CONNEXT

ANTI-MONEY LAUNDERING, TERRORIST FINANCING AND K. Y. C. POLICY & PROCEDURES

CONNEXT LLC

ANTI-MONEY LAUNDERING, TERRORIST FINANCING and K.Y.C. POLICY & PROCEDURES

Connext L.L.C.

VERSION: 1.0.1 – DECEMBER 2022
Effective from 01.01.2023 until Further Notice

Preamble

December 2022- Connext L.L.C. (hereafter referred to as "ConnextFX", "Company", "we", or "our") is a registered company in Saint Vincent and the Grenadines with the company number 2652 LLC 2022, and its registered office is at Richmond Hill Road, P.O. Box 2897, Kingstown, Saint Vincent, and the Grenadines. Following the International Business Companies (Amendment and Consolidation) Act, Chapter 149 of Saint Vincent, and the Grenadines Revised Laws of 2009 (hereafter referred to as "Law"), the Company is authorised as an international business company for providing forex trading brokerage activities.

The Company is committed to protecting your privacy and offering you a robust online experience by safeguarding your personal and financial data. Under this Policy, "personal data" refers to any information the Company can use to identify or potentially identify a person. This information might include but is not limited to a client's name, address, identification number, phone number, date of birth, and other financial data (hereafter referred to as "personal data").

St Vincent and the Grenadines has implemented legislation aimed at detecting, preventing and prosecuting money laundering, terrorist financing and other serious crimes, as well as confiscating the profits of crime. The legislative measures reflect international best practices and consider the 40 Recommendations of the Financial Action Task Force (from now on, "FATF") on money laundering and terrorist financing and the 19 Recommendations of the Caribbean FATF.

The relevant laws are:

- Financial Intelligence Unit Act, Cap 174 of the Revised Laws of 2009
- Exchange of Information Act, Cap 146 of the Revised Laws of 2009
- Mutual Assistance in Criminal Matters Act, Cap 177 of the Revised Laws of 2009
- Proceeds of Crime Act, 2013
- Anti-Money Laundering and Terrorist Financing Regulations, 2014
- Anti-Terrorist Financing and Proliferation Act 2015
- Anti-Money Laundering and Terrorist Financing (Amendment) Regulations 2017
- Anti-Money Laundering and Terrorist Financing Code 2017
- Anti-Terrorist Financing and Proliferation Amendment Act 2017
- Anti-Money Laundering and Terrorist Financing (Non-Regulated Service Providers Regulations) 2022
- Immigration Restriction Amendment Act 2017
- Proceeds of Crime Amendment Act 2017

After careful study and consideration of the abovementioned legal framework in Saint Vincent and the Grenadines, we have concluded that we are exempted from any legal obligation to perform any of the activities described in it because we are authorised as an international business company to perform forex trading brokerage activities. The authorisation of our Company does not imply any license anyhow from Saint Vincent and the Grenadines (from now on, "SVG").

The Financial Services Authority in the SVG clearly states the following *"While registered St. Vincent and the Grenadines Business Companies (B.C.s), or Limited Liability Companies (L.L.C.s) are able to engage in any legal activity, if they engage in forex trading and brokerage, they are doing so without a licence from this jurisdiction. Until such time that appropriate legislation is put in place to address Forex activities, there is no legal prohibition against a B.C. or L.L.C. carrying out that activity or from so stating in its Articles of Incorporation or Articles of Formation."*

Regardless of our exception from the relevant regulatory framework, we decided and formed this Policy following, to a reasonable and risk-based degree, the guidelines issued by the SVG for Non-Regulated Services Providers (from now on, "NRSPs") in 2019, with the latest updated being on the 11th of October 2021.

The NRSPs are prohibited from carrying out any type of relevant business within Saint Vincent and the Grenadines unless registered (Section 155 (1) of the Proceeds of Crime Act, 2013 as amended by Act No.18 of 2017 (POCA)). The Registration of NRSPs is scheduled to commence after the passage of the Non-Regulated Service Providers Regulations, 2019.

According to Regulation 36 (b) of the Anti-Money Laundering and Terrorist Financing Regulations 2014, as amended by S.R.O No.25 of 2017 (AMLTFR), Saint Vincent and the Grenadines Financial Intelligence Unit (from now on, "SVGFIU") is designated as the supervisory authority of Non-Regulated Service Providers (NRSPs) which comprises of:

1. Real estate agents
2. Casinos
3. Car dealers
4. Jewelers
5. Lawyers, Notaries, Accountants and Auditors who engage in the following activities:

a. buying and selling of real estate
b. management of client money, securities, or other assets
c. management of the bank, savings, or securities accounts
d. the organisation of contributions for the creation, operation, or management of companies
e. creation, operation or management of legal persons or arrangements

Over the years, SVGFIU has conducted various training and awareness-raising sessions/workshops to sensitise NRSPs to their Anti-Money Laundering/Counter-Financing of Terrorism (AML/CFT) obligations under the AMLTF Regulations. The Supervisory Department was subsequently established on the 15th of August 2018.

Connext L.L.C., even if exempt, recognises the significance of performing the necessary measures to protect society, its clients, partners, and stakeholders from the harmful socioeconomic impacts of Money Laundering and Terrorist Financing activities.

This Policy applies to existing clients/employees/contractors and affiliates, potential clients/employees/contractors and affiliates, website visitors and clients/employees/contractors and affiliates whose contractual relationship with the Company has been terminated by either the Company or the client/employee/contractor and affiliate or both (from now on, jointly referred to as "related persons", "User(s)", "Client(s)" or "you" or "your") and who are using and/or otherwise accessing the Company's website(s), mobile and web applications and trading platforms (from now on referred to as the "Platforms").

By registering with or accessing the ConnextFX website, mobile and web applications, and trading platforms, you consent to collecting and using the personal data we require from you. By registering an account with Connext L.L.C., you agree to have your personal data processed and expressly consent to the collection, systematisation, aggregation, storage, revision (updating, changing), usage, anonymisation, blocking deletion, and distribution (transfer) of said personal data to third parties following the conditions outlined in the Privacy Policy as well as the current ANTI-MONEY LAUNDERING, TERRORIST FINANCING And K.Y.C. POLICY & PROCEDURES (hereafter referred to as "A.M.L. Policy", " Policy Statement", "Statement", or "Policy").

You agree to the personal data practices outlined in the Privacy Policy by using the ConnextFX website. You agree to the Company's collection and use of your information if you use the Company's website or provide it to us in other ways. You also guarantee to provide truthful, accurate, and current information. Users and/or clients and prospective users and/or clients are urged to thoroughly read the Terms of Service and Conditions before entering a contractual relationship with the Company.

Additionally, related persons, prospective users, and/or clients are urged to thoroughly read our detailed Privacy Policy on our website, which should always be in conjunction with the Terms of Service and Conditions and form an integral and indivisible part thereof.

This Policy is a fundamental component of the Terms of Service and Conditions and an integral part of them, and in the case of a conflict between them, the Terms of Service and Conditions will take precedence, leaving the other conditions intact.

The English version of this Policy is the official, authoritative version. Translations that may be provided are for your convenience only and should always be cross-referenced with the English text, which is the only version of the text intended to have legal effect.

This Policy establishes guidelines for Connext L.L.C.'s "Anti-Money Laundering", "Counter-Terrorist Financing", and "Know Your Client" (from now on, "KYC") procedures for both new and existing clients. If a Client is proven to have committed money laundering, he/she is responsible for any damage or loss which may occur, and the Company is excluded from his/her fraudulent actions. To the Company's best knowledge, all monetary transactions shall be free from money laundering and terrorist activities. The Company operates with integrity and is committed to implementing the measures established. The Client's failure to comply with the Company's policies

and/or procedures would mean the immediate account's termination and/or dismissal in the case of an employee.

As a company, we are committed to doing business according to the highest ethical standards, including complying with all applicable laws and international standards to combat money laundering and terrorist financing. The Company has developed this Policy to reduce the risk of money laundering and terrorist financing associated with its business and the sale of its products. This Policy explains our responsibility in complying with anti-money laundering and counter-terrorist financing laws and standards ("A.M.L. Laws") worldwide and ensuring that any third parties we engage in acting on our behalf do the same.

To counter money laundering and other illegal activity, we have decided not to support any cash transactions, regardless of their stated purpose. Our Company has the right to cancel or deny a transaction at any point if there are suspicions regarding its legality.

The management of the Company is committed to complying with all laws. Any employee who violates the rules in this Policy and/or permits anyone to violate those rules may be subject to appropriate disciplinary action, up to and including dismissal, and may be subject to personal civil or criminal fines.

If you disagree with any of the terms stated in any section of this Policy,
you are not permitted to use
the Platforms and any other Company's belongings
anyhow.

CONNEXT

Table of Contents

ANTI-MONEY LAUNDERING, TERRORIST FINANCING and K.Y.C. POLICY & PROCEDURES

The format of this document has been prepared primarily using the Compliance Programme Structural Guidelines for Non-Regulated Service Providers issued by the Supervisory Department of the SVGFIU on the 6th of October 2021 with reference number FIU REF:002/2021

Introduction

What is money laundering?

Money laundering means exchanging money or assets obtained illegally for legitimate assets. The expression "money laundering" covers all procedures to conceal the origins of criminal proceeds so that they appear to have originated from a legitimate source. Clean money or legitimate assets do not have an obvious link with any illegal activity.

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

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

The broad definition of money laundering means that anybody (including any Company's Employee) could violate the Law if they become aware of, or suspect, the existence of criminal property within the business and becomes involved in or continues to be involved in a matter which relates to that property being linked to the Company without reporting his/her concerns.

Property can be criminal property that derives from any illegal conduct, whether the underlying criminal conduct has occurred in the country where you are situated or overseas. There are three typical stages of money laundering, which occur in sequence but often overlap. It should be noted, however, that all stages may not be present in every situation:

Placement

This is the physical disposal of criminal proceeds. In the case of many serious crimes (such as drug trafficking and robbery), the proceeds take the form of cash, which needs to be placed in the financial system.

Techniques such as "structuring" or "smurfing" are used in which, instead of making a significant deposit transaction to cause suspicion, illegal receipts are broken up into smaller sums and deposited into single or multiple accounts and using other individuals to make the deposits.

Placement may include:

- placing cash on deposit at a bank (often intermingled with a legitimate credit to obscure the audit trail), thus converting money into a readily recoverable debt;
- physically moving cash between jurisdictions;
- making loans in cash to businesses which seem to be legitimate or are connected with legitimate businesses, thus also converting money into debt;
- purchasing high-value goods for personal use or expensive presents to reward existing or potential colleagues;
- purchasing the services of high-value individuals;
- purchasing negotiable assets in one-off transactions; or
- placing cash in the client account of a professional intermediary such as an attorney.

Layering

This occurs after the funds have entered the financial system and involve the separation of criminal proceeds from their source by creating layers of transactions designed to disguise the paper trail and provide the appearance of legitimacy.

Layering may include:

- rapid switches of funds between banks and/or jurisdictions;
- use of cash deposits as collateral security in support of legitimate transactions;
- switching cash through a network of legitimate businesses and "shell" companies across several jurisdictions; or
- resale of goods/assets.

Integration

This is the stage in which criminal proceeds are treated as legitimate. After the layering stage, integration places the criminal proceeds back into the economy to appear as legitimate funds or assets. These laundered funds are then used to further illegal activity or enhance the criminal lifestyle, such as real estate investments or purchasing luxury assets.

What is terrorist financing?

Terrorist financing is the process by which funds are provided to an individual or group to fund terrorist activities. Unlike money laundering, funds to finance terrorism can derive from legitimate sources such as personal donations, non-profit organisations, state sponsorship, profits from legitimate commercial businesses or criminal activity such as drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion. Similar to money laundering, terrorist financiers also move funds to disguise their source, destination, and purpose for which the funds are to be used. Terrorist financing may not involve the proceeds of criminal conduct but rather an attempt to conceal the origin or intended use of the funds, which will later be used for illegal purposes.

Red Flags

Where any suspicions arise that criminal conduct may have taken place involving a customer, colleague or third party, you should consider whether there is a risk that money laundering or terrorist financing has occurred or may occur.

Some examples of red flags to be reported include:

- A customer provides insufficient, false, or suspicious information or is reluctant to provide complete information
- Methods or volumes of payment that are not consistent with the payment policy or that are not customarily used in the course of business, e.g., payments with money orders, traveller's checks, and/or multiple instruments, and payments from unrelated third parties
- Receipts of multiple negotiable instruments to pay a single invoice
- Requests by a customer or partner to pay in cash
- Early repayments of a loan, especially if payment is from an unrelated third party or involves another unacceptable form of payment
- Orders or purchases that are inconsistent with the Customer's trade or business
- Payments to or from third parties that have no apparent or logical connection with the Customer or transaction
- Payment to or from countries considered high risk for money laundering or terrorist financing
- Payments to or from countries considered to be tax havens or offshore jurisdictions
- Payments from countries unrelated to the transaction or not logical for the Customer
- A customer's business formation documents are from a tax haven or a country that poses a high risk for money laundering, terrorism or terrorist financing, or a country that is not logical for the Customer
- Overpayments followed by directions to refund a payment, especially if requested to send the payment to a third party
- Any customer for whom you cannot determine the true beneficial owner
- Structuring transactions to avoid government reporting or record-keeping requirements

- Unusually complex business structures and payment patterns that reflect no real business purpose
- Wire transfer activity that is not consistent with the business activities of the Customer or which originates or terminates with parties unrelated to the transaction
- Unexpected spikes in a customer's activities

The above is not intended to be an exhaustive list. Deviation from customers and accepted business practices should alert the Company further to investigate the activity under this Policy.

General Information of the Policy

This Policy covers the website www.connextfx.com and all its related sub-domains, trading-related Platforms and mobile applications owned, registered and/or operated by the Company.

The Law does not prohibit any of the Company's objectives and/or activities. This statement includes, but is not limited to, all financial, commercial, trading, lending, borrowing, service activities, and participation in other businesses and/or enterprises, as well as the provision of brokerage, managed account services, and trading.

The Company does not aim to display its website and services to persons in countries where the use of the website and its services is contrary to their national regulatory framework. When a user accesses this website from a country with or without prohibited access to this website, it is the user's responsibility to use the website or services under his/her local laws or regulations. The Company does not guarantee or claim that this website's information is suitable for all legal jurisdictions.

The Company describes in the Policy the procedures it follows while collecting, storing, using, and disclosing the Client's personal data to prevent money laundering, terrorist financing and proliferation financing. This Policy applies to Connext L.L.C., which must abide by its fundamental principles.

The Company is dedicated to safeguarding the confidentiality of all Clients' Personal Data, which it handles under the terms of this Policy, the Privacy policy and the Company's Terms of Service and Conditions (hereafter referred to as "Terms of Service" or "Terms of Business")

A. Policy Statement on A.M.L.

It is Company's Policy to comply with all applicable A.M.L. Laws in our operations worldwide. This Policy is intended to help employees, contractors, and other third parties acting on the Company's behalf to understand where breaches of A.M.L. Laws might arise and to support them in making the right decisions in line with our corporate position as stated in this Policy. To this end, Connext L.L.C. will only conduct business with customers involved in a legitimate business activity whose funds are derived from legitimate sources.

B. Board Endorsement and purpose of the Policy

The Board of Connext L.L.C. will not criticise management for any loss of business resulting from adherence to this Policy. No employee or contractor will suffer as a consequence of bringing to the attention of the Board or senior management, in good faith, a known or suspected breach of this Policy, nor will any employee or contractors suffer any adverse employment or contract decision for abiding by this Policy.

The purpose of this Policy is to:

▪ enable the Company to identify, assess, mitigate, manage, and monitor the risk that the provision by the Company of its products or services may involve or facilitate money laundering activities or the financing of terrorist and related activities.

▪ provide how the Company determines if a person is:

- A prospective client in the process of establishing a business relationship or entering into an occasional transaction with the Company, or
- A client who has established a business relationship or entered into an occasional transaction is a client of the Company.

▪ provide how the Company complies with the compliance obligations of not establishing a business relationship or concluding an occasional transaction with an anonymous client or a client with an apparent false or fictitious name.

▪ provide for how and the processes by which the Company:

- Establishes and verifies the Identity of a client; and
- Establishes a client representative's authority to establish a business relationship or to conclude a single transaction on behalf of a client.

▪ provide for how and the processes by which the Company determines whether future transactions that will be performed during the business relationship are consistent with the Company's knowledge of a prospective client.

▪ provide for how and the processes by which the Company conducts additional due diligence measures in respect of legal persons, trusts and partnerships.

▪ provide for how and the processes by which the Company conducts ongoing due diligence and account monitoring in respect of business relationships.

▪ provide for how the examination of:

- Complex or unusually large transactions, and

• Unusual patterns of transactions which have no apparent business or lawful purpose take place.

▪ provide how and the processes by which the Company will confirm information relating to a client when the Company has doubts about the veracity of previously obtained data.

▪ provide for how, and the processes by which the Company will perform the Client's due diligence requirements under the following compliance obligations:

- The identification of clients and other relevant persons;
- Understanding and obtaining information on business relationships;
- Additional due diligence measures relating to legal persons, trusts and partnerships;
- Ongoing due diligence occurs during a business relationship and/or when the Company suspects or knows that a transaction or activity is suspicious or unusual.

▪ provide for how the Company will terminate an existing business relationship where the Company is unable to:

• Establish and verify the Identity of a client or other relevant person,
• Obtain information describing the nature of the business relationship, the intended purpose of the business relationship concerned and the source of funds which a prospective client expects to use in concluding transactions in the course of the business relationship involved,
• Conduct ongoing due diligence.

▪ provide for how and the processes by which the Company will determine whether a prospective client is a foreign prominent public official or a domestic prominent, influential person.

▪ provide for how and the processes by which enhanced due diligence is conducted for higher-risk business relationships and when simplified client due diligence might be permitted in the Company.

▪ provide the manner, place, and period for which client due diligence and transaction records are kept.

▪ enable the Company to determine when a transaction or activity is reportable to the SVGFIU.

C. Who is subject to this Policy?

This Policy applies to Connext L.L.C.'s operations globally, including all legal entities owned or controlled by Connext L.L.C. (including all group companies), and to all directors, officers, employees, contractors, and other third parties acting on behalf of the preceding.

This A.M.L. Policy applies to:

- The Company's governing body;
- Where applicable, all branches, business units and divisions of the Company;
- All employees and Clients.

The Company's governing body requires all employees to comply with the processes and procedures outlined herein. Any gross negligence or willful noncompliance with the provisions of this Policy and/or the processes and procedures outlined within this Policy will be considered a severe form of misconduct which may result in a dismissal.

D. What's the risk?

Violations of A.M.L. Laws may lead to severe civil and/or criminal penalties against companies and individuals, including significant monetary fines, imprisonment, extradition, blacklisting, revocation of licences, and disqualification of directors.

In addition, violations of A.M.L. Laws can lead to damaging practical consequences, including harm to reputation and commercial relationships, restrictions in how we can do business, and extensive time and cost in conducting internal investigations and/or defending against government investigations and enforcement actions.

E. Compliance controls and Programme

Senior management of the Company is responsible for ensuring that their business has a culture of compliance and adequate controls to comply with A.M.L. laws and regulations to prevent, detect and respond to money laundering and counter-terrorism financing and to communicate the severe noncompliance consequences to employees.

The Compliance Programme of our Company includes these five (5) keys elements to have an effective system of internal controls:

1. The appointment of a reporting/compliance officer (from now on "AMLCO");
2. The development and application of written and updated compliance policies and procedures (from now on, "KYC Policy and Procedures") about Customer Due Diligence and Enhance Due Diligence protocols, the detection and reporting of suspicious activities/ transactions, ongoing monitoring and record-keeping procedures.

3. an assessment and documentation of risks related to money laundering and terrorist financing, as well as the documentation and implementation of mitigation measures to deal with those risks;
4. an ongoing compliance training program for employees and staff; and
5. the periodic documented reviews/audits of the effectiveness of implementing the policies and procedures, training, and risk assessment.

Our Company tries to ensure that relevant policies, processes, and controls are communicated to all relevant employees and Customers. An effective AML/CFT programme will only work if the employees and Customers who are most likely to interact with the money launderers are aware of the policies. Therefore, training and development sessions about anti-money laundering and counter-terrorist financing are required. Without effective communication of the obligations of the business concerning money laundering, the Company will be blindsided as it relates to the use of the business as a medium for money laundering and terrorist financing purposes.

F. Employee, Client, and Contractor Responsibility

Employees, Clients, and Contractors must read, understand, agree, and follow this Policy to understand and identify any red flags that may arise in their business activities and to escalate potential compliance concerns related to A.M.L. to Ethics and Compliance or the Legal Department without notifying anyone involved in the transaction and should not take any actions before receiving advice and/or instructions

G. Due Diligence and Record-Keeping

Various factors will determine the appropriate forms and levels of screening. It is our Policy to carry out Customer due diligence ("C.D.D.") and take prudent measures to Know our Clients (“K.Y.C.”) at the outset of any business relationship and, if necessary, where any red flags arise subsequently on our Customers, as defined and mentioned earlier in this document, so we can be satisfied that they are whom they say they are and so that we can ensure that there are no legal barriers to working with them before contracts are signed, or transactions occur. It would be best if you escalated any instances where you have cause for suspicion due to carrying out C.D.D. and ongoing monitoring to Ethics and Compliance or the Legal Department, who will advise them regarding which tools and processes should be used to facilitate appropriate screening.

In consultation with the Ethics and Compliance or the Legal Department, you must carefully consider screening outcomes before deciding whether to do business with a third party. Finance managers and/or back-office managers must regularly monitor and/or review Customers to identify business activity or governance that could indicate money laundering or terrorist financing is taking place.

Record-keeping is essential to the audit trail required to assist in any investigation. The Company must maintain records as evidence of the C.D.D. and ongoing monitoring undertaken.

The Company should gather sufficient information to be satisfied that it has identified all relevant risk factors, including, where necessary, applying additional C.D.D. measures, and assess those risk factors to obtain a holistic view of the risk associated with a particular business relationship or occasional transaction.

The Company monitors transactions to ensure they align with the Customer's risk profile, economic profile, and business and, where necessary, examines the source of funds to detect possible ML/TF. The Company must keep their risk assessment up to date and under review. The Company also save the documents, data, or information they hold up to Date, intending to understand whether the risk associated with the business relationship has changed and/or amended anyhow.

H. General Measures

The Company collects several types of Personal Data via the Company's Platforms from Clients who visit the Platforms or access, use, manage or request products and services offered by the Company. It is the Company's A.M.L. and K.Y.C Policy to apply to all clients the below-mentioned general measures:

- check the Identity of the Client
- monitor any suspicious Client activities and/or transactions
- have a record of all the related information and/or documents of the Client's financial transactions

The Company's KYC and due diligence procedures are applied by the Company's Back Office when accepting clients to open trading accounts and by the Human Resources department when it has to do with Company’s employees.

Clients are responsible for ensuring that the Personal Data they provide to the Company by themselves and/or through a third party and recorded in their account remain accurate and up to date throughout their contractual and/or business relationship with the Company.

Since payments are made through third parties (only banks), we do not, at any time, collect the information you use when making any such payments. Third parties have terms and conditions for using their services; we cannot and do not assume any liability concerning using such third-party services. You must know such terms and/or conditions when making payments through third parties.

We use various methods to gather data for you, including but not limited to those mentioned in our Privacy Policy.

I. Restricted Business and Jurisdictions

Our Company does not provide services to clients whose activities are associated with high-risk or banned activities. Furthermore, the Company does not accept clients from high-risk countries, including but not limited to the following countries:

- Cuba
- Iran
- North Korea
- Afghanistan
- Iraq
- Syria
- United States
- China
- Russia
- Singapore
- Brazil
- South Africa
- Hong Kong
- Japan

Furthermore, the Company does not accept clients from Jurisdictions under Increased Monitoring, and high-risk countries as per the guidelines of FATF, which are updated accordingly can be found at https://www.fatf-gafi.org/publications/?hf=10&b=0&s=desc(fatf_releasedate) and also mentioned at Appendix 1 and 2.

J. Noncompliance

Our Company has zero tolerance for possible exposure to money laundering, terrorist financing and proliferation financing risks.

Any employee or Customer who violates this Policy may be subject to appropriate disciplinary action, independently from potential other penalties resulting from their behaviour.

The Compliance team and the Internal Audit shall conduct regular checks on local businesses to ensure compliance with A.M.L. Laws as our Company's second and third layer of defence concerning money laundering, terrorist financing and proliferation financing risks.

K. Updates, Review and Ownership

This Policy may be updated from time, and the updated version of the Policy will be immediately made available on the Company's intranet and official website, i.e., www.connextfx.com

L. Definitions

1. "Client(s)" or "Customer (s)", in addition to the general term given in the Preamble, means any natural or legal person:

    a) who seeks to enter a business relationship or conduct an individual transaction with the Company or
    b) to whom an investment firm provides any investment or ancillary services or
    c) Suppliers, distributors, counterparties, agents, and any person with whom the Company has an established business relationship that will involve transferring or receiving funds.

2. "business relationship" means a business, professional or commercial relationship between the Customer and the Company, which is connected with the business activities of the Company and is expected by the Company, at the time of entering into the contact, to be of some duration

3. "occasional transaction" means a business, professional or commercial transaction between the Customer and the Company which is connected with the business activities of the Company and is expected by the Company, without entering into the contact, not to have duration.

4. "Source of Funds" refers to the origin of the particular funds or assets which are the subject of the business relationship between the Company and its Client and the transactions the Company is required to undertake on the Client's behalf (e.g., the amounts being invested, deposited, or remitted).

5. "Source of Wealth" refers to the origin of the entire body of wealth (i.e., total assets) of the client

6. "politically exposed person" or "P.E.P." means a natural person who has or has been entrusted with an important public function in any country, a direct close relative of such a person, as well as a person known to be a close associate of such a person:

    Provided that, for this definition, "important public function" means any of the following public functions:

a. Head of State, Head of Government, Minister, Deputy Minister, and Deputy Minister;
b. a member of parliament or a similar legislative body;
c. a member of the governing body of a political party;
d. a member of a supreme court, constitutional court, or other high-level judicial body whose decisions are not subject to further legal remedies, except in exceptional circumstances;
e. a member of the supervisory Board and Board of directors of a central bank;
f. ambassador, chargé d'affaires and senior officer of the armed forces and security forces;
g. member of an administrative, management or supervisory body of a state enterprise;
h. director, deputy director and board member or a person holding an equivalent position in an international organisation;
i. mayor: It is further understood that the abovementioned public functions do not include a person occupying an intermediate or low position in the civil service hierarchy:

Provided further that "a close relative of a politically exposed person" includes the following persons:

a. Spouse, or person resembling a spouse of a politically exposed person;
b. a child of a politically exposed person and his spouse or a person resembling a spouse of a child of a politically exposed person;
c. parents of a politically exposed person;

Provided further that "a person known to be a close associate of a politically exposed person" means a natural person-

a. who is known to be a joint beneficial owner of a legal entity or legal arrangement or to be associated with any other close business relationship with a politically exposed person;
b. 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 politically exposed person;

7. "Risk" means the impact and likelihood of ML/TF taking place. Risk refers to inherent risk, the level of risk that exists before mitigation. It does not refer to residual risk, that is, the level of risk that remains after mitigation.

8. "Risk factors" means variables that, either on their own or in combination, may increase or decrease the ML/TF risk posed by an individual business relationship or

occasional transaction.

9. "Risk-based approach" means an approach whereby competent authorities and firms identify, assess, and understand the ML/TF risks to which firms are exposed and take AML/CFT measures that are proportionate to those risks.

M. Acronyms Used in the Policy

A.M.L.- Anti-Money Laundering
CTF- Counter Terrorist Financing
MLCO- Money Laundering Control Officer
KYC- Know Your Customer
FATF- Financial Action Task Force
C.D.D.- Customer Due Diligence
E.D.D.- Enhanced Due Diligence

N. Duties of the Board of Directors and the Senior Management

The duties of the Board of Directors and the Senior Management are the following:

i. The Board of Directors defines, records, and approves the general principles of the Company's Policy for the prevention of money laundering and terrorist financing, which it communicates to Senior Management and the Anti-Money Laundering Compliance Officer (from now on, the "AMLCO" or “Compliance Officer”). An effective program for the prevention of money laundering and terrorist financing requires a clear message from the Company's management concerning the risk appetite, which will determine the organisation's expectations, parameters and limits of operation and the commitment against money laundering and terrorist financing.

ii. The Board of Directors gives an example of leadership by consistently expressing the underlying values of corporate compliance culture, ensuring that its behaviour reflects the values it embraces.

iii. The Board of Directives and Senior Management should know the level of risk for money laundering and terrorist financing that the Company is exposed to decide whether all necessary measures are taken for its management and minimisation, according to the risk appetite of the credit institution.

iv. The AMLCO is responsible for cooperation with other departments of the Company for designing policies, procedures, and controls and also the description and precise definition of responsibilities and limits of responsibility of each department that is dealing with matters related to the prevention of money laundering and terrorist financing. Therefore, an appropriate manual of procedures and risk management is prepared. After approval by the Senior Management of the Company, it is communicated to the officials and all staff

responsible for implementing the Company's policy, procedures, and controls.

v. The manual is periodically assessed and is updated when deficiencies are found or when the need arises to adapt the Company's procedures for more effective management of the risks from money laundering and terrorist financing. It should be noted that any updates of the manual should be approved by Senior Management.

vi. The AMLCO and other members of staff who have been assigned with the duty of implementing the procedures for the prevention of money laundering and terrorist financing have full and prompt access to all data and information concerning customers' Identity, transactions' documents and other relevant files and information maintained by the credit institution to be fully facilitated in the effective discharge of their duties.

vii. The staff of the Company is informed about the person appointed as AMLCO to whom they should report any information concerning transactions and activities for which they believe or suspect that they might be related to money laundering and terrorist financing.

viii. There is a clear and concise reporting chain explicitly prescribed in the manual of procedures and risk management by which information regarding suspicious transactions is reported without delay and directly to the AMLCO.

ix. Policies, procedures, and measures are applied so that the risk of money laundering and terrorist financing is identified, assessed, and managed during the day-to-day operations of the Company about:

a. the development of new products, services, and new business practices, including new delivery channels
b. the use of new or developing technologies for both new and existing products and
c. possible changes in the Company's business profile (e.g., penetration to new markets by opening branches/subsidiaries in new countries/areas).

x. This risk assessment should take place before the launch of new products, business practices, or new or developing technologies.

xi. The ability to make proper decisions might be weakened by insufficient data quality. Hence, the Company must ensure adequate data quality is maintained in the customers' files and the information systems. In this respect, the Company ensures that its policies, controls, and procedures provide data quality management in terms of accuracy, validity, and integrity. The roles and responsibilities regarding data quality should be clearly defined and well organised.

xii. The Company's Senior Management ensures that the AMLCO has sufficient resources, including competent staff and technological equipment.

xiii. The Board of Directors and the Senior Management receive regular, adequate, and objective information to obtain an accurate picture of the risks of money laundering and terrorist financing to which the credit institution is exposed through its operations/activities and/or business relationships.

xiv. The Board of Directors and the Senior Management receive regular, adequate, and objective information from the AMLCO and the Internal Auditor regarding the effectiveness of the measures and controls against money laundering and terrorist financing.

xv. The Internal Audit inspects and evaluates, at least on an annual basis, the effectiveness and adequacy of the Policy, procedures and controls applied by the Company for preventing money laundering and terrorist financing and periodically and according to the risk through regular or special audits, verifies the level of compliance of the Company with the A.M.L. Laws.

xvi. The audit program should be appropriate to the Company's size, nature of operations and risk profile.

xvii. The Internal Auditor monitors the implementation of his/her recommendations through progress reports or other means. The Internal Audit findings and observations are submitted to the Board of Directors' Audit Committee. They are notified to the Senior Management and the AMLCO of the Company, who take the necessary measures to rectify any weaknesses and omissions that have been recorded.

xviii. The Company applies explicit recruitment procedures and standards and evaluates the employees' integrity (existing and newcomers).

O. Duties of the AMLCO

The AMLCO is responsible for the following:

- To prepare and submit for approval to the Board of Directors through the Senior Management a report recording and assessing the risks for money laundering and terrorist financing, considering the areas where:
    - the Company is operating,
    - the provision of new products and services,
    - acceptance of new customers,
    - the expansion to new markets/countries,
    - the complex shareholding structure of legal persons,
    - the method of attracting customers,
    - the measures are taken for their management and minimisation and also
    - the mechanisms for monitoring the right and effective operation of internal regulations, procedures, and controls

The AMLCO Objectives are:

- To protect the integrity of the Company through the continued management of money laundering and terrorist financing risk.
- To apply a risk-based approach to client transactions and understand the purpose of all business relationships with clients.
- To educate employees on identifying business relationships and transactions that pose a higher risk to money laundering and terrorist financing.
- To implement robust Client Due Diligence and K.Y.C. procedures that will make it more difficult for criminals to hide the proceeds of unlawful activities.
- To submit to the Board of Directors relevant reports concerning all transactions identified as being suspicious, unusual or above the prescribed threshold.
- Keep accurate records of all transactions, Client Due Diligence, and K.Y.C. procedures.
- To prevent any reputational fallout or brand damage due to non-compliance with A.M.L. Laws.
- To prevent any civil or criminal fines or penalties due to noncompliance with A.M.L. Laws.
- To prevent loss of sales and client confidence due to noncompliance with A.M.L. Laws.

P. Employee Awareness and Training

The Company:

a) Undertakes measures to ensure that all 'relevant' employees are 'made aware' of the laws relating to money laundering and terrorist financing within St. Vincent and the Grenadines and regularly provides training on recognising and dealing with transactions which may be related to money laundering or terrorist financing. Training is made available to all partners in firms, managers, sole practitioners, and it is necessary to train all client-facing staff.

b) Develops a training plan, in which the objective is to create an environment effective in preventing money laundering and terrorist financing and which thereby helps protect individuals and the business.

c) Considers not only staff who have involvement in client work or are interacting with customers but also, where appropriate, those who deal with the business finances and those who deal with procuring services on behalf of the business and who manage those services.

d) Provides comprehensive training to all relevant staff members or chooses to tailor its provision to match the role of the employees concerned more closely.

e) Provides training on the internal consultation and advisory systems (to assist individuals in assessing whether they have a valid suspicion), internal reporting systems and expectations for confidentiality and the avoidance of tipping off and alerting a money launderer.

f) Provides training on an annual basis or based on new trends and typologies in money laundering and terrorist financing, using new case law or national/international findings, or by a change in the profile and perceived risks of the business

g) Keeps records of training provided. Training methods may be selected to suit the size, complexity and culture of the business and may be delivered in a variety of ways, including face-to-face, self-study, e-learning and video, or a combination of methods

h) Makes arrangements to ensure new staff are trained as soon as possible after they join the business.

The training will take place as follows for every type of employee in our Company:

- New professional staff dealing with clients or their affairs, irrespective of seniority, must obtain a general appreciation of the background on money laundering or terrorist financing, C.D.D. and KYC procedures and the procedures for identifying and reporting any suspicious transactions to the Compliance Officer. New staff should be aware that suspicious transaction reporting is also their personal obligation.

- Front-line staff who deal directly with clients are likely to be the first point of contact with potential money launderers or terrorist financiers, and their efforts are vital to the firm's reporting system. Training should be provided on factors that may give rise to suspicions and the procedures to be adopted when a transaction or activity is deemed suspicious. Particular emphasis should be given to the fact that this group of staff is the "eyes and ears" of the firm, which can identify any abnormal behaviour or patterns of the Client.

- Staff accepting clients must receive the training recommended for front-line staff. Such staff should be aware of the types of suspicious information that may need to be reported to the Compliance Officer, like forged documents, sanction-related information, inconsistent activities with the client's economic profile, etc. They must also know what procedures to follow in these circumstances. In addition, the need to verify the Client's Identity must be understood, and training should be given on the firm's client verification procedures.

- Top-level management responsible for supervising or managing staff should be provided with a higher level of instruction covering all aspects of money laundering or terrorist financing.

- The Compliance Officer must receive in-depth training concerning all aspects of the A.M.L. Laws and recent developments on the field, enabling him/her to update internal procedures effectively. In addition, the Compliance Officer should receive extensive initial and ongoing training on the validation and reporting of suspicious transactions, feedback arrangements, and new criminal activity trends and patterns.
  Compliance culture

  When designing pieces of training, our Company aims to create an A.M.L. compliance culture within the organisation, avoiding tick-the-box approaches and always paying particular attention to the risk-based approach. Developing a compliance culture within the Company is the most crucial safeguard an organisation can have in the fight against money laundering, terrorist financing and financial crime.

Customer Due Diligence or "C.D.D."

Effective Customer due diligence measures are an essential part of our system designed to prevent money laundering and terrorist financing and are a cornerstone of the AML/CFT Obligations. However, risks must be assessed before the appropriate level of Customer due diligence can be applied. Customer due diligence measures and KYC procedures are conducted in the following circumstances:

- when establishing a business relationship,
- when carrying out an occasional transaction,
- where there is a suspicion of money laundering or terrorist financing; and
- where there are doubts concerning the veracity of previous identification information.

The KYC procedure is a requirement to comply with International law provisions, including the ones designed to prevent money laundering. When a client applies to open an account with us, the Company has to ensure that various documents and/or other third-party evidence are received along with the application.

Customer Due Diligence is central to identifying, assessing, and managing the ML/TF risk associated with individual business relationships and occasional transactions in a risk-based, proportionate, and effective way. C.D.D. and K.Y.C for our Company mean:

- identifying the Customer and verifying the Customer's Identity based on documents, data or information obtained from a reliable and independent source;
- identifying the Customer's beneficial owner and taking reasonable measures to verify their identity so that the obliged entity is satisfied that it knows who the beneficial owner is;
- assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and
- conducting ongoing monitoring of the business relationship. This includes transaction monitoring and keeping the underlying information up to Date.

We use our business-wide risk assessment findings to decide the appropriate level and type of C.D.D. we will apply to individual business relationships and occasional transactions.

Before entering into a business relationship or carrying out an occasional transaction, we apply initial C.D.D., which includes at least risk-sensitive measures to:

a. Identify the Customer and, where applicable, the Customer's beneficial owner or legal representatives;
b. verify the Customer's Identity based on reliable and independent sources and, where applicable, verify the beneficial owner's Identity in such a way that the firm is satisfied that it knows who the beneficial owner is; and
c. establish the purpose and intended nature of the business relationship.

We also perform during the onboarding stage:

a. Pre-screening via both Email and Phone verification
b. Verification via Identity Document, World databases check, Liveness check, AML screening, Address verification, age verification, video identification and business verification

In addition, during the account activity, we perform the following:

1. At the login, we perform face authentication via third-party licensed entities
2. Bank card verification and face authentication
3. Ongoing transaction monitoring.

We adjust the extent of initial C.D.D. measures, KYC procedures, and controls on a risk-sensitive basis. Where the risk associated with a business relationship is low, and to the extent permitted by national legislation, we apply simplified Customer due diligence measures (S.D.D.). Where the risk associated with a business relationship is increased, we use enhanced customer due diligence measures (E.D.D.) and/or reject the Client and/or terminate our business relationship with him/her.

Individuals/Natural Persons

(this also applies to natural persons involved in a legal entity, such as Directors, Shareholders, or authorised persons)

In respect of individuals or natural persons we:

- Obtain C.D.D. information (identification and relationship information) of every Customer, third party and beneficial owner.

❖ Identification information includes:

o The full legal name of the individual
o Gender of the individual
o Principal residential address of the individual
o Date of birth of the individual

❖ Relationship information includes:

o The purpose and intended nature of the business relationship
o Type, volume, and value of the expected activity

o Source of funds (Any transaction that exceeds the value of 10,000 United States Dollars (from now on "USD") must be documented on the "Declaration of the source of Wealth" Form)

- Request two (2) forms of identification during the C.D.D. process, one (1) to identify and the other to verify. In high-risk situations, three (3) forms of identification are necessary, one (1) for identification and two (2) for verification.

  ❖ The best forms of identification and verification documents are:

  o A current passport
  o A current national government-issued identification card
  o A current driver's license

  ❖ Acceptable sources for verifying residential addresses are:

  o An independent data source such as the register of electors, telephone directory, commercially available databases maintained by credit reference agencies, business information services and commercial agencies that provide electronic identity checks.
  o A recent bank statement or utility bill (preferential option)
  o Correspondence from a central or local government department or agency
  o A letter of introduction confirming residential address from a regulated person or foreign regulated person.

- Verify the Identity of the Customer and any third party and take reasonable measures, on a risk-sensitive basis, to verify the identity of each beneficial owner. Verification of Identity may, in certain circumstances, be conducted after the establishment of a business relationship if this is necessary not to interrupt the ordinary course of business and there is little risk of money laundering or terrorist financing occurring, provided the verification is completed as soon as practicable after contact is first established.

- Conduct ongoing monitoring of the business relationship. During a business relationship, the Company monitors activity on an ongoing basis. This includes scrutiny of transactions, source of funds and other elements of knowledge collected in the customer due diligence process to ensure that the new information is consistent with additional knowledge of the Client and keeping the documentation concerning the Client and the relationship updated.

- Ensure customer due diligence procedures are applied to all new and existing clients.

- Ensure that the identification data is kept up-to-date and review the records of higher-risk customers or business relationships as appropriate.

1. Proof of Identity (P.O.I.)

P.O.I. is any document used to prove a person's Identity. It should be valid, indicating expiration date, not expired as a document and have the Client's photo. For European citizens, an Identification card is sufficient. For all others, it should be a passport. Without a passport, identification with a driving license will be accepted instead. These documents are checked both electronically and manually to decrease the possibility of fraud and/or other related matters, such as synthetic identification documents.

2. Proof of Residence (P.O.R.)

- Proof of residence is a document confirming where the Client lives. It needs to have both the name of the individual and his/her address printed on it. Such documents are Recent Utility Bill. This can be a water bill, electricity bill, bank statement or bank reference letter, tax bill, municipality bill where the home address is shown or,
- Any other official document with the information mentioned above.

3. Proof of Bank Account Ownership

All our transactions relating to deposits and withdrawals to and from the client accounts take place via bank wires through recognised and well-known banks and credit institutions using their internet and mobile banking facilities. Those banks are a mitigating measure we have added for safeguarding the additional preventive measures for money laundering, terrorist financing and proliferation financing via their individual and independent from us KYC procedures, ongoing monitoring of the transactions and other related standards for the purposes of Anti-money laundering, Counter Terrorist financing and counter proliferation financing.

Corporate Account for Legal person or Entity In

respect of a legal person or entity, the Company is doing the following:

• The Company obtains for identification information:

- The full name of the legal person
- The date of incorporation, registration and/or formation
- Official identifying number
- The registered office or the address of the head office
- The name and address of the registered agent
- The mailing addresses
- The principal place of business
- The names of the directors

- Identification information of the directors
- Identification information on the individuals who are beneficial owners of 15% of the company/business

• It verifies the Identity of the directors/ beneficial owners of the Company or business
• It conducts ongoing monitoring of the business relationship
• It ensures that the identification data is kept up-to-date and review the records of higher-risk customers or business relationships as appropriate

When a legal person wishes to open an account with our Company, the following must be collected:

Company's Incorporation Documents

- ✓ Certificate of incorporation or equivalent
- ✓ Certificate of registered office or equivalent
- ✓ Certificate of directors and secretary or equivalent
- ✓ Certificate of shareholders or equivalent
- ✓ Memorandum and articles of association of the legal person
- ✓ A recent copy (up to three months) of a bank statement or utility bill to verify the head office address
- ✓ Identity of Directors and Shareholders with their relevant KYC documents required of Natural Persons
- ✓ Authorised person resolution signed by the Board of directors ('BoD')

Additional Documents

In addition, depending on the amount the Client wishes to exchange, the Company has formed Tiers where the required documentation differs. These Tiers are:

Tier 1- Up to 5,000 USD/EUR

- ✓ PoR (proof of residence)
- ✓ PoI (proof of Identity) + Selfie (holding I.D. for face recognition)
- ✓ Bank statement showing fund transfer for the crypto purchase

Tier 2- Between 5,000 – 15,000 USD/EUR

- ✓ PoR (proof of residence)
- ✓ PoI (proof of Identity)
- ✓ Selfie (holding I.D. for face recognition)
- ✓ Bank statement showing monthly income (salary/pension and others for last three months)
- ✓ DoD (Declaration of deposit signed)

Tier 3- Above 15,000 USD/EUR

- ✓ PoR (proof of residence)
- ✓ PoI (proof of Identity)
- ✓ Selfie (holding I.D. for face recognition
- ✓ Bank statement showing monthly income salary/pension and others for last three months)
- ✓ DoD (Declaration of deposit signed)
- ✓ Proof of Wealth
- ✓ Source of funds

Terminations

In cases where the Company is unable to comply with any of the following C.D.D. measures and/or K.Y.C. procedures and/or relevant controls, namely:

• To apply C.D.D. measures before the establishment of a business relationship or before carrying out an occasional transaction;
• To complete the verification of the Identity of a customer, third party or beneficial owner after the establishment of a business relationship; or
• To undertake ongoing monitoring concerning a business relationship

It does not open an account, commence business relations, accept instructions, or perform any transaction.

Where C.D.D. obligations for existing business relationships and clients are not met due to the Client's refusal to comply or causing unacceptable delays, the Company terminates the business relationship and considers filing a Suspicious Activity Report (S.A.R.) with the SVGFIU.

Customer due diligence measures are critical to the anti-money laundering and counter-terrorist financing requirements. They ensure that the Company knows who its clients are and does not accept clients unknowingly who are outside its standard risk tolerance or whose business it will not understand with sufficient clarity to be able to form money laundering or terrorist financing suspicions when appropriate. Continued alertness for changes in the nature or ownership of the Client, its business model, or its susceptibility to money laundering or Terrorist Financing – or actual evidence of the latter - is maintained.

Construction of Economic Profile

The data and information we collect before the establishment of the business relationship and the execution of any transactions to construct the Customer's economic profile as part of our Company's C.D.D. measures and K.Y.C. procedures and controls, as a minimum, includes the following:

a. the purpose and the reason for opening the account,
b. the anticipated account turnover,
c. the nature of the transactions,
d. the expected origin (e.g., countries and names of principal counterparties) of funds to be credited to the account and the expected destination (e.g., countries and names of central counterparties) of outgoing transfers/payments,
e. the source and size of the Customer's wealth and annual income,
f. the clear and detailed description of the primary business/ professional activities/operations.

Ongoing monitoring of transactions and business relationships

Ongoing monitoring is vital to effective Anti-money laundering and counter-terrorist financing compliance systems as part of our Company's controls. Ongoing monitoring procedures assist obliged entities in updating existing knowledge of their clients and detecting any unusual or suspicious activities.

Ongoing monitoring procedures are customised depending on the type of services offered to the Client. An audit client's ongoing monitoring procedures differ from those adopted for a client that obtains directorship or bank management services.

For example, the Company can perform ongoing monitoring by:

a. Reviewing the documents and information collected for C.D.D. purposes relating to the Client to ensure they are up-to-date and relevant
b. Examining transactions carried out by the Client or on behalf of the Client to ensure that they are consistent with the existing knowledge of the clients' functions, business, risk profile and size and source of funds and/or wealth (economic profile of Client)
c. Identifying complex transactions, unusually large in amount or of an unusual pattern or that have no apparent economic or lawful purpose which may indicate money laundering and/or terrorist financing
d. Making appropriate inquiries of clients

When examining transactions, the Company considers the following factors:

a) Geographical source/destination of funds
b) High or inconsistent amounts
c) Numerous small transactions that, when combined, exceed the anticipated threshold
d) Nature or type of individual transactions or series of transactions
e) Clients' usual pattern of activities or size of turnover
f) Changes in the usual method of communication with the Client

In cases where the substance of a business relationship changes significantly, the Company performs additional C.D.D. procedures to identify and subsequently mitigate, if necessary, the money laundering and terrorist financing risks involved. If the revised risk is not in line with the Company's risk appetite, then consideration is made to terminate the business relationship.

Ongoing monitoring of the transactions

The procedures and intensity of monitoring accounts and examining transactions are based on the level of risk and, as a minimum, achieve the following:

- Identifying all high-risk customers to facilitate enhanced monitoring of accounts
- detecting unusual or suspicious transactions that are inconsistent with the economic profile of the Customer for further investigation;
- ascertaining the source and origin of the funds credited to accounts;
- investigating unusual or suspicious transactions from the employees who have been appointed for that purpose. It is noted that the results of the investigations are recorded in a separate memo and kept in the file of the Customer concerned. Based on the investigation findings, measures are taken, including internal reporting of suspicious transactions/activities to the Compliance Officer.

Automated electronic management information systems

The Company implements, where appropriate and proportionate, given the nature, scale and complexity of its business and the nature and range of the investment services and activities undertaken in the course of that business, adequate automated electronic management information systems which will be capable of supplying the Board of Directors and the Compliance Officer, on a timely basis:

a. All the valid and necessary information for the identification, analysis and effective monitoring of customer accounts and transactions based on the assessed risk for ML or T.F. purposes.
b. Monitoring accounts and transactions by periodically comparing the actual movement of the account with the expected turnover as declared at the establishment of the business relationship.
c. Monitoring of dormant accounts exhibiting unexpected movements.

d. Extract data and information missing regarding customer identification and construct a customer's economic profile.
e. Add up the movement of all related accounts on a consolidated basis and detect unusual or suspicious activities and types of transactions. This is done by setting limits for a particular type, or category of accounts (e.g. high-risk accounts) or transactions (e.g. deposits and withdrawals in cash, transactions that do not seem reasonable based on usual business or commercial terms, significant movement of the account incompatible with the size of the account balance), taking into account the economic profile of the Customer, the country of his origin, the source of the funds, the type of transaction or other risk factors.

The Company gives particular attention to transactions exceeding the abovementioned limits, which may indicate that a customer might be involved in unusual or suspicious activities.

Transactions executed for the Customer are compared and evaluated against the anticipated account's turnover, the usual turnover of the activities/operations of the Customer and the data and information kept for the Customer's economic profile. Significant deviations are investigated, and the findings are recorded in the respective Customer's file.

Transactions not justified by the available information on the Customer are thoroughly examined to determine whether suspicions over ML or T.F. arise for submitting an internal report to the Compliance Officer.

Change-driven updates of the C.D.D. may be triggered by:

Changes in terms of a business relationship with clients may include, amongst others, the following:

i. Changes in the shareholding structure
ii. Changes in the activities or turnover of a client that does not have a commercial rationale
iii. Enquiries and provision of new higher-risk services
iv. Changes in the nature of transactions of a client that cannot be explained
v. Set up of new corporate structures Suspicions,
vi. Changes in the Client's Beneficial Owner,
vii. Changes in services provided,
viii. Changes in professionals servicing the Client,
ix. Changes in general affairs,
x. Changes in line of business,
xi. Changes in the geographical area of operations,
xii. Changes in key management, and
xiii. Any other changes.

It is noted that the above list is not exhaustive.

Depending on the findings of ongoing monitoring procedures, the Company considers the reclassification of a client risk profile and, subsequently, the application of risk-appropriate due diligence measures. Sufficient guidance and training are given to staff members to enable them to monitor effectively. Scheduled/routine C.D.D. updates are carried out on a risk-sensitive basis. Hence the higher the risk, the more frequently the scheduled C.D.D. update is carried out.

Enhanced Due Diligence (E.D.D)

A risk-based approach to customer due diligence will identify situations that, by their nature, can present a higher risk of money laundering or terrorist financing, which means that the Company must obtain additional Customer due diligence information about the Client.

E.D.D. must be applied:

i. if a client has not been physically present for identification purposes, and if so, one or more additional measures must be taken to enhance due diligence, for example by, among other things, gathering additional documents, data, or information, or taking further steps to verify documents; or

ii. if a business relationship or occasional transaction is to be undertaken with a:

- politically exposed person (P.E.P.),
- family member or close associate of a P.E.P.;
- a beneficial owner of a customer, a third party for whom the Customer is acting or a beneficial owner of a third party for whom the Customer is a P.E.P. or family member or close associate of the P.E.P.; or
- person who is or has been entrusted with a prominent function by an international organisation, i.e., Director, Deputy Director and Member of the Board or equivalent functions.

In this case, the senior management will take the decision to approve, if possible, the relationship to be established after adequate measures have been taken to verify the source of wealth and funds which are involved and enhanced monitoring has been enacted to be actively conducted of any relationship entered into; and

iii. Where a related person has, or proposes to have, a business relationship with, or proposes to carry out an occasional transaction with, a person connected with a country that does not apply, or insufficiently applies, the FATF Recommendations.

iv. If any other situation, it can present a higher risk of money laundering and terrorist financing.

The Company performs the E.D.D. for higher-risk categories of customers, business relationships or transactions in the following way such as:

i. Requesting three (3) forms of identification documents, one (1) for identification and two (2) for verification.

ii. Obtaining due diligence reports from independent experts to confirm the veracity of the Customer due diligence information

iii. Requiring Board and senior management approval for higher-risk customers

iv. Requiring more frequent reviews of high-risk business relationships

v. Enhanced ongoing monitoring

In assessing the risks concerning money laundering and terrorist financing, the Company applies systems and controls that can appropriately identify and manage the enhanced risk associated with clients or transactions in or from countries prone to corruption, terrorism, or conflicts. The Company uses relevant findings issued by the FATF, the CFATF, the F.I.U. and the Financial Services Authority (F.S.A.). Additionally, in conducting its E.D.D., the Company ensures that it is aware of new or developing technologies that might favour anonymity and take measures to prevent its use for the purpose of money laundering and terrorist financing.

Establishing the source of wealth as part of Enhanced Due Diligence (E.D.D.)

Three steps we follow when establishing the source of wealth:

1. we obtain information on net worth
2. we obtain information on where that net worth came from
3. we verify the information on a risk-sensitive basis

Transfer Of Funds

In an effort to counter money laundering and other illegal activity, we have decided not to support any cash transactions, regardless of their stated purpose. Our Company has the right to cancel or deny a transaction at any point if there are suspicions regarding its legality.

All our transactions relating to deposits and withdrawals to and from the client accounts take place via bank wires through recognised and well-known banks and credit institutions using their internet and mobile banking facilities. Those banks are a mitigating measure we have added for safeguarding the additional preventive measures for money laundering, terrorist financing and proliferation financing via their own individual and independent from us KYC procedures, ongoing monitoring of the transactions and other related actions for the purposes of Anti-money laundering, Counter Terrorist financing and counter proliferation financing.

The Company does not gather, store, or process personal credit or debit card information. All payment transactions are processed through payment service providers.

When transferring money for purchasing digital currency, the sender's name and the information held on file should match. If there is any transaction discrepancy, we

reserve the right to cancel or suspend the transaction automatically. Money transfers from another party other than the account holder are strictly prohibited. Furthermore, we will refuse any third-party transfers towards one of our Clients. Similarly, third parties are forbidden to conduct the transaction to replace the Client.

Important Notes

- The Senior Management approval is mandatory before opening a "Politically Exposed Person" account.
- When a P.E.P. is a potential client, we need to obtain a bank reference letter.
- Where the documents are not in English:

We need a translation from a translator (external and/or an employee of the Company). If there is no one to translate the documents, we ask the Client to send us an official translation from a notary.

The Company has the right to refuse any client without giving a reason. This Policy and procedures have been implemented to protect the Company and its clients.

Non-Face To Face Business

When the Company conducts non-face-to-face business with clients that have not been physically present for identification and verification, it has policies, procedures, systems, and controls in place to manage specific risks associated with such non-face-to-face business, relationships, or transactions. (see Sections above)

Where the Company is approached via the internet, post, or telephone, it carries out non-face-to-face verification, either electronically or by reference to documents. The Company applies additional E.D.D. measures and undertakes enhanced ongoing monitoring, such as:

- Obtaining copies of identification documents which are certified by:

  • A member of the judiciary, a senior public servant
  • An officer of an embassy, consulate, or high commission of the country of issue of documentary evidence of Identity
  • A lawyer or notary public who is a member of a recognised professional body
  • An actuary who is a member of a recognised professional body
  • An accountant who is a member of a recognised professional body
  • A director, officer or manager of a regulated person or a branch or subsidiary of a group headquartered in a well-regulated jurisdiction

- Verifying additional aspects of Identity or other C.D.D. information from independent sources
- The Company ensures that adequate procedures for monitoring the activities of non-face-to-face businesses are implemented and managed effectively. Where a client is a legal person, the Company requires documentary evidence of the continuing existence of the legal person (certificate of good standing) and a certified copy of identification and address documentation to verify the address of any person defined therein. Contacting the Customer via telephone on a home or business number is verified before establishing a relationship or before transactions are permitted, using the call to verify additional aspects of identification information previously provided.

Suspicious Activity Reporting (S.A.R.s)

The Company routinely monitors for and tries to detect, if any, suspicious activity and examines the background and purpose of the following:

- Complex or unusually large transactions, which have no apparent visible economic or lawful purpose. This covers both completed and attempted transactions;
- Transactions outside the usual pattern of the Client's activity;
- Transactions that are deemed to be of high risk concerning a client or business relationship or as they relate to high-risk geography, products or services; and
- Transactions, clients, or business relationships that cause the Company to have reasonable grounds to suspect money laundering, terrorist financing or some other predicate offence.

The Company ensures that its directors, officers, and employees (permanent and temporary) are advised not to disclose to the subject or any other person that a S.A.R. or related information has been or will be reported or provided to the Compliance / Reporting Officer or the SVGFIU. This is considered an offence, tipping off and prejudicing an investigation.

Internal and external reporting

- Internal and external reporting

In light of the obligation to file Suspicious Activity Reports (S.A.R.s), the Company implements relevant internal policies, procedures, processes, and controls to detect money laundering and terrorist financing. This should enable employees to report to the Compliance/ Reporting Officer any suspicion or knowledge of money laundering, terrorist financing or other predicate offence identified.

The internal procedures clearly state what is expected of individuals who form suspicions or obtain such knowledge. The relevant personnel are aware of the internal procedures to be used, and all the necessary information is captured. Consideration should be given to minimising the number of copies of reporting information held within a business. Copies of third-party documents must supplement the report. S.A.R. forms can be found on the SVGFIU's website for external reporting to the F.I.U., which must be used when submitting an external S.A.R. to the SVGFIU.

The Compliance Officer is responsible for ensuring that every employee is aware of his/her role and duty to receive or submit internal suspicious activity reports.

In certain circumstances, where the Compliance Officer is unsure whether the matter amounts to suspicion, they are advised to err on caution and file the S.A.R. However, it should not be defensive filing, and all relevant supporting documents must be provided.

The Compliance Officer must assess suspicious activity internally and make an internal report outlining the outcome of his/her assessment, which should include the decision on whether or not to file an external S.A.R. with the SVGFIU. This practice would help protect the Company from situations where the Supervisory Authority is conducting onsite examinations and where a transaction is later flagged as suspicious either internally or externally.

The justification for such a decision must be recorded when the Compliance Officer concludes that no external report should be made.

The Company, via the AMLCO, will inform all employees of their obligation to report any suspicious activity to the Compliance/ Reporting Officer or to the SVGFIU, the failure of which constitutes an offence.

General Suspicious Activity/ Indicators

The following serves as general guidance to be observed by ALL COMPANY'S RELATED PERSONS in respect of identifying suspicious activity:

a) The Customer has an unusually comprehensive knowledge of money laundering issues and the A.M.L. Law without justification. For instance, if the Customer points out that he/she wishes to avoid being reported.

b) Attempts to divide the amounts of any operations below the applicable designated threshold of reporting to the competent authorities regarding money laundering or terrorist financing suspicion.

c) The Customer has an unusual interest in the internal policies, controls, regulations, and supervisory procedures and unnecessarily elaborates on justifying a transaction.

d) When a customer has accounts with several international banks or has lately established relationships with different financial institutions in a specific country without clear grounds, particularly if this country does not apply an acceptable AML/CFT regime.

e) The Customer is reserved, anxious or reluctant to have a personal meeting.

f) The Customer uses different names and addresses.

g) The Customer requests or seeks to carry out the transactions without disclosing his Identity.

h) The Customer refuses to submit original documentation, including those related to his identification.

i) The Customer intentionally conceals essential information like his address (actual residence) and telephone number or gives a non-existent or disconnected telephone number.

j) The Customer uses a credit card issued by a foreign bank with no branch/headquarters in the Client's country of residence while he/she does not reside or work in the country that issued the said card.

k) Unusual transactions in comparison with the volume of the previous transactions or the activity pursued by the Customer

l) Unnecessarily complex transactions or those that do not seem to have economic feasibility.

m) Transactions involving a country that does not have an efficient AML/CFT regime are suspected of facilitating money laundering operations or where drug manufacturing or trafficking is widespread.

Risk-Based Approach

Our Company implements a risk-based approach regarding its A.M.L. and CTF procedures. We use the risk factors they identified to assess the overall level of ML/TF risk, as mentioned in Appendix 3 for those factors indicating a lower and Appendix 4 for those indicating a higher risk of ML/TF.

Our Company classifies after it collects customer information into the following risk categories and performs either normal or Enhanced due diligence on a per-case basis. The risk score considers the factors of Appendix 3 and 4, the information of the Client provided via a form relating to personal data and information requested for constructing his/her economic profile as described above, ongoing information received and information received from outsourced service providers who perform documents verification, checks whether the person relates with a Politically exposed person and whether the person it is included in Sanctions lists and/or whether there are adverse media available for this person, on a frequent basis. Also, the third party performs biometric checks during the onboarding stage for the Client.

Risk Category based on the risk score	Actions of the Company
Low	Accept the Client and perform Simplified due diligence
Medium to Low	Accept the Client and perform Normal due diligence
Medium	Accept the Client and perform Normal due diligence
Medium to High	Accept the Client and perform Enhanced due diligence
High	Reject the Client
Very High	Reject the Client

Our Company does not onboard clients:

a. Who has a risk score indicating either a high or a very high risk of Money Laundering and/or Terrorist financing risks,
b. Who is included in the sanctions lists of the United Nations and the United States of America,
c. Who are politically exposed persons, or they are close family members and/or associates with politically exposed persons.

As a Company, we take a holistic view of the ML/TF risk factors we have identified that will determine the level of ML/TF risk associated with a business relationship, an occasional transaction, or our business.

When weighing risk factors, our Company ensures that:

- weighting is not unduly influenced by just one factor;
- economic or profit considerations do not influence the risk rating;
- weighting does not lead to a situation where it is impossible for any business relationship to be classified as high-risk;
- the firm's weighting cannot overrule national legislation regarding situations that always present a high money laundering risk; and
- It can override any automatically generated risk scores where necessary.

The rationale for the decision to over-ride such scores is documented appropriately

When identifying the risk associated with our Customers, including their customers' beneficial owners, we consider the risk related to the Customer's and the Customer's beneficial owner's business or professional activity; the Customer's and the Customer's beneficial owner's reputation; and the customer's and the Customer's beneficial owner's nature and behaviour, including whether this could point to increased T.F. risk.

When identifying the risk associated with countries and geographical areas, we consider the risk related to the jurisdictions in which the Customer is based or is a resident and the beneficial owner is a resident; the jurisdictions that are the Customer's and beneficial owner's main places of business; and the jurisdictions to which the Customer and beneficial owner have relevant personal or business links, or financial or legal interests.

When identifying the risk associated with our products, services, or transactions, we consider the risk related to the level of transparency, or opaqueness, the product, service, or transaction affords; the complexity of the product, service, or transaction; and the value or size of the product, service, or transaction.

When identifying the risk associated with the way in which the Customer obtains the products or services they require, we consider the risk related to a) the extent to which the business relationship is conducted on a non-face-to-face basis; and b) any introducers or intermediaries, the firm might use and the nature of their relationship with the firm.

Record Keeping

We only keep personal data if it is necessary to accomplish the goals for which it was initially collected, including meeting any legal, tax, accounting, regulatory, technical, or reporting requirements. In the event of a complaint or if there may be a chance of litigation involving our relationship with you, we may keep your personal information for longer.

When determining the proper retention period for personal data, we take into account several factors, including the volume, nature, and sensitivity of the data, the risk of harm from unauthorised use or disclosure, the purposes for which we process the data, and whether those purposes can be fulfilled by other means, as well as any applicable legal, regulatory, tax, accounting, or other requirements.

For compliance reasons with this Policy, we retain our customers' basic information (including contact details, identity card, financial information, and transaction data) for a minimum of seven (7) years after the end of our business relationship with the Client or after the last occasional transaction performed. Assessment of client documents will be made on an annual basis. When the Company determines that personal information is no longer required for the purpose for which it was collected, the Company has the right to delete all data received from the Client.

All client documents and record transactions will be kept safe and backed up for a minimum seven (7) year period after the end of our business relationship and/or the performance of an occasional transaction.

Our Company keeps records of clients' or customers' identity, the supporting evidence of verification of Identity (in each case including the original and any updated documents), all account files, its business relationships (including correspondence) with them and details of any occasional transactions and monitoring of the relationship. We ensure the retention of historical as well as current records for any reference in the future.

Our Company securely stores information relating to both internal and external reports for at least seven years after receipt.

Our Company keeps all records following the relationship's establishment or the transaction's completion, regardless of whether the account or business relationship is ongoing or has been terminated.

Our Company maintains records of the annual compliance report and any other reports highlighting compliance, deficiencies, and actions, including reports submitted to senior management.

Audit Function

The internal audit department reviews and assesses every amount that flows in or out of the Company via deposits and withdrawals to and from the client trading accounts. For any withdrawal amount, it assesses all the trading account transactions, the Client's documentation, and whether it is up to date before providing the final approval for releasing the funds to the Client's bank account. If the deposits exceed 15,000 United States Dollars, it requests the Source of Funds as described in Appendix 5.

The internal audit department of the Company reviews and evaluates, at least on an annual basis, the appropriateness, effectiveness and adequacy of the Policy, practices, measures, procedures, and control mechanisms applied to prevent money laundering and terrorist financing. The findings and observations of the internal auditor are submitted, in a written report form, to the Board of directors, which decides the necessary measures that need to be taken to rectify any weaknesses and/or deficiencies detected. The minutes of the abovementioned decision of the Board of directors and the internal auditor's report are kept for internal purposes and form the primary source for updating the risk-based compliance monitoring schedule for the following year.

Internal Audit

The scope of the Internal Audit Examination (from outsourced entities on top of the internal team) covers the accuracy of customer identification information, suspicious transaction reports, and all other records and internal controls about compliance with AML/CFT obligations. Internal audits from outsourced entities are conducted at least once (1) every year or at such frequency as necessary, consistent with the company's risk assessment. Internal audits from the internal team take place in every transaction relating to the funding department, as required to be compatible with the company's risk assessment.

External Audit

Independent External Audit Examinations are conducted once every year or at such frequency as necessary, consistent with the Company's risk assessment. This audit is performed by a licensed third party to complete this task.

The internal and external audit results shall be timely and directly communicated to the Company's Board of Directors, the senior management, partners, or sole proprietor, as the case may be, and the compliance officer. There shall also be a written procedure by which deficiencies in a compliance program are promptly remedied once identified by either the internal or external audit. Moreover, audit results relative to AML/CFT compliance shall quickly be made available to the F.I.U. upon request.

GENERAL INFORMATION

Amendments to this Policy

- The Company retains the right to periodically review and modify this Policy for any reason and to provide notice of any such modifications to Clients by posting an updated version of this Policy on the Company's website (s).

- The Company will occasionally update and/or amend this Policy statement to reflect Company and user/client feedback and keep it in line with legal requirements. The Company encourages you to review this statement periodically to keep yourself informed of how the Company protects your information.

- You can always stay informed about the data we collect, how we use it, and when we disclose it by checking back on this page whenever this Policy Statement is updated or amended.

- The Client must regularly review the Policy and any updates to it.

Enquiries and Contact Details

- For any general enquiries regarding this Policy, do not hesitate to contact the Company by emailing the Customer Support Department at support@connextfx.com.

- The Company welcomes your comments and feedback regarding this Policy statement. If you believe that the Company has not adhered to this statement, do not hesitate to contact the Company as per the Terms of Service and Conditions, Article 19. We shall use all reasonable efforts to determine and remedy the matter promptly.

Appendices

Appendix 1

Jurisdictions with strategic deficiencies as per FATF[1]

1. Albania
2. Barbados
3. Burkina Faso
4. Cambodia
5. Cayman Islands
6. Democratic Republic of the Congo
7. Gibraltar
8. Haiti
9. Jamaica
10. Jordan
11. Mali
12. Morocco
13. Mozambique
14. Panama
15. Philippines
16. Senegal
17. South Sudan
18. Syria
19. Tanzania
20. Turkiye
21. Uganda
22. United Arab Emirates
23. Yemen

[1] https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-october-2022.html

Appendix 2

High-Risk Jurisdictions subject to a Call for Action

1. Democratic People's Republic of Korea (DPRK)
2. Iran
3. Myanmar

Appendix 3

Risk Factors indicating lower risk

Lower risk	Types of evidence of potentially lower risk:
Customer risk factors:	(a) Public companies listed on a stock exchange and subject to disclosure requirements, either by stock exchange rules or through Law or enforceable means, which impose requirements to ensure adequate transparency of beneficial ownership (b) public administrations or enterprises (c) customers that are residents in geographical areas of lower risk as set out in paragraph (3)
Product, service, transaction, or delivery channel risk factors:	(a) life insurance policies for which the premium is low (b) insurance policies for pension schemes if there is no early surrender option and the Policy cannot be used as collateral (c) a pension or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme (d) financial products or services that provide appropriately defined and limited services to certain types of customers to increase access for financial inclusion purposes (e) products where other factors, such as purse limits or transparency of ownership, such as certain types of electronic money, manage the risks of money laundering and terrorist financing
Geographical risk factors:	(a) Member States of the European Union (b) third countries having effective AML/CFT systems (c) third countries identified by credible sources as having a low level of corruption or other criminal activity (d) third countries, based on credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the revised FATF Recommendations and effectively implement those requirements.

Appendix 4

Risk Factors indicating higher risk

High Risk	Types of evidence of potentially higher risk:
Customer risk factors:	(a) the business relationship is conducted in unusual circumstances (b) customers that are residents in geographical areas of higher risk, as set out in paragraph (3) (c) legal persons or arrangements that are personal asset-holding vehicles (d) companies that have nominee shareholders or shares in bearer form (e) cash-intensive businesses (f) The ownership structure of the Company appears unusual or excessively complex, given the nature of the Company's business
Product, service, transaction, or delivery channel risk factors:	(a) private banking (b) products or transactions that might favour anonymity (c) non-face-to-face business relationships or transactions without certain safeguards, such as electronic signatures (d) payment received from unknown or unassociated third parties (e) new products and new business practices, including new delivery mechanisms and the use of new or developing technologies for both new and pre-existing products
Geographical risk factors:	(a) countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems (b) countries identified by credible sources as having significant levels of corruption or other criminal activity (c) countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations and the United States of America (d) countries providing funding or support for terrorist activities or that have designated terrorist organisations operating within their country.

Appendix 5

List of examples of appropriate information and/or supporting documentation required to establish the Source of Wealth and Funds

Source of funds/wealth	Information / Documents that may be required
Employment Income	- Nature of employer's business - Name and address of the employer - Annual salary and bonuses for the last couple of years - Last month/recent pay slip - Confirmation from the employer of annual salary - Latest accounts or tax declaration if self employed
Savings / deposits	Bank statement and enquiry of the source of wealth
Property Sale	- Details of the property sold (i.e. address, date of sale, sale value of property sold, parties involved) - Copy of contract of sale - Title deed from land registry
Sale of shares or other investment	- Copy of contract - Sale value of shares sold and how they were sold (i.e. name of stock exchange) - Statement of account from agent - Transaction receipt/confirmation - Shareholder's certificate - Date of sale

Source of funds/wealth	Information / Documents that may be required
Gift	- Date received - Total amount - Relationship to client - Letter from donor explaining the reason for the gift and the source of donor's wealth - Certified identification documents of donor - Donor's source of wealth
Maturity/surrender of life policy	- Amount received - Policy provider - Policy number/reference - Date of surrender
Other income sources	- Nature of income, amount, date received and from who - Appropriate supporting documentation

Source of funds/wealth	Information / Documents that may be required
Loan	- Loan agreement - Amount, date and purpose of loan - Name and address of Lender - Details of any security
Company Sale	- Copy of the contract of sale - Internet research of Company Registry - Name and Address of Company - Total sales price - Clients' share participation - Nature of business - Date of sale and receipt of funds - Media coverage
Company Profits / Dividends	- Copy of latest audited financial statements - Copy of latest management accounts - Board of Directors approval - Dividend distribution - Tax declaration form
Inheritance	- Name of deceased - Date of death - Relationship to client - Date received - Total amount - Solicitor's details - Tax clearance documents