activity:

- The bank acts as an intermediary for the transfer of funds from a bank outside the United States to another bank also outside the United States, without having direct knowledge of the originator and/or the beneficiary of those funds. The transfer is not in favour of a customer of the intermediary bank or of any other bank operating in the United States.
- Use of letters of credit and other methods of trade finance to move money between countries where such trade is inconsistent with the customer's usual business.

- Customers making regular, high-value payments, including bank transfers, which cannot be clearly identified as legitimate transactions, or who receive regular, high-value payments from countries typically associated with the production, processing or trafficking of drugs.
- Accumulation of large balances, which are inconsistent with the known turnover of the customer's business, and subsequent transfer to accounts held abroad.
- Unexplained transfers of funds made by customers, whether incoming, outgoing or without passing through an account.
- Numerous electronic transfers received into an account where each transfer falls below the reporting threshold in the sending country.
- Wire transfer activity to or from a high-risk jurisdiction without an apparent commercial reason, or where it is inconsistent with the customer's business or history.
- Funds originating from companies operating in high-risk jurisdictions, for example, jurisdictions that do not implement or inadequately implement the FATF recommendations against money laundering and terrorist financing.
- Wire transfers to or from a natural person where information regarding the payer or the person on whose behalf the transaction is being carried out is not provided alongside the transfer.
- A large number of small-value electronic fund transfers received, which are almost immediately, in full or in the main, sent to a country in a manner inconsistent with the customer's business profile or history.
- Large incoming electronic transfers on behalf of a foreign customer with no explicit reason or with a very flimsy one.
- Electronic transfer activity that is unexplained, repetitive or exhibits unusual patterns. Payments or receipts with no apparent links to legitimate contracts, goods or services.

4. Correspondent accounts:

- Large-value electronic transfers, where the correspondent account has not previously been used for similar transfers.
- The routing of transactions involving a correspondent bank through various jurisdictions and/or financial institutions before or after they reach the bank, with no apparent purpose other than to conceal the nature, source, ownership or control of the funds.
- Frequent or numerous electronic transfers, whether to or from the correspondent account of a respondent bank, originating in or destined for a jurisdiction that does not apply, or applies inadequately, the FATF recommendations on the prevention of money laundering.

5. Secured and unsecured loans:

- Requests from a customer for a bank to provide or arrange financing where the source of the customer's financial contribution to a transaction is unclear, particularly where real estate is involved.

6. Customers providing insufficient or suspicious information:

- A customer is reluctant to provide complete information when opening an account regarding the nature and purpose of their business, the intended activity of the account, previous banking relationships, the names of their officers and directors, or information on the location of their business. They generally provide minimal or misleading information that is difficult or costly for the bank to verify.

- A customer provides unusual or suspicious identification documents that cannot be easily verified.
- The customer's home or business telephone number is disconnected.
- A customer carries out frequent or large-value transactions and has no record of past or present employment.

7. Activity inconsistent with the customer's business profile:

- The transaction appears to be inconsistent with the normal type of transactions for the particular sector.
- A transaction that is unnecessarily complex given its business purpose.
- The customer's activities are inconsistent with those declared.
- The types of transactions show an unexpected change that does not align with the customer's usual operations.
- Ship-owning and ship-managing companies carrying out transactions or activities unrelated to the shipping business.

8. Characteristics of the customer or their business activity:

- With regard to non-profit or charitable organisations, payment transactions for which there appears to be no logical economic purpose or where there appears to be no link between the organisation's stated activity and the other parties to the transaction.
- A safe deposit box is opened in the name of a business entity when the customer's business activity is unknown or does not appear to justify the use of a safe deposit box.
- Unexplained inconsistencies arising from the customer identification or verification process (for example, in relation to the previous or current country of residence, the country of issue of the passport, the countries visited according to the passport, and the documents presented to confirm the name, address and date of birth).

9. Transactions by employees, agents or trustees:

- Changes in employees' lifestyle, for example, a lavish lifestyle or avoiding being away from the office due to holidays.
- Changes in employees' performance or behaviour.
- Customers who wish to be served by the same bank employee at all times, including for routine transactions, or who cease to conduct business with the bank when a specific employee is absent.
- Complex network of trusts or nominees.
- Transactions or business structures that are set up or operate in an unnecessarily commercial manner.
- For example, companies with bearer shares or bearer derivatives, or the use of a postcode.
- The trustee's unwillingness to retain the necessary information or exercise the necessary controls in the proper performance of their duties.
- The use of trust documents in a manner that restricts the control exercised by the company's Board of Directors.
- Customers using accounts in the name of trustees instead of their own bank accounts.

TERRORIST FINANCING

1. Sources and methods:

The financing of terrorist organisations stems from both legal and illegal revenue-generating activities. Criminal activities that generate such revenue include kidnapping (requiring a ransom), extortion (demanding money in exchange for protection), smuggling, theft, robbery and drug trafficking. Legal fundraising methods used by terrorist groups include:

- Collection of membership fees and/or subscriptions;
- The sale of books and other publications;
- Cultural and social events;
- Donations;
- Appeals to the community and fundraising campaigns; and
- Funds obtained from illegal sources are laundered by terrorist groups using the same methods as criminal groups. These include the smuggling of cash by couriers or shipments of large amounts of cash, structured deposits or withdrawals from bank accounts, purchases of monetary instruments (traveller's cheques, bank cheques, postal orders), use of credit and debit cards, electronic transfers using 'front men', false identities, front companies and fictitious entities, as well as individuals designated from among their close relatives, friends and associates.

2. Non-profit organisations:

Terrorist groups also use non-profit and charitable organisations as a means of raising funds and/or as a cover for transferring funds in support of terrorist acts. The potential misuse of non-profit and charitable organisations can take the following forms:

Establishment of a non-profit organisation with a stated charitable purpose, but which in reality exists solely to channel funds to a terrorist organisation.

- A non-profit organisation with a legitimate humanitarian or charitable purpose is infiltrated by terrorists who divert funds raised for an apparently legitimate charitable purpose in order to support a terrorist group.
- The non-profit organisation serves as an intermediary or front for the movement of funds internationally.
- The non-profit organisation provides support functions to the terrorist movement.
- The following are unusual characteristics of non-profit organisations that may indicate they are being used for illicit purposes:
    1. Inconsistencies between the apparent sources and the amount of funds raised or transferred.
    2. A discrepancy between the pattern and volume of financial transactions and the stated purpose and activity of the non-profit organisation.
    3. A sudden increase in the frequency and amounts of financial transactions in a non-profit organisation's account.
    4. The absence of contributions from donors located in the non-profit organisation's country of origin.

Appendix 5 – Additional documents and declarations required in the case of companies with bearer shares

1. Letter signed by the director (whose details we hold) regarding 'Clarifications and undertakings regarding the share capital of Company A' (see Letter 1).
2. Please note that, in the case of companies where the director is also a holder of bearer shares, the letter must also be completed and signed by the company's secretary or registered agent. Where the secretary or registered agent is another legal entity, it must be signed by a director (always a natural person) of the secretary or registered agent.
3. Letter of instructions from Company A to the bank where the bearer shares are deposited (see Letter 2).
4. A letter of confirmation from the bank where the bearer shares are deposited (see Letter 3). It should be noted that, in accordance with the Bank of Canada's Anti-Money Laundering Regulations
5. (November 2004), bearer shares may only be deposited with a bank authorised to do so and operating in the US and EEA countries. EEA countries include: Austria, Belgium, Bulgaria, Canada, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Estonia, Finland, France, Greece, Hungary, Ireland, Iceland, Italy, Latvia, Liechtenstein, Luxembourg, Malta, Norway, the Netherlands, Poland, Portugal, the United Kingdom, the Czech Republic, Romania and Sweden. **Please note that Switzerland is not included in the above list; therefore, the deposit of bearer shares with a Swiss bank will not be accepted.**
6. Notarised copy of the bearer share certificates.

LETTER 1

ON PAPER WITH THE CLIENT'S LETTERHEAD

TO:

FINANCREDITS BNK

DATE DD/MM/YY

For the attention of: Account Management Departments

Clarifications and undertakings regarding the share capital of Company A Limited (the 'Company')

Dear Sirs,

I/we am/are writing to you in my/our capacity as director(s) and/or secretary and/or registered agent of Company A Ltd (hereinafter, the "Company"). This letter is addressed to FINANCREDITS BNK and we acknowledge that the Firm may, at its sole discretion, rely on the contents of this letter to determine whether to enter into or continue a business relationship with the Company.

We wish to confirm to you, in my/our capacity as duly authorised representative(s) of the Company, the following, which, having taken all appropriate measures, we consider to be true and accurate:

1. As at the date of this letter, the Company's total nominal/authorised share capital is USD/EUR, comprising _____ registered ordinary shares of USD/EUR each and/or _____ bearer ordinary shares of USD/EUR each. We enclose updated, relevant and duly certified extracts from the Deed of Incorporation and the Articles of Association of the Company / or from the statement of share capital filed with the Company's national registration authority.

2. That Mr _____, a citizen of with passport number _____, is the owner of _____ of the Company's bearer shares, and Mr _____, a national of _____ with passport number____is the holder of bearer shares in the Company (the 'bearer shareholders'). In total, these comprise all the bearer shares issued by the Company.

3. That, regardless of whether the Bank has notified you of any proposed change, we shall also inform you of such change.

4. That any intention on the part of the Company, the bearer shareholders or myself/ourselves to revoke such instruction must first be communicated to you and that the Bank shall also be obliged to inform you of such intention.

5. That, should you, at your sole discretion, be dissatisfied with the proposed change or with the identity of the proposed new shareholder or shareholders, you are entitled to terminate any business relationship between the Company and you, without any obligation or liability whatsoever to the Company, save for accrued obligations arising solely for the benefit of the former holders of bearer shares of the Company.

6. That, in the event a new class of bearer shares is established for the Company, we shall notify you within 3 working days of the Company's approval of such change.

7. That in the event of a proposal to issue new bearer shares (regardless of class), we shall provide you with a copy of the proposed resolution, which shall detail the persons who will acquire such shares. Furthermore, we shall ensure that the procedures set out in points 1 to 8 above are followed for such new issue of bearer shares.

8. That the holders of bearer shares are at all times aware of the existence of this letter and accept and consent to the disclosures and actions set out in or resulting from this letter.

Yours faithfully

_____

Note: Where the Director is also the holder of bearer shares, this Letter must also be completed and signed by the Company's Secretary or Registered Agent. Where the Secretary or Registered Agent is another Legal Entity, it must be signed by a Director (always a natural person) of the Secretary/Agent

LETTER 2

ON THE CLIENT'S LETTERHEAD

To: Bank

[Address]

DATE DD/MM/YY

Dear Sirs

Company A (hereinafter, the 'Company') intends to establish a business relationship with FINANCREDITS BNK.

Given that the Company's share capital includes bearer shares, which have been deposited by their respective holders, Ms_____and Ms _____ (the 'bearers'), at_____(name of the Bank) (hereinafter, the 'Bank'), we hereby provide you, by virtue of the authorisation granted to us by the Company and the holders of bearer shares, with the following irrevocable instructions:

1. That you shall not deliver or lend the bearer share certificates deposited with your Bank, either to the holders of bearer shares or to any third party, without first informing FINANCREDITS BNK and ourselves, providing us with the full names of the proposed persons to whom the delivery would be made.

2. That you immediately notify FINANCREDITS BNK of any new instructions received from the Company, its directors, the secretary, the owners or any other person with actual or declared authority to represent the Company and its owners, by which it is intended to revoke or limit this irrevocable authorisation issued by us regarding the ongoing disclosure of the aforementioned information to the aforementioned parties, or by which the provision of the service of custody, safekeeping and administration of the bearer share certificates deposited at your institution is terminated, modified or reduced.

3. That you provide FINANCREDITS BNK, at such time as you deem appropriate, including immediately upon receipt of this letter, with the required certifications regarding the bearer share certificates you have deposited with your institution (including details of the owners, the serial numbers of the share certificates and the number of shares per certificate).

We confirm that the holders of the bearer shares agree to the above instruction. Yours faithfully

Director	Secretary or registered agent
Name:	Name:
Company seal:	Position (if the secretary or agent is a legal entity):

LETTER 3

ON BANK LETTERHEAD

To:

FINANCREDITS BNK DATE

DD/MM/YY

For the attention of: Account Management Departments

Dear Sirs

Bearer share certificates of Company A

We refer to an irrevocable instruction received on behalf of and in the name of Company _____ (the 'Company') and its bearer shareholders, and signed by its director, Mr _____ and/or the secretary, Mr _____

The Bank is regulated in the conduct of its business by ……. under licence number… The Bank acts as custodian of the Company's bearer share certificates.

The provision of this service falls within the scope of the Bank's regulated activities.

We hereby confirm the following:

1. The details of the bearer share certificates deposited with our Bank in relation to the Company are as follows: Share certificate serial number Number of bearer shares Holder (name, nationality, passport)
2. The Bank will not deliver or lend the aforementioned bearer share certificates deposited with the Bank, either to the aforementioned owner(s) or to any third party, without first providing such information to FINANCREDITS BNK and the Company, fully informing them of the names of the proposed persons to whom the delivery is to be made.
3. The Bank shall immediately notify you of any new instructions it receives from the Company, its directors, the secretary, the owners or any other person with actual or declared authority to represent the Company and its owners, by which the irrevocable authorisation granted to us regarding the ongoing disclosure of the aforementioned information to you is revoked or intended to be revoked or limited, or by which the provision of the custody, safekeeping and administration service for the aforementioned bearer share certificates is terminated, modified or reduced.
4. The Bank shall provide FINANCREDITS BNK, at such time as it deems appropriate and within a reasonable period, with the required certifications regarding the bearer share certificates that we have deposited with our institution (including details of the owners, the serial numbers of the share certificates and the number of shares per certificate).

5. We confirm that the Bank applies, in accordance with the rules established by our regulatory body, anti-money laundering procedures to all its activities, including the custody, deposit and administration of

financial instruments, such as bearer shares

We also confirm that the Bank will send you all the above information by fax to the number _____, for the attention of your Management Department

For any further clarification, please contact us by telephone on _____, by fax at____or by email at _____

Yours faithfully

_____

Name Position Stamp

Note: This will only be accepted if it has been issued by an authorised bank operating within the EEA. EEA countries include: Austria, Belgium, Bulgaria, Canada, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom. Switzerland is excluded.

Appendix 6 – Additional declaration required in the case of companies with registered shares in circulation, but with a provision in their articles of association allowing them to issue bearer shares or exchange registered shares for bearer shares

ON THE CLIENT'S LETTERHEAD TO: FINANCREDITS BNK DATE:

For the attention of: Account Management Departments Dear Sirs:

Clarifications and undertakings regarding the share capital of Company A Limited (the 'Company')

I/we write to you in my/our capacity as director(s) and/or secretary and/or registered agent of Company A Limited (hereinafter, the "Company"). This letter is addressed to FINANCREDITS BNK and we acknowledge that, at its sole discretion, it will rely on the contents of this letter to determine whether to enter into or continue a business relationship with the Company.

We wish to confirm to you, in my/our capacity as duly authorised representative(s) of the Company, the following, which, having taken all appropriate measures, we consider to be true and accurate:

1) As at the date of this letter, the Company's total authorised share capital is …… USD comprising …….. registered ordinary shares of USD each.

2) Should the issue of bearer shares be proposed, whether new or exchanged for registered shares (regardless of their class), we shall notify you immediately in writing and provide you with a certified copy of the bearer share certificate(s), together with the details of the persons acquiring such shares.

Yours faithfully,

_____ _____

Director Secretary or registered agent:

Company seal: Position (if the secretary or registered agent is a legal entity):

Note: Where the director is also the ultimate beneficial owner, this letter must also be completed and signed by the company's secretary or registered agent. Where the secretary or registered agent is another

Appendix 7 – High-risk and prohibited countries

Sanctioned/prohibited countries: refuse/terminate cooperation

1. Afghanistan
2. Anguilla
3. Antigua and Barbuda
4. Aruba
5. Azores
6. Bahamas
7. Bangladesh
8. Barbados
9. Belarus
10. Belize
11. Bermuda
12. Bhutan
13. Bolivarian Republic of Venezuela
14. Bosnia
15. British Virgin Islands
16. Brunei Darussalam
17. Cayman Islands
18. Chad
19. Commonwealth of Dominica
20. Congo
21. Cook Islands
22. Cuba
23. Curaçao
24. Democratic Republic of the Congo
25. Djibouti
26. Eastern Republic of Uruguay
27. Ecuador
28. Fiji
29. Gaza National Liberation Front
30. Gibraltar
31. Guatemala
32. Guernsey
33. Herzegovina
34. Iran
35. Iraq
36. Isle of Man
37. Jersey
38. Kenya
39. Kingdom of Bahrain
40. Kingdom of Tonga
41. Kosovo
42. Lebanon
43. Liberia
44. Libya
45. Madeira
46. Maldives
47. Marshall Islands
48. Mauritius
49. Mongolia
50. Montserrat
51. Myanmar (Burma)
52. Namibia
53. Nauru
54. Nepal
55. Niue
56. North Korea (Democratic People's Republic of Korea)
57. Pakistan
58. Palau
59. Russia
60. Saint Helena, Ascension and Tristan da Cunha
61. Saint Kitts and Nevis
62. Saint Pierre and Miquelon
63. Samoa
64. Serbia
65. Sierra Leone
66. Sierra Leone
67. Saint Martin (part of the Netherlands)
68. Somalia
69. Sudan
70. Sudan
71. Syria
72. Tahiti
73. Trinidad and Tobago
74. Turks and Caicos Islands
75. United States Virgin Islands
76. Vanuatu
77. Vanuatu
78. Yemen
79. Zimbabwe

High-risk countries: if the customer, the customer's beneficial owner or their representative has links to any of these countries, the customer is considered high-risk.

Note: FINANCREDITS BNK reserves the right to accept or reject any of the countries of operation mentioned above at its reasonable discretion, without giving any reason.

1. Albania
2. Algeria
3. Angola
4. Armenia
5. Azerbaijan
6. Bahrain
7. Benin
8. Burkina Faso
9. Cambodia
10. Colombia
11. Dominican Republic
12. Guinea
13. Guinea-Bissau
14. Haiti
15. Indonesia
16. Israel
17. Jamaica
18. Jordan
19. Kazakhstan
20. Kiribati
21. Kyrgyzstan
22. Laos
23. Macedonia
24. Mali
25. Mexico
26. Morocco
27. Nicaragua
28. Palestine
29. Peru
30. Philippines
31. Puerto Rico
32. Senegal
33. Tajikistan
34. Tonga
35. Turkey
36. Turkmenistan
37. Tuvalu
38. Uganda
39. Ukraine
40. United Arab Emirates
41. Uruguay
42. Uzbekistan

Appendix 8 – Prohibited Activities

The production or trade of any product or activity deemed illegal under the laws or regulations of the host country or under international conventions and agreements, including, but not limited to, the host country's requirements relating to environmental, health and safety, and labour matters.

1. Production or trade in arms and ammunition.
2. Production or trade in alcoholic beverages (including beer and wine).
3. Production or trade in tobacco.
4. Trade in wildlife or wildlife products regulated by CITES.
5. Production or trade in radioactive materials.
6. Commercial logging operations or the purchase of logging equipment for use in primary tropical rainforests.
7. Production or trade in pharmaceutical products subject to international phase-outs or bans.
8. Production or trade in pesticides/herbicides subject to international phase-outs or bans.
9. Drift-net fishing in the marine environment using nets longer than 2.5 km.
10. Production or activities involving harmful or exploitative forms of forced labour or harmful child labour.
11. Production or trade in ozone-depleting substances subject to international phase-out.
12. The production or trade of timber or other forest products from unmanaged forests.
13. The production, trade, storage or transport of large quantities of hazardous chemicals, or the commercial use of hazardous chemicals.
14. Any business related to pornography or prostitution
15. Quarrying, mining or processing of metallic ores or coal
16. Giving or receiving gifts that could be interpreted as an attempt to influence business decisions
17. Misuse of confidential or material information not in the public domain
18. Trade in animal skins, bones and ivory
19. Trade in diamonds without Kimberley Certification
20. Indecent and obscene material, including child pornography
21. Cultural objects such as sculptures, statues, antiques, collectables and archaeological artefacts, particularly those originating from Iraq
22. Trade in fireworks, explosives and nuclear weapons
23. Drug trafficking, including chemicals used to manufacture synthetic drugs or narcotics
24. Ship safety
25. Online dating/adult chat rooms
26. Investments by multiple parties (third parties) without proper authorisation
27. Human body parts and pathogens
28. Gambling/betting/casinos/horse racing/bingo/unlicensed sports betting.
29. Online casinos/online poker/online gambling/unlicensed online betting.
30. Prize draws/gift cards/any form of lottery/unlicensed scratch cards.
31. Bearer shares and bonds.

32. Online service provider (funds from payment gateways or client accounts are not accepted)
33. Unlicensed derivatives/options/hedging/FOREX trading.
34. Currency exchange agent
35. Unlicensed traders in jewellery, gems and precious metals.
36. Cash pooling structure

The above list is not exhaustive and may be subject to periodic changes.
It should be noted that FINANCREDITS BNK reserves the right to accept, reject or refuse any application or commercial activity at its reasonable discretion without giving any reason.

Approved by the Director and the MRLO