Easy Crypto SA (Pty) Ltd t/a
EasyCrypto
Registration number 2018/351198/07
(“the Company”)

Anti-money laundering and counter-terrorist financing Risk Management and Compliance Programme (“the RMCP”)

1. Policy approval and information

Policy owner	Board of directors
Policy type	Compliance
Policy drafter	Gigi Vorlaufer
Policy reviewer	Gigi Vorlaufer
Policy creation date (1st version)	November 2020
Policy review date (this version)	July 2021
Approver's signature	
Approved by (this version)	Earle John Loxton
Adopted by (this version)	Board of directors
Approval date (this version)	2021-07-06
Approval date (1st version)	2020-11-11
Version number	V01.05

Summary of policy history

Version number	Drafted/adapted/reviewed by	Creation/review date	Approved by	Approval date
V01.01	Gigi Vorlaufer (generic draft)	August 2019	N/A	N/A
V01.02	Adapted for the Company	November 2020	Earle Loxton	2020-11-11
V01.03	Gigi Vorlaufer: reliance agreements included	January 2021	Earle Loxton	2021-01-20
V01.04	Registered company name changed	April 2021	Earle Loxton	2021-04-21
V01.05	Insert reference to EC10 bundle	July 2021	Earle Loxton	2021-07-06

2. Purpose and scope

The FICA Risk Management and Compliance Programme (the **RMCP**, or the **Policy**) is prescribed in terms of section 42 of the Financial Intelligence Centre Act 38 of 2001, as amended (the **FICA**). Every accountable institution (**AI**) must develop, document, maintain, and implement, a programme for anti-money laundering, and counter-terrorist financing risk management. The Company is a **crypto assets service provider (CASP)**. Currently, the Company is not required to be registered as an AI, because **CASPs** are not defined as AIs, in terms of the FICA.

The Company has voluntarily applied the obligations applicable to AIs, because it is a CASP, and it wants to proactively implement a risk-based approach to mitigate the risk of the Company being used for money laundering and/or terrorist financing. This approach is aligned with the fact that the **Financial Action Task Force** (**FATF**) has assessed that money laundering, and terrorist financing, risks exist for crypto assets, and the related activities thereto. The **FATF** has updated its Standards, by amending Recommendation 15 (relating to new technologies). The obligations specified within Recommendation 15 require member countries to assess, and mitigate, their risks associated with crypto asset activities, and CASPs; license, or register, CASPs, and subject them to supervision, or monitoring, by competent national authorities. Member countries will not be permitted to rely on a self-regulatory body for supervision, or monitoring; and member countries must implement sanctions, and other enforcement measures, when CASPs fail to comply with their obligations; and underscore the importance of

international cooperation. Some countries may decide to prohibit crypto asset activities, based on their own assessment of the risks, and regulatory context, or to support other policy goals. South Africa is a FATF member, so it is obliged to adhere to the FATF recommendations. For those reasons, the proposed amendments to the FICA will include CASPs being included as AIs.

Currently, in South Africa, crypto assets are unregulated. Therefore, the members of the **Intergovernmental Fintech Working Group** (the **IFWG**) established a Crypto Assets Regulatory Working Group (CAR WG), to formulate a coherent, and comprehensive, policy stance on crypto assets, while ensuring the continued integrity, and efficient functioning, of financial markets, maintaining financial stability, protecting the rights, and interests, of customers, and investors, and combating illegitimate cross-border financial flows, anti-money laundering, and counter-terrorist financing. Therefore, in the near future, it is likely that crypto assets, and CASPs, will be incorporated into the financial institutions legislation, by incorporating it into the Conduct of Financial Institutions Bill (the **COFI Bill**), and the related legislation, and subordinate legislation. At that stage, crypto assets will become regulated in South Africa. Until legislation is amended, it is prudent for CASPs to self-regulate, and voluntarily apply stricter control measures, in accordance with legislation. Amongst other things, this will assist CASPs to mitigate the risk of their businesses being used for money laundering, and terrorist financing.

The purpose of this Policy is to provide the:

2.1. foundation of the programme, to enable the Company to identify, assess, monitor, mitigate and manage the risk that the providing of financial products and services by the Company may involve, or facilitate, money laundering activities, or the financing of terrorist and related activities.

2.2. way the Company determines if a person is a prospective client, in the process of establishing a business relationship, or entering into a single transaction, with the Company, or is an existing client, who has established a business relationship, or entered into a single transaction.

2.3. way the Company ensures that it does not establish a business relationship, or conclude a single transaction, with an anonymous client, or a client with an apparent false or fictitious name.

2.4. way the Company establishes and verifies the identity of the persons whom it must identity, in terms of the customer due diligence requirements, and the processes it uses.

2.5. way the Company performs the customer due diligence requirements relating to identifying persons whom it must identify, understanding and obtaining information about the business relationship, additional due diligence measures for legal persons, trusts and partnerships, and ongoing due diligence, when it suspects that a transaction, or activity, is suspicious, or unusual, during the business relationship.

2.6. way 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.

2.7. way the Company performs additional customer due diligence measures for legal persons, trusts and partnerships, and the processes it uses.

2.8. way the Company performs ongoing due diligence and account monitoring of business relationships, and the processes it uses.

2.9. way the Company examines complex, or unusually large, transactions, and unusual patterns of transactions, which have no apparent business, or lawful, purpose, and keeps written findings thereof.

2.10. way the Company confirms information about a client, when the Company has doubts about the accuracy of previously obtained information, and the processes it uses.

2.11. way the Company will terminate a business relationship, when it is unable to conduct the customer due diligence.

2.12. way the Company determines whether a prospective client is a foreign prominent public official (**FPPO**), or a domestic prominent influential person (**DPIP**), and the processes it uses.

2.13. way the Company performs enhanced due diligence for higher-risk business relationships and determines when it permits simplified customer due diligence.

2.14. way the Company keeps records and the place where the records are kept.

2.15. criteria to enable the Company to determine when a transaction, or activity, is reportable to the Centre.

2.16. processes for reporting information to the Centre.

2.17. way the RMCP is implemented in branches, subsidiaries, or other operations of the Company, in foreign countries, to enable the Company to comply with its obligations under the FICA.

- **This requirement IS NOT applicable to the Company, because it has no foreign branches, subsidiaries, or operations.**

2.18. way the Company determines if the host country of a foreign branch, or subsidiary, permits the implementation of measures required under the FICA.

- **This requirement IS NOT applicable to the Company, because it has no foreign branches, subsidiaries, or operations.**

2.19. way the Company will inform the Centre and supervisory body, if the host country does not permit the implementation of measures required under the FICA.

- **This requirement IS NOT applicable to the Company, because it has no foreign branches, subsidiaries, or operations.**

2.20. processes for the Company to implement its RMCP.

2.21. Board of directors to approve the RMCP.

2.22. processes for the Company to review its RMCP at regular intervals, to ensure the RMCP remains relevant to its operations and achieving the requirements.

2.23. processes for the Company to make documents describing its RMCP, available to each employee involved in transactions to which the FICA applies.

2.24. processes for the Company to make documents describing its RMCP, available to the Centre or a Supervisory body, which performs regulatory or supervisory functions for the Company.

This policy is applicable to the Company, and all employees of the Company. The Company's Board requires all employees to fully comply with the processes, and procedures, contained in the RMCP. Any gross negligence, or wilful non-compliance, with the provisions of the FICA and/or the processes, and procedures, contained within the Company's RMCP, will be considered a serious form of misconduct, which may result in a summary dismissal.

This policy is supplemented, and supported, by the relevant procedures, systems, and controls, implemented within the Company, which together comprise the RMCP.

3. Legislative framework

The reference to legislation, subordinate legislation and supervision documents includes amendments made from time to time.

- Financial Sector Regulation Act 9 of 2017 (the FSRA)
- Conduct of Financial Institutions Bill (the COFI)
- Financial Intelligence Centre Act 38 of 2001 (the FICA), regulations thereto, compliance and guidance documents
- Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 of 2004 (the POCDATARA)
- Prevention of Organised Crime Act 121 of 1998 (the Prevention Act)
- Prevention and Combating of Corrupt Activities Act 12 of 2004 (the PCCAA)
- FATF Recommendations, published by the Financial Action Task Force (the FATF) and guidance documents

4. Definitions and abbreviations

The below key definitions, and abbreviations, are used in this policy. Other terms may be defined elsewhere in this Policy.

4.1. **Accountable Institution (AI)** means entities that have specific compliance obligations in terms of the FICA. The affected entities are listed in Schedule 1 of the FICA.

- **The Company is not an AI, but in respect of being a CASP, it has voluntarily applied the obligations applicable to AIs**.

4.2. **Crypto asset** means a digital representation of value that is not issued by a central bank, but is traded, transferred, and stored, electronically, by natural, and legal, persons, for the purpose of payment, investment, and other forms of utility, and applies cryptography techniques in the underlying technology. The definition of crypto asset includes a stablecoin (and global stablecoin), which is a crypto asset designed to maintain a stable value, relative to another asset (typically a unit of currency, or commodity), or a basket of assets. A global stablecoin is a stablecoin with a potential global reach, and which can rapidly scale in terms of the users/holders of the crypto asset. A crypto asset is purchased for different reasons, such as speculative investing (a perceived increased future value), as a medium of exchange in facilitating transactions for goods and/or services, or for access to specific products, services, and utilities. Crypto assets can also be purchased for the specific purpose of on-selling or trading. Crypto asset is a broader, or umbrella, term for different crypto asset tokens.

Crypto asset tokens (tokens) are either fungible, or non-fungible. Fungible crypto asset tokens (each token is the same, and no token has a special value) may be classified into three types:

- **Exchange/payment token**: token designed to be used as a means of exchange, or payment, for buying goods and services. Some users utilise it for investment purposes. Examples include Bitcoin (BTC), Litecoin, Dash, Bitcoin Cash, Monero, Zcash, and ERC-20.
- **Security token**: token that provides rights, such as ownership, the repayment of a specific sum of money, or entitlement to a share in future profits. Examples include ERC-20.
- **Utility token**: token that can be redeemed for access to a specific product, or service, which is typically provided using a distributed ledger technology (DLT) platform. Examples include Ether (ETH), and ERC-20.

Non-fungible crypto asset tokens (each token is unique) may be classified into three types:

- **Certification token**: token used to prove the origins of a document, piece of data, or even a physical object in the real world. The anti-counterfeit nature of non-fungible tokens lends itself well to certifying the authenticity of various types of information and content.
- **Digital identity token**: token used for digital personhood. You would not be able to trade identity tokens, but you would be able to share the UTXO of their issuance with anyone who wanted to verify your identity on the blockchain. Each of these tokens would exist digitally on a universal blockchain, but they would belong distinctly to you. Some work is needed to obfuscate the identity details contained in these tokens, so that only those with permission can access the information. However, theoretically your whole identity could live on a blockchain, and you could pick and choose what to share with who, and when.
- **Identity of things token**: token used to digitally identify objects, devices, and machines. This identity of things (IDoT) is a major step on the road to blockchain-based supply chains, IoT applications, and smart cities.

Crypto assets can be purchased from:

- crypto asset trading platform (South African, or foreign), or any other entity facilitating, or providing, the mentioned services
    - A variation of a crypto asset trading platform is a decentralised exchange, which uses an artificial intelligence (AI) system that can connect crypto asset traders electronically. These trades are done simultaneously, through an atomic swap, using a smart contract, and without any intermediation from a third party.
- crypto asset vending machine
    - The crypto asset vending machine allows the user to make a physical deposit, or an electronic deposit, using fiat currency that is credited to a crypto asset digital wallet. The operator of these machines acts as the counterparty to all transactions.
- bilateral transactions with other existing holders (peer-to-peer transactions)
    - The buyer may require a crypto asset digital wallet to acquire crypto assets, which can be obtained through software platforms, or can be provided by a crypto asset digital wallet service provider, or a crypto asset trading platform.

4.3. **Crypto asset service provider (CASP)** means a person that provides services for crypto assets, including businesses that exchange crypto assets for fiat currencies, or *vice versa*, conduct transactions that move crypto assets from one crypto asset address, or account, to another, provide facilities for the safekeeping, or administration, of crypto assets, or instruments, which enable the control of crypto assets, and participate in, or provide, financial services for issuers' offers, or sale, of crypto assets. The crypto asset services provided by CASPs include:

- **crypto asset trading platform** (or any other entity facilitating, or providing, the mentioned services)
    - **intermediary services for the buying, and selling, of crypto assets**
    - **trading, conversion, or exchange, of fiat currency, or other value, into crypto assets**
    - **trading, conversion, or exchange, of crypto assets, into fiat currency, or other value**
    - **trading, conversion, or exchange, of crypto assets, into other crypto assets**
    - remittance services using crypto assets as a means of facilitating credit transfers (remitter, or value transfer provider)
- crypto asset vending machine provider
    - intermediary services for the buying, and selling, of crypto assets (including any of the above-mentioned services)
- crypto asset token issuer
    - initial coin offering (ICO), including security, payment/exchange, or utility, tokens
    - issuance of stablecoins
    - issuance of global stablecoins
    - participation in, and provision of, financial services related to an issuer's offer, or sale, of crypto assets

- **crypto asset fund, or derivative, service provider**
  - **offer investment funds, or derivative products, with crypto assets as the underlying asset**
- crypto asset digital wallet provider (custodial wallet)
  - offer a software program, with the ability to store private, and public, keys that are used to interact with various digital protocols, which enable the user to send, and receive, crypto assets, with the additional ability to monitor balances, and execute control over the clients' crypto assets
- crypto asset safe custody service provider (custodial service)
  - safeguard, store, hold, or maintain, custody of crypto assets belonging to another party

4.4. **Crypto asset digital wallet** means a software program with the ability to store private, and public, keys that are used to interact with various blockchain protocols that enable the user to send, and receive, crypto assets, with the ability to monitor balances.

4.5. **Administrative sanction** means an administrative sanction, as contemplated in section 45C of the FICA (refer to **Annexure 1** of this policy).

4.6. **Non-compliance (also non-compliant, fails to comply, failure to comply)** means any act, or omission, that constitutes a failure to comply with a provision of the FICA, or any order, determination, or directive, made in terms of the FICA and which does not constitute an offence in terms of the FICA.

4.7. **Beneficial owner**, in respect of a **legal person**, means a natural person who, independently, or together with another person, directly, or indirectly, owns the legal person, or exercises effective control of the legal person.

4.8. **Business relationship** means an arrangement between a **client** and an **AI**, for the purpose of concluding transactions regularly.

4.9. **Client** means a person who has entered into a **business relationship**, or a **single transaction**, with an **AI**.

4.10. **Single transaction** means a transaction, other than a transaction concluded in the course of a **business relationship**, AND where the value of the transaction is not less than the amount prescribed **(currently R5,000.00)**, except in the case of section 20A of the FICA (anonymous clients and clients acting under false or fictitious names).

4.11. **Cash** means coin, paper money and travellers' cheques.

4.12. **Centre, or FIC**, means the Financial Intelligence Centre, established by section 2 of the FICA.

4.13. **Domestic prominent influential person (DPIP)** means a person referred to in Schedule 3A of the FICA (refer to **Annexure 2** of this policy).

4.14. **Foreign prominent public official (FPPO)** means a person referred to in Schedule 3B of the FICA (refer to **Annexure 3** of this policy).

4.15. **Money laundering, or money laundering activity (ML)**, means an activity to (or is likely to) conceal or disguise the illegal nature, source, location, disposition, or movement of the proceeds of unlawful activities, or any interest that anyone has in these proceeds, and includes activities that constitute an offence in terms of section 64 of the FICA or sections 4,5, or 6 of the Prevention Act.

4.16. **Proceeds of unlawful activities**, in terms of section 1 of the Prevention Act, means any property, or any service, advantage, benefit, or reward, which was derived, received, or retained, directly or indirectly, in

South Africa or elsewhere, at any time, in connection with, or as a result of, any unlawful activity, carried on by any person, and includes any property representing property so derived.

4.17. **Property**, in terms of section 1 of the Prevention Act, means money, or any other movable, immovable, corporeal, or incorporeal thing, and includes any rights, privileges, claims and securities, and any interest therein, and all proceeds thereof.

4.18. **Terrorist and related activities** means, as defined in section 1 of POCDATARA, the collection or provision of funds, with the intention to be used, or knowing that it will be used, to commit an act regarded as a terrorist act. Property connected to terrorist financing includes money or any other movable, immovable, or corporeal, thing, rights, privileges, claims, securities, interests therein, proceeds thereof, relating to terrorist financing.

4.19. **Terrorist financing (TF)** means the financing of terrorist and related activities.

4.20. **Legal person** means any person, other than a natural person, that establishes a **business relationship**, or enters into a **single transaction**, with an AI, and includes a person incorporated as a company, close corporation, foreign company, or any other form of corporate arrangement, or association, but excludes a **trust**, partnership, or sole proprietor.

4.21. **Trust** means a trust defined in section 1 of the Trust Property Control Act 57 of 1988, other than a trust established by virtue of a testamentary disposition, by virtue of a court order, in respect of persons under curatorship, by the trustees of a retirement fund for the benefits payable to the beneficiaries of that retirement fund, and includes similar arrangements established outside South Africa.

4.22. **Risk Management and Compliance Programme (the RMCP, or Policy)**, means the programme for anti-money laundering and counter-terrorist financing risk management, which every AI must develop, document, maintain and implement, as prescribed in terms of section 42 of the FICA.

4.23. **Cash threshold report (CTR)** means a report that must be submitted to the Centre, by accountable and reporting institutions, in terms of section 28 of the FICA, concerning a cash transaction concluded with a client (paid to, or received from, a client, or a person acting on behalf of a client), in excess of the prescribed amount **(currently R24,999.99, or an aggregate of smaller amounts that combine to exceed this amount), within 2 days of becoming aware**.

4.24. **Suspicious or unusual activity report (SAR)** means a report that must be submitted to the Centre, by an accountable and reporting institution, in terms of section 29(1) and (2) of the FICA, concerning proceeds of unlawful activities, or money laundering, relating to an activity that **does not involve a transaction** between two or more parties, or relating to a transaction, or series of transactions, about which enquiries are made, but which has not been concluded, **within 15 days of becoming aware**.

4.25. **Suspicious or unusual transaction report (STR)** means a report that must be submitted to the Centre, by an accountable and reporting institution, in terms of section 29(1) of the FICA, concerning proceeds of unlawful activities, or money laundering, **relating to a transaction, or series of transactions**, between two or more parties, **within 15 days of becoming aware**.

4.26. **Terrorist financing activity report (TFAR)** means a report that must be submitted to the Centre, by an accountable and reporting institution, in terms of section 29(1) and (2) of the FICA, concerning the financing of terrorism and related activities, relating to an activity that does not involve a transaction between two, or more, parties, or relating to a transaction, or series of transactions, between two or more parties, **within 15 days of becoming aware**.

4.27. **Terrorist financing transaction report (TFTR)** means a report that must be submitted to the Centre, by an accountable and reporting institution, in terms of section 29(1) of the FICA, concerning the financing of terrorism and related activities, relating to a transaction, or series of transactions, between two, or more, parties, **within 15 days of becoming aware**.

4.28. **Terrorist property report (TPR)** means a report that must be submitted to the Centre, by an AI, in terms of section 28A of the FICA, concerning property associated with terrorist and related activities and financial sanctions pursuant to Resolutions of United Nations Security Council, **within 5 days of becoming aware**.

4.29. **Reporting institution** means a person with reporting obligations in terms of the FICA, referred to in Schedule 3 of the FICA, which persons are currently:

- Motor vehicle dealers
- Kruger rand dealers

4.30. **Supervisory body** means a functionary or institution referred to in Schedule 2 of the FICA, currently:

- Financial Sector Conduct Authority
- South African Reserve Bank
- Estate Agency Affairs Board
- Independent Regulatory Board for Auditors
- National Gambling Board and Provincial licensing authority, in terms of the National Gambling Act
- Law society, in terms of the Attorneys Act

4.31. **Reliance agreement** means an agreement that sets out the duties and obligations of the first party accountable institution, and the third party accountable institution, where the third party accountable institution provides shared client information to the first party accountable institution, for establishing, and verifying, the identity of the shared clients.

4.32. **First party accountable institution** means the AI that receives customer due diligence documents and/or information about the shared client from the third party accountable institution.

4.33. **Third party accountable institution** means the AI that has collected the customer due diligence documents and/or information about the shared client, and provides this information and/or documents to the first party accountable institution.

4.34. **Shared client** means the shared clients of both the first party accountable institution and the third party accountable institution, for a single transaction, or business relationship. For the sake of clarity, a shared client is not a client of both the first party accountable institution and the third party accountable institution, coincidentally, and is not the underlying clients of the shared client.

4.35. **Shared client information** means the information, or documents, obtained during the initial CDD process, relating to identifying, and verifying, the shared client, and the other people involved in the business relationship, and source of funds, source of wealth, and geographic location. Shared client information excludes the screening, and risk rating, aspects of the initial CDD process, the entire ongoing CDD process performed for existing clients, and the reporting obligations.

5. Roles and responsibilities

5.1. **Board of directors (Board)** maintains overall responsibility for the Policy, which may be delegated to the relevant stakeholders for implementation. The **Board must approve the RMCP**, and ensure compliance with this Policy, and must have an overview of the general, and specific, compliance requirements.

5.2. **Executive committee (Exco)** is the most senior management team within the Company. It is responsible for drafting, and implementing, this Policy, and for submitting it to the Board, for approval. It must ensure that all employees, and associates, are aware of the Policy, and understand the contents thereof, and provide training, and awareness, to facilitate this. The Exco may delegate the implementation thereof to line management.

5.3. **Governance structure**
The Company must have governance structures in place, to ensure compliance with this Policy. The Board, and the relevant Board Committees, which may include a Risk Committee and Audit Committee, must have an overview of the general, and specific, compliance requirements.

5.4. **Compliance officers (compliance function)** must monitor compliance with this Policy, and report non-compliance to the Board, the Exco, and any other relevant components of the governance structure. They must provide ongoing guidance, and training, to employees, to assist them to comply with, and understand, their obligations, in terms of the FICA, and the Policy.

5.5. **Person responsible for submitting reports to the Centre (responsible person)**, or his/her alternatives, if the responsible person is not available, must submit reports to the Centre, as required.

5.6. **Employees** must ensure that they understand this Policy, and always comply with it. Employees must be cognisant of the consequences of non-compliance with the Policy.

6. Nature of business

6.1. The Company is a CASP, providing services that are limited to:

- **crypto asset trading platform** (or any other entity facilitating, or providing, the mentioned services)
  - **intermediary services for the buying, and selling, of crypto assets**
    - The Company performs intermediary services for the buying and selling of the crypto assets that it offers.
  - **trading, conversion, or exchange, of fiat currency, or other value, into crypto assets**
    - The Company's clients may buy BTC, ETH, or the **EC10 bundle**, in exchange for South African Rands (ZAR).
    - The EC10 bundle is a basket of cryptocurrencies, which grants clients access to a low-cost index instrument, to easily own, and manage, a diversified crypto asset portfolio.
  - **trading, conversion, or exchange, of crypto assets, into fiat currency, or other value**
    - The Company's clients may sell their holding in BTC, ETH, or the EC10 bundle, to receive ZAR.
  - **trading, conversion, or exchange, of crypto assets, into other crypto assets**
    - The Company's clients may sell their holding in the EC10 bundle, to receive BTC.
- **crypto asset fund**, or derivative, **service provider**
  - **offer investment funds**, or derivative products, **with crypto assets as the underlying asset**
    - The EC10 bundle comprises the top 10 cryprocurrencies, weighted by market capitalisation, including BTC, ETH, ERP, and 7 others.
    - Clients own the EC10 bundle, and the underlying cryptocurrencies held within the EC10 bundle.
    - When buying the EC10 bundle, the client automatically buys the underlying cryptocurrencies inside the bundle.
    - The EC10 bundle is re-balanced, and re-constituted weekly, through direct indexing algorithmic computation methodology, which is a fully automated process.

- The EC10 bundle is priced internally, by the Company's systems, and the price is published on the website.
- Refer to the "EC10 Index Rules & Ancillary Disclosures", for details.

7. Objectives

The Company's **objectives** are to:

7.1. protect the integrity of the Company, through continuously managing the risk of money laundering and terrorist financing

7.2. apply a risk-based approach to client transactions and to understand the purpose of all business relationships with clients

7.3. educate employees how to identify business relationships and transactions that pose a higher risk to money laundering and terrorist financing

7.4. implement robust customer due diligence procedures that will make it more difficult for criminals to hide the proceeds of unlawful activities

7.5. keep accurate records of all related transactions and customer due diligence procedures

7.6. submit the relevant reports to the Centre

7.7. prevent any loss of sales and client confidence, reputational damage, civil or criminal fines or penalties, due to non-compliance with FICA and/or the Company's RMCP.

8. Obligations

8.1. The Company MUST NOT establish a business relationship, or conclude a single transaction, with an anonymous client, or a client with an apparent false or fictitious name, in terms of section 20A of the FICA.

- The customer due diligence process, **as reflected in Annexure 8**, will be followed for every prospective client, regardless of whether it relates to a single transaction, or a business relationship. Even business relationships/clients with the lowest risk rating will require enough information to be provided, so that the client will not be anonymous.

- ***Refer to Annexure 8 for details of the customer due diligence process.***

8.2. The Company MUST establish and verify the identity of all prospective and existing clients, and other people involved in the business relationship, or single transaction, with the prospective and existing clients, in terms of section 21 of the FICA.

- As part of the customer due diligence process, **as reflected in Annexure 8**, the Company applies a risk-based approach to determine the risk rating of the client, the financial product/service, the nature of the business relationship, with the aggregate thereof determining the overall risk rating of the business relationship, or single transaction.
- The **information and documents required to establish and verify the identity of the client**, and the other people involved in the business relationship, or single transaction**, differs, depending on the overall risk rating of the business relationship, or the single transaction, and the client type**.
- The risk-based approach is based on the Company's risk appetite. Several factors have been assessed and risk rated, according to the risk appetite. **Examples of factors that have been considered, to determine the risk ratings, are reflected in Annexure 6.**
- The risk rating scale comprises 5 levels.
  - 1 Very low risk

- 2 Low risk
- 3 Moderate risk
- 4 High risk
- 5 Very high risk

- A risk rating (before screening) is calculated, comprising the below factors.
  - Financial product/service client is investing into/purchasing
  - Business relationship or single transaction
  - Nature of establishing this business relationship
  - Purpose of establishing this business relationship
  - Client type
- A risk rating (after screening & compliance review) is calculated, comprising the below factors.
  - Risk rating (before screening)
  - UNSC targeted financial sanctions list
  - UNSC terrorist & related activities list
  - Foreign prominent public official (or closely associated with FPPO)
  - Domestic prominent influential person (or closely associated with DPIP)
- ***Refer to Annexure 8 for details of the customer due diligence process.***

8.3. The Company MUST understand and obtain information about the business relationship, when engaging with a prospective client, to determine whether future transactions that will be performed during the business relationship are consistent with the Company's knowledge of that prospective client, in terms of section 21A of the FICA.

- As part of the customer due diligence process, the person interacting with the prospective client (i.e. financial adviser/intermediary) must obtain enough information to reasonably enable the Company to determine whether future transactions that will be performed during the business relationship, are consistent with the Company's knowledge of the prospective client.

- The person interacting with the prospective client (i.e. financial adviser/intermediary) must include the nature of the business relationship, the intended purpose of the business relationship, and the source of the funds that the prospective client expects to use during the business relationship, on **Part 1 of the customer due diligence forms**.

- If the information inserted on the **customer due diligence forms** is not captured in specific fields within an electronic system, the compliance function must establish, populate and maintain a **customer due diligence information register**, to assist the Company to perform ongoing due diligence of existing clients.

- When assessing Part 1 and completing **Part 2 of the customer due diligence forms**, the compliance function must ensure that Part 1 and Part 2 has been fully completed and signed, and all information must be populated on the **customer due diligence information register**. In addition, the compliance officers will perform sample monitoring of the customer due diligence process.

- For existing clients, the person interacting with the client (i.e. financial adviser/intermediary) must follow a similar process, to obtain enough information to reasonably enable the Company to determine whether future transactions that will be performed during the business relationship, are consistent with the Company's knowledge of the prospective client, including obtaining the nature of the business relationship, the intended purpose of the business relationship, and the source of the funds that the prospective client expects to use during the business relationship.

8.4. The Company MUST perform additional customer due diligence measures for legal persons, trusts and partnerships, in terms of section 21B of the FICA.

- If the **prospective client is a legal person, trust agreement between natural persons, or partnership between natural persons (or similar)**, as part of the customer due diligence process, the

person interacting with the prospective client (i.e. financial adviser/intermediary) must obtain additional information, to **establish the nature of the client's business and the ownership and control structure of the client**.

- If the prospective client is a **legal person**, as part of the customer due diligence process, the person interacting with the prospective client (i.e. financial adviser/intermediary) must obtain additional information, to **establish and verify** the identity of the **beneficial owners** of the client, so that the person is satisfied that they know who the beneficial owners are. This process includes:
    - determining the identity of **each natural person** who, independently, or together with other natural persons, has a **controlling ownership interest** in the legal person. ***Important note: The percentage of shareholding with voting rights is a good indicator of control over a legal person, because a shareholder with a significant percentage of shareholding usually exercises control. As a guide, ownership of 25% or more of the shares with voting rights in a legal person is usually enough to exercise control of the legal person***;
    - determining the identity of **each natural person** who **exercises control** of the legal person **through other means** (i.e. other than by having a controlling ownership interest), **if in doubt** whether the natural person/s who have a controlling ownership interest in the legal person is/are the beneficial owner/s of the legal person, **or** where no natural person has a controlling ownership interest in the legal person;
    - determining the identity of **each natural person** who **exercises control over the management** of the legal person, including in the capacity as executive officer, non-executive director, independent non-executive director, director, or manager, **if a natural person is not identified who exercises control of the legal person through other means** (i.e. other than by having a controlling ownership interest).
- If the prospective client is a **partnership between natural persons**, as part of the customer due diligence process, the person interacting with the prospective client (i.e. financial adviser/intermediary) must obtain additional information, to **establish and verify** the **identifying name** of the partnership (if applicable), the **identity of every partner** (including every member of a partnership *en commandite*, an anonymous partnership, or any similar partnership), the **identity of the person who exercises executive control** over the partnership, the **identity of each natural person who is authorised** to enter into a single transaction, or establish a business relationship, with the Company, on behalf of the partnership, so that the person is satisfied that they know the identities of the persons concerned.
- If the prospective client is a **trust agreement between natural persons**, as part of the customer due diligence process, the person interacting with the prospective client (i.e. financial adviser/intermediary) must obtain additional information, to **establish and verify** the **identifying name and number** of the trust (if applicable), the address of the Master of the High Court where the trust is registered (if applicable), the **identity of the founder**, the **identity of each trustee**, the **identity of each natural person who is authorised** to enter into a single transaction, or establish a business relationship, with the Company, on behalf of the trust, the **identity of each named beneficiary** (if beneficiaries are not named, details of how the beneficiaries are determined), so that the person is satisfied that they know the identities of the persons concerned.
- The person interacting with the prospective client (i.e. financial adviser/intermediary) must include the relevant additional information on **Part 1 of the relevant customer due diligence forms**.
- When assessing Part 1 and completing **Part 2 of the relevant customer due diligence forms**, the compliance function must ensure that Part 1 and Part 2 has been fully completed and signed, and all relevant additional information must be populated on the relevant **customer due diligence information**

register. In addition, the compliance officers will perform sample monitoring of the customer due diligence process.

- For existing clients, where the client is a legal person, trust or partnership (or similar), the person interacting with the client (i.e. financial adviser/intermediary) must follow a similar process, to obtain the relevant additional information.

8.5. The Company MUST perform ongoing due diligence of the business relationship with clients, in terms of section 21C of the FICA.

- The company will perform ongoing due diligence of all existing business relationships with clients, **as reflected in Annexure 8**.

- ***Refer to Annexure 8 for details of the customer due diligence process.***

8.6. The Company MUST repeat customer due diligence process, and where necessary, confirm information about a client, after entering into a single transaction, or establishing a business relationship, when it has doubts about the accuracy of previously obtained information, in terms of section 21D of the FICA.

- If an employee doubts the accuracy of previously obtained information, **at any point (including while regularly monitoring transactions and keeping information updated)** after entering into a single transaction, or establishing a business relationship, with a client, he/she must repeat the customer due diligence process, including completing the relevant **customer due diligence forms**, and where necessary, confirm information about the client.

- If the compliance function, while performing scheduled ongoing due diligence, doubts the accuracy of previously obtained information, he/she must request the person interacting with the existing client (i.e. financial adviser/intermediary), to repeat the customer due diligence process, and after the information has been confirmed, the compliance function must update the information reflected in the **customer due diligence information register**.

8.7. The Company MUST avoid establishing business relationships, or concluding transactions (either single, or during a business relationship), and must terminate existing business relationships, when it is unable to fully perform the customer due diligence (initial and ongoing), in terms of section 21E of the FICA.

- If an employee cannot fully perform the customer due diligence (initial and/or ongoing), the Company, as the case may be,
    - may not establish a business relationship, or conclude a single transaction, with a client;
    - may not conclude a transaction during a business relationship, or perform any act relating to a single transaction; or
    - MUST terminate an existing business relationship with a client.

- ***Refer to Annexure 8 for details of the customer due diligence process.***

8.8. The Company MUST perform additional customer due diligence requirements, if it determines that a prospective client, with whom it engages, to establish a business relationship, or the beneficial owner of that prospective client, is an FPPO, or is an immediate family member, or a known close associate, of an FPPO, in terms of section 21F and 21H of the FICA.

- As part of the customer due diligence process, employees must obtain the details of the profession/occupation, employer, source of funds and source of wealth, of the prospective client, and each beneficial owner of the prospective client. This information must be reflected on Part 1 of the

relevant **customer due diligence forms**. Part 1 of the **customer due diligence forms** must be completed by the person interacting with the client (i.e. financial adviser/intermediary).

- As part of the customer due diligence process, the compliance function must complete Part 2 of the relevant customer due diligence forms, and must compare the details of the profession/occupation and employer of the prospective client, and each beneficial owner of the prospective client, with the list of FPPOs (refer to Annexure 3 of this policy), to determine whether the prospective client, or any of the beneficial owners of the prospective client, are FPPOs, or are immediate family members, or known close associates, of FPPOs. This review should also be supplemented by public media searches.

- If the prospective client, or any of the beneficial owners of the prospective client, are FPPOs, or are immediate family members, or known close associates, of FPPOs, **the overall risk rating of the prospective business relationship, or single transaction, MUST be determined to be risky**, and senior management must sign Part 2 of the form, approving, or declining, establishing the risky business relationship, or single transaction. If senior management declines the establishing of the risky business relationship, or single transaction, the person interacting with the client must notify the client that the Company will not be proceeding with the proposed business relationship, or single transaction.

- If senior management **approves establishing the risky business relationship**, or single transaction, the Company **must conduct enhanced ongoing monitoring of the business relationship**.

- It is important to note that even though a prospective client, or a beneficial owner of a prospective client, is not a FPPO, or an immediate family member or known close associate of a FPPO, at the time of performing the initial compliance due diligence, this status may change during the business relationship. Therefore, employees should be alert to changes with the existing client's profession/occupation or employer, and update the client's records, accordingly, including the relevant customer due diligence information register. In addition, the Company will periodically ask existing clients to confirm the accuracy of information on record.

8.9. The Company MUST perform additional customer due diligence requirements, if it determines that a prospective client, with whom it engages, to establish a business relationship, or the beneficial owner of that prospective client, is a DPIP, or is an immediate family member, or a known close associate, of a DPIP, and that the prospective business relationship entails higher risk, in terms of section 21G and 21H of the FICA.

- As part of the customer due diligence process, employees must obtain the details of the profession/occupation, employer, source of funds and source of wealth, of the prospective client, and each beneficial owner of the prospective client. This information must be reflected on Part 1 of the relevant **customer due diligence forms**. Part 1 of the **customer due diligence forms** must be completed by the person interacting with the client (i.e. financial adviser/intermediary).

- As part of the customer due diligence process, the compliance function must complete Part 2 of the relevant customer due diligence forms, which includes assessing the information reflected on Part 1, to determine the overall risk rating of the business relationship or single transaction, and must compare the details of the profession/occupation and employer of the prospective client, and each beneficial owner of the prospective client, with the list of DPIPs (refer to Annexure 2 of this policy), to determine whether the prospective client, or any of the beneficial owners of the prospective client, are DPIPs, or are immediate family members, or known close associates, of DPIPs. This review should also be supplemented by public media searches.

- If the prospective client, or any of the beneficial owners of the prospective client, are DPIPs, or are immediate family members, or known close associates, of DPIPs, **AND the overall risk rating of the prospective business relationship, or single transaction, has been determined to be risky**, then senior management must sign Part 2 of the form, approving, or declining, establishing the risky business

relationship, or single transaction. If senior management declines the establishing of the risky business relationship, or single transaction, the person interacting with the client must notify the client that the Company will not be proceeding with the proposed business relationship, or single transaction.

- If senior management **approves establishing the risky business relationship**, or single transaction, the Company **must conduct enhanced ongoing monitoring of the business relationship**.

- It is important to note that even though a prospective client, or a beneficial owner of a prospective client, is not a DPIP, or an immediate family member, or known close associate, of a DPIP, at the time of performing the initial compliance due diligence, this status may change during the business relationship. Therefore, employees should be alert to changes with the existing client's profession/occupation or employer, and update the client's records, accordingly, including the relevant **customer due diligence information register**. In addition, the Company will periodically ask existing clients to confirm the accuracy of information on record.

8.10. The Company MUST keep records of all customer due diligence information obtained about clients, or prospective clients, and the records must be kept for at least five (5) years from the date that the business relationship is terminated, or from the date of the conclusion of the single transaction, respectively, in terms of section 22 and 23 of the FICA.

- As part of the customer due diligence process, employees must ensure that all records relating to the customer due diligence information obtained about clients, or prospective clients, are kept. These records must **be kept for at least five (5) years from the date that the business relationship is terminated, or from the date of the conclusion of the single transaction, respectively**.

- The records must include:

    - copies of, or references to, information provided to, or obtained by, the Company, to verify a person's identity; and
    - in addition, for business relationships, information about:
        - the nature of the business relationship;
        - the intended purpose of the business relationship; and
        - the source of the funds that the prospective client expects to use for transacting during the business relationship.
    - The Company must ensure that electronically kept records are backed-up frequently, and can be reproduced in a legible format.
    - Compliance officers will perform scheduled sample monitoring.

8.11. The Company MUST keep records of every transaction, regardless of whether the transaction is a single transaction, or concluded during a business relationship, for at least five (5) years from the date on which the transaction was concluded, in terms of section 22A and 23 of the FICA.

- The Company will keep record of every transaction, whether the transaction is a single transaction, or concluded during a business relationship, which transactions are reasonably necessary to enable that transaction to be readily reconstructed.

- The records must include:

    - amount involved and the currency in which it was denominated;
    - date on which the transaction was concluded;
    - parties to the transaction;
    - nature of the transaction;
    - business correspondence; and

- if the Company provides account facilities to its clients, the identifying particulars of all accounts, and the account files at the Company that are related to the transaction.

- These records must **be kept for at least five (5) years from the date that the transaction was concluded**.

- The Company must ensure that electronically kept records are backed-up frequently, and can be reproduced in a legible format.

- Compliance officers will perform scheduled sample monitoring.

8.12. The Company MUST keep records of transactions, or activities, that give rise to an SAR or STR, for at least five (5) years from the date that the report was submitted to the Centre, in terms of section 23 and 29 of the FICA.

- The person responsible for reporting to the Centre (or his/her alternatives, if the responsible person is not available) will keep records of transactions, or activities, that give rise to an SAR or STR, for at least five (5) years from the date that the report was submitted to the Centre, in terms of section 23 and 29 of the FICA.

8.13. The Company MUST ensure that it has easy access to records in terms of section 22 and 22A of the FICA that are kept by third parties, and that the records are readily available to the Centre and the relevant supervisory body, and provide the Centre and the relevant supervisory body with the details of the third party, in terms of section 24 of the FICA.

- The Company has appointed a third party to keep records on its behalf. The Company will **immediately provide the Centre and the relevant departments of the FSCA with the following details of the third party**:

  - full name, if the third party is a natural person; or
  - registered name, if the third party is a close corporation or company;
  - name under which the third party conducts business;
  - full name and contact particulars of the individual who exercises control over access to the records;
  - address where the records are kept;
  - address from where the third party exercises control over the records; and
  - full name and contact particulars of the individual who liaises with the third party, on behalf of the Company, regarding the retention of the records.

- **This requirement IS NOT applicable to the Company, because it has not appointed a third party to keep records on its behalf.**

- The Company will ensure that it has easy access to the customer due diligence and transaction records, and that they are readily available to the Centre and the relevant departments of the FSCA.

- The Company notes that if it **fails to provide the Centre and the relevant departments of the FSCA with the details of the third party,** it is non-compliant with Regulation 20, and is subject to an **administrative sanction**.

8.14. The Company MUST avoid entering into prospective single transactions and business relationships with persons and entities identified in a resolution by the Security Council of the United Nations, and to freeze property and transactions, relating to these persons and entities who are existing clients, in terms of section 26A, 26B and 26C of the FICA.

- The FICA places the responsibility to administer the targeted financial sanctions (TFS) measures adopted by the United Nations Security Council (UNSC) in its Resolutions, on the Centre.

- This inclusion of TFS measures is, *inter alia*, due to Recommendation 7 of the Financial Action Task Force (FATF) Recommendations, which requires member countries to implement the TFS proposed by the UNSC, to combat the financing of the proliferation of weapons of mass destruction. The use of TFS by the UNSC also extends beyond the instances relating to the financing of the proliferation of weapons of mass destruction. Therefore, the relevant provisions of the FICA aim at enabling South Africa to meet these international obligations.

- Sanctions impose restrictions on activities that relate to countries, goods and services, or persons and entities. TFS measures generally restrict sanctioned persons and entities from having access to funds and property that is under their control, and from receiving financial services, relating to those funds and property. To give effect to these sanctions, the FICA requires the Company (all AIs) **to freeze property and transactions, relating to financial sanctions imposed in the UNSC Resolutions**.

- It is important to note that **TFS ONLY provide for financial sanctions**, and include a list of all persons and entities who are subject to TFS under the FICA. **This does not apply to resolutions of the UNSC contemplated in section 25 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act (POCDATARA), which imposes additional reporting obligations, in terms of section 28A of the FICA**.

- To implement the UNSC Resolutions, the Minister of Finance must publish a Notice of the adoption of the UNSC Resolution in the Government Gazette, and the Director of the Centre must publish a Notice of persons who are subject to the sanction measures (the TFS list). These Notices may be revoked, if it is considered that they are no longer necessary, to give effect to the applicable UNSC Resolutions. Otherwise the sanctions announced in these Notices remain in effect indefinitely.

- These public Notices are meant to **advise** both sanctioned persons and entities, and **AIs, who may have them as clients, or prospective clients, of the relevant sanctions**. Therefore, **if the Company has a sanctioned person, or entity, as a client, it may draw the attention of the person, or entity, to the relevant sanctions' notices**.

- The acquisition, collection, or use, of the property of persons, or entities, whose names appear in the TFS list, is prohibited. Therefore, the **providing of financial services and products to those persons or entities, is prohibited**. **The Company is not allowed to transact with a sanctioned person, or entity, or to process transactions for those persons or entities**. The status quo at the time that the sanction was imposed, must be retained, relating to the property, or funds, of the sanctioned person or entity, and no financial services may be provided to the person or entity. Therefore, **the Company must avoid entering into single transactions and business relationships with persons and entities whose names appear on the TFS list, and must freeze property and transactions, relating to these persons and entities who are existing clients**.

- As part of the customer due diligence process, the compliance function must complete Part 2 of the relevant customer due diligence forms, which includes searching the TFS list, to determine whether the prospective client's name appears on the list, by using the online search facility provided by the FIC, on the FIC website (https://www.fic.gov.za/International/sanctions/Pages/search.aspx). **If matches are found, indicating that a prospective client is named on the TFS list, the compliance function must advise the person interacting with the client (i.e. financial adviser/intermediary), who must advise the prospective client that the Company may not enter into a single transaction, or business relationship with the prospective client, and the prospective client may be alerted to the fact that their name appears on the TFS list. In addition, the person responsible for reporting to the Centre (or his/her alternatives, if the responsible person is not available), must submit a TPR to the Centre, in terms of section 28A of the FICA, within 5 days of becoming aware. It is an offence to continue with a transaction.**

- Each compliance officer and compliance assistant of the Company must subscribe to receive notifications of changes to the TFS list, via the FIC website (https://www.fic.gov.za/International/sanctions/SitePages/Home.aspx).

- Whenever changes to the TFS list are published, the compliance function must check the names against the existing clients' records. The relevant **customer due diligence information register** may be used, to assist with searching for matching names of existing clients. **If matches are found, indicating that existing clients are named on the TFS list, the compliance function must instruct the relevant employees to freeze the existing client's property and transactions, and must advise the person interacting with the client (i.e. financial adviser/intermediary), who may alert the existing client that the Company must freeze the existing client's property and transactions, as the existing client may be alerted to the fact that their name appears on the TFS list. In addition, the person responsible for reporting to the Centre (or his/her alternatives, if the responsible person is not available), must submit a TPR to the Centre, in terms of section 28A of the FICA, within 5 days of becoming aware**. **It is an offence to continue with a transaction.**

- For existing clients, the compliance function must perform scheduled searches of the TFS list, to determine whether any existing clients names appear on the TFS list, by using the online search facility provided by the FIC, on the FIC website (https://www.fic.gov.za/International/sanctions/Pages/search.aspx). The relevant customer due diligence information register may be used, to assist with searching for matching names of existing clients. The compliance function must use the risk-based approach, to prioritise the order of searching for existing clients' names on the list. The foreign clients should be prioritised first, as there is a higher probability of their names appearing on the list. Thereafter, the overall risk rating of the business relationship should be used for ordering the searches, starting with very high risk and ending with very low risk business relationships. **If matches are found, indicating that existing clients are named on the TFS list, the compliance function must instruct the relevant employees to freeze the existing client's property and transactions, and must advise the person interacting with the client (i.e. financial adviser/intermediary), who may alert the existing client that the Company must freeze the existing client's property and transactions, as the existing client may be alerted to the fact that their name appears on the TFS list. In addition, the person responsible for reporting to the Centre (or his/her alternatives, if the responsible person is not available), must submit a TPR to the Centre, in terms of section 28A of the FICA, within 5 days of becoming aware**. **It is an offence to continue with a transaction.**

- When using the FIC online search facility, it may not always be clear whether there is a match between the name provided and any name on the TFS List, the Company may ask the FIC TFS Support/PQP to assist, to determine whether, or not, an asset is owned, or controlled, by a person, or entity, on the TFS List. To facilitate this process, a PQP Request form can be used, which should be sent to the FIC at the following address:
  FIC PQP TFS:
  e-mail: TFSsupport@fic.gov.za
  Fax: +27 12 641 6458
  Phone: +27 12 641 6000

- The only exception to this general prohibition is in specific instances where the Minister of Finance has permitted, in writing, either on his/her own initiative, or upon request by an affected person, certain financial services, or dealings, with property. The Director of the Centre must publish permissions granted by the Minister of Finance. If an affected person wants to request permission to provide financial services, or deal with property, the details are on the FIC website (https://www.fic.gov.za/International/sanctions/Pages/assets.aspx#application).

- The Minister of Finance may permit the providing of financial services, or the dealing with property, if it is necessary to:

    - provide for basic expenses, including:
        - foodstuffs;
        - rent or mortgage;
        - medicines or medical treatment;
        - taxes;
        - insurance premiums;
        - public utility charges;
        - maintenance orders;
        - reasonable professional fees, and
    - reimburse expenses associated with the provision of legal services;
    - satisfy a judgment, or arbitral award, that was made before the date on which the person, or entity, was identified by the UNSC;
    - make a payment to a third party, which is due under a contract, agreement, or other obligation, made before the date on which the person, or entity, was identified by the UNSC;
    - accrue interest, or other earnings, due on accounts holding property affected by a prohibition under section 26B of the FICA;
    - make a payment due to a person, or entity, affected by a prohibition under section 26B of the FICA, by virtue of a contract, agreement, or other obligation, made before the date on which the person, or entity, was identified by the UNSC, as long as the payment is not directly, or indirectly, being received by that person, or entity.

8.15. The Company MUST provide the Centre with information relating to its existing clients, or previous clients, which an authorised representative of the Centre has specifically requested, within the specific timeframe, in terms of section 27 of the FICA.

- If an authorised representative of the Centre requests the Company to provide any of the below information relating to its existing clients, or previous clients, the Company must provide the requested information to the authorised representative of the Centre, within the timeframe specified in the written request.
    - Whether a specified person is, or has been, a client of the Company;
    - Whether a specified person is acting, or has acted, on behalf of any client of the Company;
    - Whether a client of the Company is acting, or has acted, for a specified person;
    - Whether a number specified by the Centre was allocated by the Company to a person with whom the Company has, or has had, a business relationship; or
    - The type and status of a business relationship with a client of the Client.

- The person responsible for reporting to the Centre (or his/her alternatives, if the responsible person is not available) will receive information requests from the Centre. The compliance function must assess the lists of existing clients and previous clients, to determine whether the requested information is on record. The relevant **customer due diligence information register** may be used, to assist with finding information about existing clients and previous clients. If the information is not on record, no response is required. If the information is on record, the person responsible for reporting to the Centre (or his/her alternatives, if the responsible person is not available) must respond to the authorised representative of the Centre, within the timeframe specified in the written request.

8.16. The Company MUST provide authorised representatives of the Centre with reasonable assistance, without delay, to access any of the records that must be kept, or records relating to reports made to the Centre, during ordinary working hours, in terms of section 27A of the FICA.

- The Company must provide authorised representatives of the Centre with reasonable assistance, without delay, to access any of the records that must be kept, or records relating to reports made to the

Centre, during ordinary working hours, to enable that representative to exercise the powers granted to the Centre.

- For records that the public is NOT entitled to have access to, the authorised representatives of the Centre may only exercise the powers to access any of the records that must be kept, or records relating to reports made to the Centre, by virtue of a warrant, issued in chambers, by a magistrate, or regional magistrate, or judge, of an area of jurisdiction within which the records, or any of them, are kept, or within which the Company conducts business. Therefore, in this case, BEFORE providing the authorised representatives of the Centre with reasonable assistance, the employee must request the warrant to be provided by the authorised representative of the Centre.

8.17. The Company MUST submit CTRs to the Centre, concerning cash transactions concluded with a client (paid to, or received from, a client, or a person acting on behalf of a client, or a person on whose behalf the client is acting), in excess of the prescribed amount (currently R24,999.99, or an aggregate of smaller amounts that combine to exceed this amount), within 2 days of becoming aware, in terms of section 28 of the FICA.

- The Company must, **within 2 days of becoming aware**, **report** the prescribed details about a transaction concluded with a client, **to the Centre**, **in the prescribed format**, **via the FIC online reporting portal (http:www.fic.gov.za)**, if cash is paid to, or received from, a client, or a person acting on behalf of a client, or a person on whose behalf the client is acting, in excess of the prescribed amount (currently R24,999.99, or an aggregate of smaller amounts that combine to exceed this amount).

- **Although the business rule is that the Company DOES NOT accept cash payments, to ensure that no cash has been paid into the bank accounts, the Company has nominated employees to review the bank accounts DAILY, to identify cash transactions. All cash transactions identified must immediately be reported to the person responsible for reporting to the Centre (or his/her alternatives, if the responsible person is not available), including as much of the required information, as possible. The person responsible for reporting to the Centre (or his/her alternatives, if the responsible person is not available), will submit CTRs to the Centre, for all prescribed cash transactions, within 2 days of becoming aware.**

- **The Company should continue with, and carry out, the related transaction, or series of transactions, unless the Centre instructs it to not proceed.**

- **The person responsible for reporting to the Centre (or his/her alternatives, if the responsible person is not available), must also consider submitting an STR to the Centre, in terms of section 29 of the FICA, for the cash transaction, or series of cash transactions.**

- After submitting a CTR to the Centre, the Centre may request the Company to provide additional information.

- **The Company DOES NOT pay out any cash to clients.**

- **The information that must be included in a CTR is reflected in Annexure 4 of this policy**.

- **If the Company fails to provide the information to be reported, for a CTR, it is guilty of an offence.**

- **If the Company fails to provide the information to be reported, for a CTR, it is non-compliant, and is subject to an administrative sanction.**

8.18. The Company MUST submit TPRs to the Centre, concerning property associated with terrorist and related activities and financial sanctions pursuant to Resolutions of United Nations Security Council, within 5 days of becoming aware, in terms of section 28A of the FICA.

- If the Company **KNOWS** that it possesses, or controls, property owned, or controlled by, or on behalf of, or at the direction of,
  - any person, or entity that has committed, or attempted to commit, or facilitated, the commission of a specified offence, as defined in the POCDATARA (including offences such as terrorism, associated, or connected, with terrorist activities, or a convention offence); and/or
  - a specific person, or entity, identified in a Proclamation issued under section 25 of the POCDATARA; and/or
  - a specific person, or entity, identified in a Notice of persons who are subject to the sanction measures (the TFS list), published by the Minister of Finance, in terms of section 26A(1) of the FICA,

it must, within 5 days of becoming aware, **submit a TPR**, including the prescribed details, **to the Centre**, **in the prescribed format**, **via the FIC online reporting portal (http:www.fic.gov.za)**.

- After submitting a TPR to the Centre, the Director of the Centre may direct the Company to report, within specified intervals, that it is still in possession, or control, of the property, and any change in the circumstances about the Company's possession, or control, of that property.

- Immediately after the publication of, a Proclamation issued under section 25 of the POCDATARA, or the TFS list, **the compliance function**, on behalf of the Company, **must scrutinise the information of clients with whom it has business relationships**, to determine whether any client is a person, or entity, mentioned in the Proclamation or the TFS list.

- The consolidated list is located on the United Nations (UN) website (https://www.un.org/securitycouncil/content/un-sc-consolidated-list). The latest list can be downloaded, or searches can be made on the UN website. The individuals and entities whose names appear on these lists, are those whom the UNSC has identified as being associated with the Taliban, Al Qaida, and the so-called Islamic State of Iraq and Levant. **It is important to note that these lists are the only sanctions lists related to terrorist activities, which are legally recognised within South Africa, and can be accessed directly on the UN website.**

- **All positive matches must immediately be reported to the person responsible for reporting to the Centre (or his/her alternatives, if the responsible person is not available), including as much of the required information, as possible. The person responsible for reporting to the Centre (or his/her alternatives, if the responsible person is not available), will submit TPRs to the Centre, within 5 days of becoming aware.**

- Dealing with, property that is associated with acts of terrorism, persons, or organisations, that carry out acts of terrorism, or sanctioned entities, is prohibited. Therefore, the **providing of financial services and products to those persons or entities, is prohibited**. **The Company is not allowed to transact with a sanctioned person, or entity, or to process transactions for those persons or entities**. The status quo at the time that the sanction was imposed, must be retained, relating to the property, or funds, of the sanctioned person or entity, and no financial services may be provided to the person or entity. Therefore, **the Company must avoid entering into single transactions and business relationships with persons and entities whose names appear on the consolidated list, and must freeze property and transactions, relating to these persons and entities who are existing clients**. **It is an offence to continue with a transaction.**

- As part of the customer due diligence process, the compliance function must complete Part 2 of the relevant customer due diligence forms, which includes searching the consolidated list, to determine whether the prospective client's name appears on the list, by using the online search facility provided by the UN, on the UN website (https://www.un.org/securitycouncil/content/un-sc-consolidated-list). **If**

matches are found, indicating that a prospective client is named on the consolidated list, the compliance function must advise the person interacting with the client (i.e. financial adviser/intermediary), who must advise the prospective client that the Company may not enter into a single transaction, or business relationship with the prospective client. In addition, the person responsible for reporting to the Centre (or his/her alternatives, if the responsible person is not available), must submit a TPR to the Centre, in terms of section 28A of the FICA, within 5 days of becoming aware. It is an offence to continue with a transaction.

- Each compliance officer and compliance assistant of the Company must subscribe to receive notifications of changes to the consolidated list, via the UN website (https://www.un.org/securitycouncil/content/un-sc-consolidated-list).

- Whenever changes to the consolidated list are published, the compliance function must check the names against the existing clients' records. The relevant **customer due diligence information register** may be used, to assist with searching for matching names of existing clients. **If matches are found, indicating that existing clients are named on the consolidated list, the compliance function must instruct the relevant employees to freeze the existing client's property and transactions. In addition, the person responsible for reporting to the Centre (or his/her alternatives, if the responsible person is not available), must submit a TPR to the Centre, in terms of section 28A of the FICA, within 5 days of becoming aware**. **It is an offence to continue with a transaction.**

- For existing clients, the compliance function must perform scheduled searches of the consolidated list, to determine whether any existing clients names appear on the consolidated list, by using the online search facility provided by the UN, on the UN website (https://www.un.org/securitycouncil/content/un-sc-consolidated-list). The relevant customer due diligence information register may be used, to assist with searching for matching names of existing clients. The compliance function must use the risk-based approach, to prioritise the order of searching for existing clients' names on the list. The foreign clients should be prioritised first, as there is a higher probability of their names appearing on the list. Thereafter, the overall risk rating of the business relationship should be used for ordering the searches, starting with very high risk and ending with very low risk business relationships. **If matches are found, indicating that existing clients are named on the consolidated list, the compliance function must instruct the relevant employees to freeze the existing client's property and transactions. In addition, the person responsible for reporting to the Centre (or his/her alternatives, if the responsible person is not available), must submit a TPR to the Centre, in terms of section 28A of the FICA, within 5 days of becoming aware**. **It is an offence to continue with a transaction.**

- A **TPR** is based on **FACT**, from information mentioned in the Proclamation or TFS list. **It does not relate to a suspicion that is formed subjectively**.

- If there is an identified client of multiple AIs within a group of companies, EACH AI must submit a separate TPR to the Centre.
  - **The information that must be included in a TPR is reflected in Annexure 4 of this policy**.
  - **If the Company, or person, fails to submit a TPR, it is guilty of an offence, in terms of both section 51A of the FICA and section 4 of the POCDATARA.**
  - **If the Company, or person, fails to provide the information to be reported in a TPR, it is guilty of an offence.**
  - **If the Company, or person, fails to provide the information to be reported in a TPR, it is non-compliant, and is subject to an administrative sanction.**

8.19. The Company MUST submit SARs, STRs, TFTRs, or TFARs to the Centre, concerning proceeds of unlawful activities, property connected to an offence relating to the financing of terrorist and related activities, or money laundering, relating to an activity that does not involve a transaction between

two or more parties, or relating to a transaction, or series of transactions, about which enquiries are made, but which has not been concluded, or relating to a transaction, or series of transactions, within 15 days of becoming aware, in terms of section 29(1) and (2) of the FICA.

- If the Company, or any of its employees, **knows, or ought reasonably to have known, or suspected that**:
  - it has **received, or is about to receive, the proceeds of unlawful activities, or property**, which is connected to an offence relating to the **financing of terrorist and related activities**;
  - a **transaction, or series of transactions**, to which it is a party:
    - facilitated, or is likely to facilitate, the transfer of the proceeds of unlawful activities, or property, which is connected to an offence relating to the financing of terrorist and related activities;
    - has no apparent business, or lawful, purpose;
    - is conducted for the purpose of avoiding a reporting duty under the FICA;
    - may be relevant to the investigation of an evasion, or attempted evasion, of a duty to pay any tax, duty, or levy, imposed by legislation administered by the Commissioner for the South African Revenue Service;
    - relates to an offence relating to the financing of terrorist and related activities; or
    - relates to the contravention of a prohibition under section 26B of the FICA (transacting with persons or entities whose names appear on the TFS list); or
  - it has been used, or is about to be used, in any way, for money laundering purposes, or to facilitate the commission of an offence relating to the financing of terrorist and related activities,

  it must, within 15 days of becoming aware, **submit an SAR, STR, TFTR, or TFAR, as the case may be**, **through the person responsible for reporting to the Centre (or his/her alternatives, if the responsible person is not available)**, including the grounds for the knowledge or suspicion, and other prescribed details, **to the Centre**, **in the prescribed format**, **via the FIC online reporting portal (http:www.fic.gov.za)**.

- If the Company, or any of its employees, knows, or suspects, that the **activity/transaction, or series of activities/transactions, about which enquiries are made, but which has not been concluded, MAY have caused any of the consequences above**, **it must, within 15 days of becoming aware**, **submit an SAR or TFAR, as the case may be**, **through the person responsible for reporting to the Centre (or his/her alternatives, if the responsible person is not available)**, including the grounds for the knowledge or suspicion, and other prescribed details, **to the Centre**, **in the prescribed format**, **via the FIC online reporting portal (http:www.fic.gov.za)**.

- **All knowledge and suspicions must immediately be reported to the person responsible for reporting to the Centre (or his/her alternatives, if the responsible person is not available), including as much of the information listed below, as possible. The person responsible for reporting to the Centre (or his/her alternatives, if the responsible person is not available), will submit SARs, STRs, TFTRs or TFARs to the Centre, as the case may be, for those cases where he/she reasonably believes that a report should be submitted, after investigating the information received, within 15 days of becoming aware.**

- **The Company may choose to continue with, and carry out, the related transaction, or series of transactions, unless the Centre instructs it to not proceed.**

- After submitting an SAR, STR, TFTR, or TFAR, to the Centre, the Centre may request the Company to provide additional information.

- If a **person knows** (including the person who has, or must, submit to the Centre), **or suspects**, that an **SAR, STR, TFTR, or TFAR**, has been, or will be, **submitted** to the Centre, **they MUST NOT tell anyone else, EXCEPT**:
  - within the scope of that person's powers and duties, in terms of any legislation;
  - for the purpose of carrying out the provisions of the FICA;
  - for the purpose of legal proceedings, including any proceedings before a judge in chambers; or
  - in terms of an order of court.

- **The information that must be included in an SAR, STR, TFTR, or TFAR, is reflected in Annexure 4 of this policy.**

- **Examples of activities that may be related to terrorist and related activities, or which may be suspicious or unusual activities/transactions, are reflected in Annexure 4 of this policy**.

- **If the Company, or person, fails to provide the information to be reported, for an SAR, STR, TFTR, or TFAR, it is guilty of an offence.**

- **If the Company, or person, fails to provide the information to be reported, for an SAR, STR, TFTR, or TFAR, it is non-compliant, and is subject to an administrative sanction.**

8.20. The Company MUST develop, document, maintain and implement a RMCP for anti-money laundering and counter-terrorist financing risk management, in terms of section 42(1) of the FICA.

- This policy, read together with the supporting documents, is the documented RMCP of the Company.

- This policy is approved by the Board.

- This policy, and the supporting documents, will be reviewed regularly, and updated, if necessary, to ensure that it remains relevant to the Company's operations, and achieving the requirements.

- This policy, and the supporting documents, will be provided to employees who are involved with transactions.

- If requested, the Company, through the compliance function, will provide a copy of this policy, and the supporting documents, to the Centre, or a supervisory body, performing regulatory, or supervisory, functions for the Company.

8.21. The Company MUST identify, assess, monitor, mitigate and manage the risk that the providing of financial products and services may involve, or facilitate, money laundering activities, or the financing of terrorist and related activities, in terms of section 42(2) of the FICA.

- The Company, and its employees, will be able to identify, assess, monitor, mitigate and manage the risk that the providing of financial products and services may involve, or facilitate, money laundering activities, or the financing of terrorist and related activities, as provided for by this policy, read together with the supporting documents.

8.22. The Company MUST govern anti-money laundering and counter terrorist financing compliance, where the Board must ensure compliance by the Company and its employees, in terms of section 42A of the FICA.

- The Board will ensure that the necessary policies and procedures are in place, and are adhered to, to ensure compliance by the Company and its employees.

- The Board will delegate responsibilities to competent employees, to assist it to ensure that compliance is achieved, and maintained. The Board, assisted by the compliance function, will monitor the performance of the delegated responsibilities.

8.23. The Company MUST have a compliance function, to assist the Board in discharging their obligations to ensure compliance by the Company, and its employees, and assign a person with enough competence, and seniority, to ensure the effectiveness of the compliance function, in terms of section 42A of the FICA.

- The Company has appointed an independent compliance practice as the compliance function, to assist the Board to ensure that the necessary policies and procedures are in place, and are adhered to, to ensure compliance by the Company and its employees.

- The compliance function will monitor the Company's, and its employees' adherence to the obligations described in this policy, including the performance of the delegated responsibilities, and report non-compliance to the Exco and the governance structures.

- The head of the independent compliance practice has been appointed as the competent, senior person, to ensure the effectiveness of the compliance function.
  - **Gigi Vorlaufer (head of Soundsolve Compliance (Pty) Ltd)**
  - **Email:** gigiv@soundsolve.co.za
  - **Mobile:** +27 82 780 8473

8.24. The Company MUST provide ongoing training to its employees, to enable them to comply with the provisions of the FICA and the RMCP that are applicable to them, in terms of section 43 of the FICA.

- The compliance function will provide ongoing guidance and training to employees, to assist them to comply with, and understand, their obligations, in terms of the FICA and the Policy.

- The training will include an assessment, with a high pass requirement, to ensure that the employee has suitable knowledge.

8.25. The Company MUST register with the Centre, within 90 days, in terms of section 43B of the FICA.

- The Company has registered with the Centre, in the prescribed way.
  - **ORG ID: 52019**

- As part of the registration, the Company has provided the Centre with the details of the competent, senior person, who has been appointed to ensure the effectiveness of the compliance function.

- As part of the registration, the Company has provided the Centre with the details of the person responsible for submitting reports to the Centre, as well as the details of alternative people, who may submit reports to the Centre, if the responsible person is not available to do so.

8.26. The Company MUST notify the Centre, in writing, of any changes to the details provided during registration with the Centre, within 90 days after a change, in terms of section 43B of the FICA.

- The Company, through the compliance function, will notify the Centre of any changes to the details provided, as part of the registration, within 90 days of the change.

- The Company, and its employees, must immediately provide the compliance function with the details of changes, so that the compliance officers can notify the Centre within 90 days of the change.

9. Reliance agreements

9.1. The Company may establish reliance agreements with other AIs, for business relationships with shared clients.

9.2. Separate agreements will be established with each AI.

9.3. The reliance agreements will stipulate whether the Company is the first party accountable institution, or the third party accountable institution. ***Refer to Annexure 8 for a list of the reliance agreements that have been established, and the incorporation into the CDD process.***

9.4. The parties to the reliance agreements will provide each other with their respective RMCPs, to determine, and understand, the CDD standards applied by the other party to the reliance agreement.

9.5. Before establishing reliance arrangements, the Company will satisfy itself that the other AI has the operational ability, and capacity, to perform the obligations effectively, reliably, and professionally.

9.6. When establishing reliance arrangements, the Company will avoid, and where this is not possible, mitigate, any conflicts between its interests, the interests of clients, and the interests of the other AI.

9.7. The Company will perform initial, and regular ongoing, due diligence reviews on the other party to the reliance agreement, to satisfy itself that the other party:

- has appropriate professional indemnity cover
- can implement, and maintain, an effective contingency plan for disaster recovery, and periodic testing of back-up facilities, where necessary
- has the necessary capability, and expertise, to properly perform its obligations, and to adequately manage risks associated with its obligations
- has the appropriate governance, and internal control, framework, to perform its obligations effectively, and in compliance with applicable legislation and/or regulatory requirements
- is financially sound.

9.8. As part of the due diligence reviews, the Company will ensure that:

- any possible termination, or disruption, of the arrangement would not impede its ability to ensure continuous, and satisfactory, service to clients
- it can identify possible concentration risk, and where identified, can take steps to ensure that it has the capability, and adequate capacity, to meet all the requirements of the arrangement, both during normal operations, and unusual circumstances (for example, unusual market activity, or physical disaster)

9.9. The Company will not establish a reliance agreement with another AI, if it is uncomfortable with the outcome of the initial due diligence review.

9.10. During reliance arrangements, the Company will identify, assess, and manage, the risks emanating from the arrangement.

9.11. If the Company is unsatisfied with the outcome of an ongoing due diligence review, it will request the other AI to make specific improvements, within a reasonable timeframe. If the Company is still unsatisfied after the reasonable timeframe, it may terminate the reliance agreement. Reasons for terminating the reliance agreements are specified in the reliance agreements.

9.12. The Company will ensure that the reliance agreement will not:

- materially increase its risks for managing financial crime
- materially impair the quality of its governance framework
- impair its ability to manage its risks, and meet its legal, and regulatory, obligations
- impede the ability of the Authority to monitor it's compliance with its regulatory obligations
- compromise the fair treatment of, or continuous, and satisfactory, service to clie

10. Consequences of non-compliance with the policy

10.1. All employees are obliged to comply with the Policy, and it is a condition of employment. Non-compliance is a breach of their employment contract, and is an action of misconduct, so employees may be subject to disciplinary action, which may lead to dismissal. Non-compliance by an employee will be dealt with according to the Company's disciplinary policy. For assessing, and addressing, the non-compliance, reports made by the compliance officers, internal audit, external audit, and the Authorities, will be considered, for appropriate action to be taken.

11. Policy review

11.1. The policy will be reviewed annually, updated, if necessary, and the latest version will be adopted, and approved, by the board.

ANNEXURE 1: ADMINISTRATIVE SANCTIONS

The Centre, or a supervisory body, may impose an administrative sanction on any AI, reporting institution, or other person to whom the FICA applies, when satisfied, on available facts and information, that the institution, or person:

a) has failed to comply with a provision of the FICA, or any order, determination, or directive, made in terms of the FICA;
b) has failed to comply with a condition of a licence, registration, approval, or authorisation, issued, or amended;
c) has failed to comply with a directive:
    a. not to proceed with the carrying out of a transaction, or proposed transaction, or any other transaction relating to the funds affected by the transaction, or proposed transaction, for a period not longer than 10 business days, as determined by the Centre, to allow the Centre to make the necessary inquiries about the transaction, and, if the Centre considers it appropriate, to inform and advise an investigating authority, or the National Director of Public Prosecutions;
    b. to provide the Centre with the information, reports, or statistical returns, specified in the notice, at the time, or at the intervals, specified in the notice, and within the period specified in the notice, with any document in its possession, or custody, or under its control; or
d) has failed to comply with a non-financial administrative sanction imposed in terms of this section.

When determining an appropriate administrative sanction, the Centre, or the supervisory body, must consider the following factors:

a) nature, duration, seriousness and extent of the relevant non-compliance;
b) whether the institution, or person, has previously failed to comply with any law;
c) remedial steps taken by the institution, or person, to prevent a recurrence of the non-compliance;
d) steps taken, or to be taken, against the institution, or person by another supervisory body, or a voluntary association, of which the institution, or person, is a member; and
e) any other relevant factor, including mitigating factors.

The Centre, or supervisory body, may impose one, or more, of the following administrative sanctions:

a) caution not to repeat the conduct that led to the non-compliance;
b) reprimand;
c) directive to take remedial action, or to make specific arrangements;
d) restriction, or suspension, of certain specified business activities; or
e) financial penalty, not exceeding R10 million, for natural persons, and R50 million, for any legal person.

The Centre, or supervisory body, may:

a) in addition to the imposition of an administrative sanction, make recommendations to the relevant institution, or person, in respect of compliance with the FICA, or any order, determination, or directive, made in terms of the FICA;
b) direct that a financial penalty must be paid by a natural person, or persons, for whose actions the relevant institution is accountable in law, if that person, or persons, was, or were, personally responsible for the non-compliance;
c) suspend any part of an administrative sanction, on any condition the Centre, or the supervisory body, deems appropriate, for a period not exceeding five years.

Before imposing an administrative sanction, the Centre, or supervisory body, must give the institution, or person, reasonable notice, in writing:

a) of the nature of the alleged non-compliance;
b) of the intention to impose an administrative sanction;
c) of the amount, or details, of the intended administrative sanction; and
d) that the institution, or person, may, in writing, within a period specified in the notice, make representations as to why the administrative sanction should not be imposed.

After considering any representations, and the factors, the Centre, or supervisory body, may impose an administrative sanction that the Centre, or supervisory body, considers appropriate. The Centre must, prior to taking a decision, consult the relevant supervisory body, if applicable.

Upon imposing the administrative sanction, the Centre, or supervisory body, must, in writing, notify the institution, or person of the decision, and the reasons therefor, and of the right to appeal against the decision.

Any financial penalty imposed, must be paid into the National Revenue Fund, within the period, and in the way specified in the relevant notice.

If the institution, or person, fails to pay the financial penalty within the specified period, and an appeal has not been lodged within the required period, the Centre, or supervisory body, may forthwith file, with the clerk, or registrar, of a competent court, a certified copy of the notice, and the notice thereupon has the effect of a civil judgment, lawfully given in that court, in favour of the Centre, or supervisory body.

An administrative sanction may not be imposed if the respondent has been charged with a criminal offence, for the same set of facts.

If a court assesses the penalty to be imposed on a person convicted of an offence in terms of the FICA, the court must consider any administrative sanction imposed, for the same set of facts.

An administrative sanction imposed in terms of the FICA, does not constitute a previous conviction, as contemplated in Chapter 27 of the Criminal Procedure Act 51 of 1977.

Unless the Director, or supervisory body, is of the opinion that there are exceptional circumstances present that justify the preservation of the confidentiality of a decision, the Director, or supervisory body, must make public the decision and the nature of any sanction imposed, if an institution, or person, does not appeal against a decision of the Centre, or supervisory body, within the required period; or the appeal board confirms the decision of the Centre or supervisory body.

ANNEXURE 2: DOMESTIC PROMINENT INFLUENTIAL PERSONS (DPIP)

A domestic prominent influential person is an individual who holds, including in an acting position, for a period exceeding 6 months, or has held, at any time in the preceding 12 months, in South Africa:

a) a prominent public function, including:
   a. the President or Deputy President;
   b. a government minister or deputy minister;
   c. the Premier of a province;
   d. a member of the Executive Council of a province;
   e. an executive mayor of a municipality elected in terms of the Local Government: Municipal Structures Act, 1998 (Act No. 117 of 1998);
   f. a leader of a political party registered in terms of the Electoral Commission Act, 1996 (Act No. 51 of 1996);
   g. a member of a royal family, or senior traditional leader, as defined in the Traditional Leadership and Governance Framework Act, 2003 (Act No. 41 of 2003);
   h. the head, accounting officer, or chief financial officer, of a national, or provincial, department, or government component, as defined in section 1 of the Public Service Act, 1994 (Proclamation No. 103 of 1994);
   i. the municipal manager of a municipality appointed in terms of section 54A of the Local Government: Municipal Systems Act, 2000 (Act No. 32 of 2000), or a chief financial officer, designated in terms of section 80(2) of the Municipal Finance Management Act, 2003 (Act No. 56 of 2003);
   j. the chairperson of the controlling body, the chief executive officer, or a natural person, who is the accounting authority, the chief financial officer, or the chief investment officer, of a public entity listed in Schedule 2 or 3 to the Public Finance Management Act, 1999 (Act No. 1 of 1999);
   k. the chairperson of the controlling body, chief executive officer, chief financial officer, or chief investment officer, of a municipal entity, as defined in section 1 of the Local Government: Municipal Systems Act, 2000 (Act No. 32 of 2000);
   l. a constitutional court judge, or any other judge, as defined in section 1 of the Judges' Remuneration and Conditions of Employment Act, 2001 (Act No. 47 of 2001);
   m. an ambassador, or high commissioner, or other senior representative, of a foreign government based in South Africa; or
   n. an officer of the South African National Defence Force above the rank of major-general;

b) the position of:
    a. chairperson of the board of directors;
    b. chairperson of the audit committee;
    c. executive officer; or
    d. chief financial officer,

of a company, as defined in the Companies Act, 2008 (Act No. 71 of 2008), **if the company provides goods or services to an organ of state and the annual transactional value of the goods or services, or both, exceeds an amount** determined by the Minister by notice in the *Gazette*; or

c) the position of head, or other executive, directly accountable to that head, of an international organisation based in South Africa.

ANNEXURE 3: FOREIGN PROMINENT PUBLIC OFFICIALS (FPPO)

A foreign prominent public official is an individual who holds, or has held, at any time in the preceding 12 months, in any foreign country, a prominent public function, including:

a) Head of State, or head of a country or government;
b) member of a foreign royal family;
c) government minister, or equivalent senior politician, or leader, of a political party;
d) senior judicial official;
e) senior executive of a state-owned corporation; or
f) high-ranking member of the military.

ANNEXURE 4: INFORMATION INCLUDED IN REPORTS SUBMITTED TO THE CENTRE

1. The CTR must include:

1.1. name of the Company making the report;
1.1. identifying details of the Company, on whose behalf the report is made, including a registration or license number;
1.2. contact address of the Company, on whose behalf the report is made;
1.3. type of business, or economic sector, of the Company, on whose behalf the report is made;
1.4. for a legal person, or entity, the surname, first name, date of birth, and contact details of a contact person; and
1.5. if the contact person is:
  1.5.1. a South African citizen, or resident, the identifying details of that person, and the source of identifying information from where the details were obtained; or
  1.5.2. not a South African citizen, or resident, the identifying details of that contact person, and the source of identifying information from where the details were obtained, and the issuing country thereof.
1.6. details of the transaction, or series of aggregated transactions, including:
  1.6.1. location where the transaction, or series of aggregated transactions, took place;
  1.6.2. date of the transaction, or series of aggregated transactions;
  1.6.3. value of the transaction, or series of aggregated transactions, in local currency; and
  1.6.4. description of how the transaction, or series of aggregated transactions, was conducted; and
  1.6.5. currency in which the funds were disposed of;
1.7. for each natural person conducting the transaction, or series of aggregated transactions, or legal person, or other entity, on whose behalf the transaction, or series of transactions, is conducted, the report must include as much of the following information as possible:
  1.7.1. for a natural person:
    1.7.1.1. title, gender, names and surname;
    1.7.1.2. date of birth, nationality and identification number;
    1.7.1.3. source of identifying information from where the details were obtained;
    1.7.1.4. alias, if any;
    1.7.1.5. contact address in South African;
    1.7.1.6. country of residence;
      1.7.1.6.1. if the person's country of residence is other than South Africa, contact address in the country of residence;
    1.7.1.7. contact number;
    1.7.1.8. occupation;

1.7.1.9. source of funds;
1.7.1.10. income tax number; and
1.7.1.11. employer's name, contact address and contact details;
1.7.2. for a legal person, or other entity:
1.7.2.1. name;
1.7.2.2. identifying number, if it has a number;
1.7.2.2.1. detailed information of the natural person with authority to conduct the transaction on behalf of the person, or entity; and
1.7.2.3. for a company, detailed information of at least one director of that company, and the role of that person in that company; or
1.7.2.4. for another entity, any information that is readily available.
1.8. a full description of the amount of cash, in excess of the prescribed limit, which is paid out by the Company;
1.9. an indicator, or indicators, of the circumstances that gave rise to the submission of the report.

2. The TPR must include:

2.1. name of the Company making the report;
2.2. identifying details of the Company, on whose behalf the report is made, including a registration or license number;
2.3. contact address of the Company, on whose behalf the report is made;
2.4. type of business, or economic sector, of the Company, on whose behalf the report is made;
2.5. surname, first name, date of birth, and contact details of a contact person; and
2.6. if the contact person is:
2.6.1. a South African citizen, or resident, the identifying details of that person, and the source of identifying information from where the details were obtained; or
2.6.2. not a South African citizen, or resident, the identifying details of that contact person, and the source of identifying information from where the details were obtained, and the issuing country thereof.
2.7. details of the property, including:
2.7.1. type of property;
2.7.2. description of the property;
2.7.3. physical address where the property is located;
2.7.4. identifying details of the property;
2.7.5. estimated value of the property; and
2.7.6. if the property was disposed of, the value of the disposition;
2.8. for each person, or entity, exercising control over the property, on behalf of the Company making a TPR, the report must include:
2.8.1. name;
2.8.2. identifying details, including an identity number, or a registration or licence number;
2.8.3. contact address;
2.8.4. for a natural person, contact details;
2.8.5. for a legal person, or an entity, the surname, first name, and contact details of a contact person; and
2.8.6. if the contact person is:
2.8.6.1. a South African citizen, or resident, the identifying details of that person, and the source of identifying information from where the details were obtained; or
2.8.6.2. not a South African citizen, or resident, the identifying details of that contact person, and the source of identifying information from where the details were obtained, and the issuing country thereof.
2.9. For every person who, according to the knowledge of the Company making a TPR, may have an interest in the property, the report must include as much of the following information as possible:
2.9.1. for a natural person:
2.9.1.1. title, gender, names and surname;
2.9.1.2. date of birth of the person, nationality and identification number;
2.9.1.3. source of identifying information from where the details were obtained;
2.9.1.4. alias, if any;
2.9.1.5. contact address in South African;
2.9.1.6. country of residence;

2.9.1.7. if the person's country of residence is other than South Africa, contact address in the country of residence;
2.9.1.8. contact number;
2.9.1.9. occupation;
2.9.1.10. source of funds with which the person acquired the interest in the property;
2.9.1.11. income tax number; and
2.9.1.12. employer's name, contact address and contact details;
2.9.2. for a legal person, or other entity:
2.9.2.1. name;
2.9.2.2. identifying number, if it has a number;
2.9.2.3. contact address in South Africa;
2.9.2.4. type of business conducted by the person, or entity;
2.9.2.5. country of origin;
2.9.2.6. if the country of origin is other than South Africa, the person's, contact address in the country of origin; and
2.9.2.7. source of the funds with which the person, or entity, acquired the interest in the property; and
2.9.2.8. for a company, detailed information of at least one director of that company, and the role of that person in that company; or
2.9.2.9. for another entity, any information that is readily available.

2.10. A TPR must include a description of the grounds on which the Company has reached the conclusion that the entity that owns, or controls, the property, or on whose behalf, or at whose direction, the property is owned, or controlled, is an entity mentioned in the consolidated list.

2.11. A TPR must include an indicator, or indicators, of the circumstances that gave rise to the submission of the TPR.

3. The SAR, STR, TFTR, or TFAR, must include:

3.1. name of the Company making the report;
3.2. identifying details of the Company, on whose behalf the report is made, including a registration or license number;
3.3. contact address of the Company, on whose behalf the report is made;
3.4. type of business, or economic sector, of the Company, on whose behalf the report is made;
3.5. for a natural person making the report, the person's surname, first name, date of birth, and contact details;
3.6. for a legal person, or entity, the surname, first name, date of birth, and contact details of a contact person; and
3.7. if the contact person is:
3.7.1. a South African citizen, or resident, the identifying details of that person, and the source of identifying information from where the details were obtained; or
3.7.2. not a South African citizen, or resident, the identifying details of that contact person, and the source of identifying information from where the details were obtained, and the issuing country thereof.
3.8. details of the activity/transaction, or series of activities/transactions, including:
3.8.1. location where the activity/transaction, or series of activities/transactions, took place;
3.8.2. date and time of the activity/transaction, or series of activities/transactions;
3.8.3. if the activity/transaction, or series of activities/transactions, involved property comprising money, the amount in local currency;
3.8.4. if the activity/transaction, or series of activities/transactions, involved property other than money, a description of the type of property and all identifying characteristics of the property;
3.8.5. description of how the activity/transaction, or series of activities/transactions, was conducted; and
3.8.6. if the activity/transaction, or series of activities/transactions, involved property, the estimated value of the property;
3.8.7. if the property involved in the activity/transaction, or series of activities/transactions, was disposed of:
3.8.7.1. way it was disposed of;
3.8.7.2. amount of the disposition, for property comprising money;
3.8.7.3. value for which the property was disposed of, for property other than money;
3.8.7.4. currency used in the disposition of the property, for property other than money;
3.8.8. if another institution, or person, was involved in the activity/transaction, or series of activities/transactions:
3.8.8.1. name of the other institution, or person; and
3.8.8.2. number of any account at the other institution involved in the activity/transaction, or series of activities/transactions;
3.8.9. name and identifying details of the branch, or office, where the activity/transaction, or series of activities/transactions, was conducted;

3.8.10. remarks, comments, reasons, or explanations, which the person conducting the activity/transaction, or series of activities/transactions, may have made, or given;

3.9. If any account held at the Company was involved in the activity/transaction, or series of activity/transactions, the report must include full details of each account, including:

3.9.1. account number;
3.9.2. name and identifying details of the branch, or office, where each account is held;
3.9.3. type of account;
3.9.4. currency in which the account is denominated;
3.9.5. date on which the account was opened;
3.9.6. reference numbers allocated by the Centre, and the Company, to any previous reports made, relating to the account;
3.9.7. balance in the account on the date on which the report is made;
3.9.8. status of the account immediately before the reported activity/transaction, or series of activities/transactions, was carried out; and
3.9.9. if the account was closed, the date on which the account was closed;
3.9.10. balance in the account immediately before the activity/transaction, or series of activities/transactions, was carried out;

3.10. for each signatory on the account:

3.10.1. title, gender, names and surname;
3.10.2. identifying number, nationality and date of birth;
3.10.3. source of identifying information from where the details were obtained;
3.10.4. alias, if any;
3.10.5. contact address in South Africa;
3.10.6. country of residence;
3.10.7. if the person's country of residence is other than South Africa, the contact address in the country of residence;
3.10.8. contact number;
3.10.9. occupation;
3.10.10. source of funds of the person;
3.10.11. income tax number;
3.10.12. employer's name, contact address and contact details.

3.11. for each holder of each account:

3.11.1. for a natural person:

3.11.1.1. names and surname;
3.11.1.2. identifying number and date of birth;
3.11.1.3. title, gender, nationality, and alias, if any;
3.11.1.4. contact address in South Africa;
3.11.1.5. country of residence;
3.11.1.6. country of residence is other than South Africa, contact address in the country of residence;
3.11.1.7. contact number;
3.11.1.8. occupation;
3.11.1.9. source of funds;
3.11.1.10. income tax number; and
3.11.1.11. employer's name, contact address and contact details; or

3.11.2. for a legal person, or other entity:

3.11.2.1. name;
3.11.2.2. identifying number, if it has a number;
3.11.2.3. contact address in South Africa;
3.11.2.4. type of business conducted by the person, or entity;
3.11.2.5. country of incorporation, or origin;
3.11.2.6. if the country of incorporation, or origin, is other than South Africa, the person's, contact address in the country of incorporation, or origin;
3.11.2.7. for a company, the surname, first name, date of birth, and contact details, of at least one director of that company, and the role of the person in that company;
3.11.2.8. if the person, or entity, has been closed, the date when it was closed; and
3.11.2.9. tax number of the person, or entity.

3.12. for each client of the Company, the report must include:

3.12.1. for a natural person:

3.12.1.1. names and surname;
3.12.1.2. date of birth and identification number;
3.12.1.3. alias, if any;

3.12.1.4. contact address in South African;
3.12.1.5. country of residence;
3.12.1.6. country of residence is other than South Africa, contact address in the country of residence;
3.12.1.7. contact number;
3.12.1.8. occupation;
3.12.1.9. source of funds;
3.12.1.10. income tax number; and
3.12.1.11. employer's name, contact address and contact details;

3.12.2. for a legal person, or other entity:
3.12.2.1. name;
3.12.2.2. identifying number, if it has a number;
3.12.2.3. type of business conducted by the person, or entity;
3.12.2.4. detailed information of the natural person with authority to conduct the activity/transaction on behalf of the person, or entity;
3.12.2.5. country of incorporation or origin and contact address;
3.12.2.6. if the country of incorporation, or origin, is other than South Africa, contact address in the country of incorporation, or origin;
3.12.2.7. for a company, detailed information of at least one director of that company, and the role of that person in that company.

3.12.3. for a natural person transacting on behalf of another natural person, legal person, or other entity:
3.12.3.1. title, gender, names and surname;
3.12.3.2. date of birth, nationality, and identification number;
3.12.3.3. source of identifying information from where the details were obtained;
3.12.3.4. alias, if any;
3.12.3.5. contact address in South African;
3.12.3.6. country of residence;
3.12.3.7. country of residence is other than South Africa, contact address in the country of residence;
3.12.3.8. contact number;
3.12.3.9. occupation;
3.12.3.10. source of funds;
3.12.3.11. income tax number; and
3.12.3.12. employer's name, contact address and contact details;

3.13. An SAR, STR, TFTR, or TFAR, must include a full description of the suspicious, or unusual, activity/transaction, or series of activities/transactions, including the reason why it is deemed to be suspicious, or unusual.

3.14. An SAR, STR, TFTR, or TFAR, must state what action the natural, or legal person, making the report, or other entity, on whose behalf the report is made, has taken, relating to the activity/transaction, or series of activities/transactions.

3.15. An SAR, STR, TFTR, or TFAR, must include an indicator, or indicators, of the circumstances that gave rise to the submission of the report.

ANNEXURE 5: EXAMPLES OF ACTIVITIES THAT MAY BE RELATED TO TERRORIST AND RELATED ACTIVITIES, OR MAY BE SUSPICIOUS OR UNUSUAL TRANSACTIONS

A. Examples of suspicious or unusual transactions

- Client is reluctant to provide complete information regarding their activities
- Deposits and withdrawals that are predominantly cash-based (not aligned with business)
- Significant changes in account balances
- Sudden or inconsistent change in transaction patterns
- Transaction differs from the normal financial activity of the client
- Frequent address changes
- Frequent bank account changes
- Refuses to provide KYC documents
- Provides potentially false KYC documents
- Reluctant to complete all fields on application forms
- Application for investment from a potential client in a distant location, where a comparable investment could be provided closer to home
- Application for business is outside the client's normal pattern of business
- Introduction by agent/intermediary in an unregulated or loosely regulated jurisdiction
- Introduction by agent/intermediary in a jurisdiction where organised criminal activities or corruption are prevalent
- Delay or refusal in the provision of verification information
- Atypical incident of the pre-payment of insurance premiums
- Client accepts unfavourable conditions unrelated to his/her health or age
- Transaction involves wire transfers (cross-border transactions)

B. Examples involving accounts

- Accounts that receive relevant periodic deposits and are dormant at other periods
- Dormant account containing a minimal value, suddenly received a deposit or series of deposits, followed by daily cash withdrawals, until the amounts are removed
- When opening an account, the customer refuses to provide information, attempts to reduce the level of information provided, or provides false or misleading information
- Account has several authorised signatories, but the parties appear to have no relation among each other (e.g. family or business relationship)
- Accounts held by legal entities have the same address and/or the same authorised signatories, but there is no apparent economic or legal reason
- Account opened in the name of a recently formed legal entity, has a higher than expected level of deposits, compared to the income of the founders of the account
- Opening of multiple accounts by the same person, with numerous small deposits spread across all accounts
- Accounts opened in the name of entities linked to terrorist organisations

C. Examples involving deposits and withdrawals

- Deposits for a business entity, in combinations of monetary instruments, that are atypical of the activity normally associated with the business
- Large cash withdrawals from a business account that is not normally associated with cash
- Large cash deposits, when the apparent activity is not normally associated with cash

- Mixing of cash deposits and monetary instruments in an account, where this doesn't appear to be normal
- Multiple transactions on the same day, at the same branch, using different tellers
- Structuring of deposits across multiple branches, of multiple people entering the same branch
- Deposits or withdrawals of cash, consistently just below thresholds
- Presentation of un-counted cash, once counted, the amount to be deposited is reduced to just below the threshold

D. Examples involving wire transfers

- Wire transfers ordered in small amounts, in an apparent effort to avoid triggering reporting
- Wire transfer to or from an individual, where the information has not been provided, but would be expected
- Use of multiple personal and business accounts, or accounts of non-profit organisations or charities, to collect and funnel funds, immediately or after a short time, to foreign beneficiaries
- Foreign exchange transactions performed on behalf of a customer, by a 3rd party, followed by wire transfers of funds to locations with no apparent connection to the client

E. Examples involving the characteristics of a client

- Funds generated by a business owned by individuals of the same origin, which is a country of concern
- Shared address for individuals involved in cash transactions, especially if the address is a business location and/or doesn't correspond to the stated occupation
- Stated occupation of the client isn't commensurate with the level/type of activity
- Non-profit or charitable organisations, where there appears to be no logical economic purpose, or no link to the stated activity of the organisation
- Safe deposit box opened by the client, where the business activity is unknown or unjustified
- Unexplained inconsistencies arising from identifying and verifying the client

F. Examples involving transactions linked to locations

- Transaction involving foreign currency exchanges, followed, within a short time, by wire transfers to locations of concern
- Deposits, followed, within a short time, by wire transfers, especially to or through locations of concern
- Business account with many incoming or outgoing wire transfers, which appear to have no economic or logical business purpose
- Use of multiple accounts to collect and funnel funds to a small number of foreign beneficiaries, especially in locations of concern
- Client obtains a credit instrument or engages in commercial financial transactions, involving the movement of funds to or from locations of concern, where there appears to be no logical business reasons for dealing in those locations
- Opening of accounts of financial institutions from locations of concern
- Sending or receiving funds by international transfers from and/or to locations of concern

ANNEXURE 6: EXAMPLES OF FACTORS THAT HAVE BEEN CONSIDERED, TO DETERMINE THE RISK RATINGS

A. Financial products (and products that are not defined as financial products)

- Does the product enable third parties, who are not known to the Company, to make use of it?
- Does the product allow for third party payments?
- Is another AI involved in the usage of the product?
- Can the product be funded with cash, or must it be funded only by way of a transfer to, or from, another financial institution?
- How easily and quickly can funds be converted to cash?
- Does the product facilitate the cross-border transfer of funds?
- Is the offering of the product subject to regulatory approval and/or reporting?
- What does the product enablement processes entail, and to what extent does it include additional checks, such as credit approvals, disclosure of information, legal agreements, licensing, regulatory approvals, registration, involvement of legal professionals?
- To what extent is the usage of the product subject to parameters set by the Company, for example, value limits, duration limits, transaction limits, or to what extent is the usage of the product subject to penalties, when certain conditions are not adhered to?
- Is the usage of the product subject to reporting to regulators and/or to the market?
- Does historic transaction monitoring information indicate a lower, or higher, prevalence of abuse of the product for money laundering, or terrorist financing purposes?
- What is the intended target market segment for the product, for example, general public, high net worth individuals, larger corporates, state owned entities, minors?
- Is the usage of the product subject to additional scrutiny from a market abuse, or consumer protection, perspective?
- What is the time duration for the conversion of funds, or property, through the usage of the product?
- Is the product an industry regulated product?
- Does the product allow for the flow of physical cash?
- Are there specific conditions that must be met, or events that must happen, for clients to have access to funds, or property?
- Does the usage of the product entail structured transactions, such as periodic payments at fixed intervals, or does it facilitate an unstructured flow of funds?
- What is the transaction volume facilitated by the product?
- Does the product have a cooling off period, which allows for a contract to be cancelled without much formality and a refund of moneys paid?
- Is the product offered, a short term, or longer-term, contractual relationship?
- Does the product require a payment from a same name account/facility, to facilitate the opening of the product?

B. Delivery channels

- Is the product offered to prospective clients directly, or through intermediaries?
- Are prospective clients on-boarded through direct interaction, or through intermediaries?
- Do clients transact by engaging with the Company directly, or through intermediaries?
- Where clients interact through intermediaries, are the intermediaries subject to licencing and/or other regulatory requirements?
- Are products and services acquired, or transactions performed, via an exchange?
- Are products and services traded in secondary markets?
- To what extent does the usage of the product require the participation of the Company, or the application of the Company's systems and transaction platforms?
- What are the payment systems, or other technological platforms, that support the functioning of the product?

- Are prospective clients on-boarded through non-face-to-face processes and/or do they use the Company's products and services through non-face-to-face transactions?

C. Clients

- Is the client an individual, or legal person?
- If the client is a legal person, is it part of a complex, or multi layered, structure of ownership, or control?
- What information does the client provide concerning their source(s) of income?
- What is the nature of the client's business activity, for example, does the activity involve transacting in large amounts of cash, cross-border movements of funds, trading in sensitive, controlled, or sanctioned, commodities?
- What is the nature of the type of the products and services offered by the client?
- Does the client operate solely within South Africa, or does it have cross-border operations?
- Is the client's product selection rational, with a view to support their business, or personal needs?
- Does the client occupy a prominent public position, or perform a public function, at a senior level, or does it have such individuals within its ownership and control structure?
- Is there adverse information about the client available from public, or commercial sources?
- Is the client known to be subject to financial sanctions?
- Does the client operate in a sector, or industry, that is subject to specific standards, market entry, or market conduct, requirements, other regulatory requirements (especially AML/CFT measures)?
- Is the client supervised for compliance with AML/CFT measures?
- Has the client been penalised, or subjected to adverse findings, relating to failures to implement AML/CFT measures?
- Has the client been in a long-term business relationship with the Company?
- What has been the patterns of transaction behaviour of a client, who has a history of a business relationship with the Company, for example, speed, frequency, size, volume?
- Has the Company previously observed suspicious, or unusual, activities, or transactions, on the part of the client?

D. Geographic locations

- Is the client domiciled in South Africa, or in another country, or does the client operate in another country?
- Is the client's country of domicile a FATF member?
- Do clients who are domiciled outside of South Africa, or operate outside South Africa, engage with the Company in South Africa, or through branches, subsidiaries, or intermediaries, outside South Africa?
- Have credible sources identified geographic locations from where clients engage with the Company, as high-risk jurisdictions?
- Are the geographic locations from where clients engage with the Company subject to sanctions regimes?
- If the client is a legal person, has it been incorporated in a country that has been identified by credible sources as a high-risk jurisdiction, or in a country that is the subject of a sanctions' regime, or does it operate in such a country?
- Has an international body, a domestic regulator, or supervisory body, or other credible source, expressed concern with weak regulatory measures against money laundering and terrorist financing, weak transparency requirements for beneficial ownership of corporate structures, or weak institutional frameworks, such as supervisory, law enforcement and prosecuting agencies, in relation to a geographic location from where clients engage with the Company?
- Are the geographic locations from where clients engage with the Company known to applying excessive client confidentiality?

E. Other

- The demographics of a society, its social and economic circumstances, trade dependencies, GDP.
- Financial inclusion objectives and how particular products and services contribute to this.
- The impact of the Company's business strategy on its ML/TF risk profile.
- The ML/TF impact on the Company, as a result of having operations in jurisdictions (i.e. jurisdictional risk associated with the Company itself, and not its clients).
- The communication of risk factors by authorities, based on their understanding of ML/TF risks, at a national, or sectoral level.
- Trends and typologies identified by the FATF and other international bodies, which indicate jurisdictions, structures, products and services, favoured by money launderers and terrorist financiers.
- Anti-fraud measures that may be in place in the Company.

- Consideration of previous regulatory fines.
- Frequency of internal audit findings and the outcomes thereof.

ANNEXURE 7: CUSTOMER DUE DILIGENCE FORM (MANUAL)

Customer due diligence form	
Client	
Part 1: Information (Financial adviser/intermediary/administrator to complete)	
Business relationship/single transaction information	
Financial product/service client is investing into/purchasing	Crypto asset trading platform: intermediary services for the buying, and selling, of crypto assets
	Crypto asset trading platform: trading, conversion, or exchange, of crypto assets, into fiat currency, or other value
	Crypto asset trading platform: trading, conversion, or exchange, of crypto assets, into other crypto assets
	Crypto asset trading platform: trading, conversion, or exchange, of fiat currency, or other value, into crypto assets
Business relationship or single transaction	Business relationship (new)
Nature of entering into this business relationship	Medium-term to long-term investment horizon
Purpose of entering into this business relationship	Investment-seeking protection from fiat currency depreciation
Client information	
Source of funds (activity that generated funds for this investment)	Disposable income
Details of source of funds (including investment value & how funds were transferred)	Disposable income
Source of funds (expected activity that generates funds for transacting during this business relationship)	Disposable income
Details of source of funds (including expected frequency of transacting during this business relationship)	Disposable income
Source of wealth (activities that generated total net worth, produced funds & property)	Salary plus bonuses

Nature of client's business/partnership/trust	N/A				
How beneficiaries are determined (as per trust deed)	N/A				
Ownership & control structure (full details)	N/A				
Client and involved persons information					
Information	**Client (each person)**	**Acting for (each person)**	**Beneficial owners (each person)**	**Trust parties (each person)**	**Partners (each person)**
Type	SA individual-adult (not retired)	N/A	N/A	N/A	N/A
Full name	0	N/A	N/A	N/A	N/A
Trading name	N/A	N/A	N/A	N/A	N/A
Identity number (ID/passport/registration)		N/A	N/A	N/A	N/A
Birth date		N/A	N/A	N/A	N/A
Birth place		N/A	N/A	N/A	N/A
Nationalities	South African	N/A	N/A	N/A	N/A
Incorporation country	N/A	N/A	N/A	N/A	N/A
Incorporation date	N/A	N/A	N/A	N/A	N/A
Telephone numbers		N/A	N/A	N/A	N/A
Email address		N/A	N/A	N/A	N/A
Physical address in South Africa		N/A	N/A	N/A	N/A
Physical address outside South Africa		N/A	N/A	N/A	N/A
Postal address		N/A	N/A	N/A	N/A
South African income tax number		N/A	N/A	N/A	N/A
South African VAT number	N/A	N/A	N/A	N/A	N/A
Foreign income tax numbers and countries		N/A	N/A	N/A	N/A
Profession/Occupation		N/A	N/A	N/A	N/A
Employer		N/A	N/A	N/A	N/A
Banking details		N/A	N/A	N/A	N/A
Risk rating (before screening)	Moderate risk				
Notes by financial adviser/intermediary (including whether the individual acted suspiciously)					
Documents to be provided by client (and other people involved in business relationship or single transaction), to verify information					
Very low risk	**Click on + sign in left margin, to view verification documents per client type.**				

Very low risk: **ALL** clients (**PLUS** relevant documents for client type)	**ALL clients (PLUS relevant documents for client type)** Ø Proof of banking details (bank issued document) Ø Agreement/application form/policy (and supporting documents), for establishing business relationship Ø Proof of authority to act, **IF** person(s) is/are acting on behalf of client or person(s) whom client is/are acting on behalf of) (e.g. power of attorney, affidavit, court order) Ø FSCA FAIS License Certificate (including Annexures), **IF** client is an FSP
Very low risk: South African citizens or residents (**PLUS** documents required for **ALL** very low risk clients)	**South African citizens or residents (PLUS documents for ALL very low risk clients)** Ø Identity documents issued by the South African governement (e.g. green bar-coded identity document, smart card, passport, driver's license, birth certificate (for minors) (note: copy of the smart card must include the front and back)
Low risk	**Click on + sign in left margin, to view verification documents per client type.**
Low risk: **ALL** clients (**PLUS** relevant documents for client type)	**ALL clients (PLUS relevant documents for client type)** Ø Proof of banking details (bank issued document) Ø Agreement/application form/policy (and supporting documents), for establishing business relationship Ø Proof of authority to act, **IF** person(s) is/are acting on behalf of client or person(s) whom client is/are acting on behalf of) (e.g. power of attorney, affidavit, court order, directors'/members'/trustees' resolution) Ø FSCA FAIS License Certificate (including Annexures), **IF** client is an FSP
Low risk: South African citizens or residents (**PLUS** documents required for **ALL** low risk clients)	**South African citizens or residents (PLUS documents stated above, for ALL low risk clients)** Ø Identity documents issued by the South African governement (e.g. green bar-coded identity document, smart card, passport, driver's license, birth certificate (for minors) (note: copy of the smart card must include the front and back) ØProof of physical residential addresses (document from independent third party, with issue date not older than 3 months) (e.g. utility bill, telephone bill (landline or mobile), retail invoice, insurance policy, lease or rental agreement)
Low risk: Foreign nationals (**PLUS** documents required for **ALL** low risk clients)	**Foreign nationals (PLUS documents stated above, for ALL low risk clients)** Ø Passport ØProof of physical residential addresses (document from independent third party, with issue date not older than 3 months) (e.g. utility bill, telephone bill (landline or mobile), retail invoice, insurance policy, lease or rental agreement)
Low risk: Companies/close corporations (**PLUS** documents required for **ALL** low risk clients)	**Companies/close corporations (PLUS documents stated above, for ALL low risk clients)** Ø Founding documents (registration certificate, amended registration certificate, notice of incorporation, amendment to company information, name change certificate) ØSARS issued document (to verify Trading Name, if applicable) Ø Proof of physical business addresses (document from independent third party, with issue date not older than 3 months) Ø Share register (reflecting current shareholders and ownership details) Ø Shareholding structure (e.g. organogram) and founding documents of majority shareholders (according to person type) ØFor each individual who is a beneficial owner, director/member, person authorised to act, documents required for South African citizens or residents OR Foreign nationals (according to person type)
Low risk: Trusts (**PLUS** documents required for **ALL** low risk clients)	**Trusts (PLUS documents stated above, for ALL low risk clients)** Ø Founding documents (trust deed, amendments to trust deed) Ø Authorisation letter from the Master of the High Court (latest letter, which reflects list of current trustees) ØFor each founder/doner, trustee, beneficiary, person authorised to act, documents required for South African citizens or residents OR Foreign nationals (according to person type)
Low risk: Retirement funds/medical schemes (**PLUS** documents required for **ALL** low risk clients)	**Retirement funds/medical schemes (PLUS documents stated above, for ALL low risk clients)** Ø Founding documents (registration certificate, amended registration certificate, rules of the fund) ØSARS issued registration document (if applicable) Ø Proof of physical business addresses (document from independent third party, with issue date not older than 3 months)

	ØFor each individual who is a trustee, principal officer, person authorised to act, documents required for South African citizens or residents OR Foreign nationals (according to person type)
Low risk: Partnerships (**PLUS** documents required for **ALL** low risk clients)	**Partnerships (PLUS documents stated above, for ALL low risk clients)** Ø Founding documents (partnership agreement) Ø Proof of physical business addresses (document from independent third party, with issue date not older than 3 months) ØFor each individual who is a partner, person exercising control, person authorised to act, documents required for South African citizens or residents OR Foreign nationals (according to person type)
Moderate risk	**Click on + sign in left margin, to view verification documents per client type.**
Moderate risk: **ALL** clients (**PLUS** relevant documents for client type)	**ALL clients (PLUS relevant documents for client type)** Ø Proof of banking details (bank issued document) Ø Agreement/application form/policy (and supporting documents), for establishing business relationship Ø SARS issued document(s) reflecting tax numbers Ø Proof of authority to act, **IF** person(s) is/are acting on behalf of client or person(s) whom client is/are acting on behalf of) (e.g. power of attorney, affidavit, court order, directors'/members'/trustees' resolution) Ø FSCA FAIS License Certificate (including Annexures), **IF** client is an FSP
Moderate risk: South African citizens or residents (**PLUS** documents required for **ALL** moderate risk clients)	**South African citizens or residents (PLUS documents stated above, for ALL moderate risk clients)** Ø Identity documents issued by the South African governement (e.g. green bar-coded identity document, smart card, passport, driver's license, birth certificate (for minors) (note: copy of the smart card must include the front and back) ØProof of physical residential addresses (document from independent third party, with issue date not older than 3 months) (e.g. utility bill, telephone bill (landline or mobile), retail invoice, insurance policy, lease or rental agreement)
Moderate risk: Foreign nationals (**PLUS** documents required for **ALL** moderate risk clients)	**Foreign nationals (PLUS documents stated above, for ALL moderate risk clients)** Ø Passport ØProof of physical residential addresses (document from independent third party, with issue date not older than 3 months) (e.g. utility bill, telephone bill (landline or mobile), retail invoice, insurance policy, lease or rental agreement)
Moderate risk: Companies/close corporations (**PLUS** documents required for **ALL** moderate risk clients)	**Companies/close corporations (PLUS documents stated above, for ALL moderate risk clients)** Ø Founding documents (registration certificate, amended registration certificate, notice of incorporation, amendment to company information, name change certificate) ØSARS issued document (to verify Trading Name, if applicable) Ø Proof of physical business addresses (document from independent third party, with issue date not older than 3 months) Ø Share register (reflecting current shareholders and ownership details) Ø Shareholding structure (e.g. organogram) and founding documents of majority shareholders (according to person type) ØFor each individual who is a beneficial owner, director/member, person authorised to act, documents required for South African citizens or residents OR Foreign nationals (according to person type)
Moderate risk: Trusts (**PLUS** documents required for **ALL** moderate risk clients)	**Trusts (PLUS documents stated above, for ALL moderate risk clients)** Ø Founding documents (trust deed, amendments to trust deed) Ø Authorisation letter from the Master of the High Court (latest letter, which reflects list of current trustees) ØFor each founder/doner, trustee, beneficiary, person authorised to act, documents required for South African citizens or residents OR Foreign nationals (according to person type)

Moderate risk: Retirement funds/medical schemes (**PLUS** documents required for **ALL** moderate risk clients)	**Retirement funds/medical schemes (PLUS documents stated above, for ALL moderate risk clients)** Ø Founding documents (registration certificate, amended registration certificate, rules of the fund) ØSARS issued registration document (if applicable) Ø Proof of physical business addresses (document from independent third party, with issue date not older than 3 months) ØFor each individual who is a trustee, principal officer, person authorised to act, documents required for South African citizens or residents OR Foreign nationals (according to person type)
Moderate risk: Partnerships (**PLUS** documents required for **ALL** moderate risk clients)	**Partnerships (PLUS documents stated above, for ALL moderate risk clients)** Ø Founding documents (partnership agreement) Ø Proof of physical business addresses (document from independent third party, with issue date not older than 3 months) ØFor each individual who is a partner, person exercising control, person authorised to act, documents required for South African citizens or residents OR Foreign nationals (according to person type)
High risk	**Click on + sign in left margin, to view verification documents per client type.**
High risk: **ALL** clients (**PLUS** relevant documents for client type)	**ALL clients (PLUS relevant documents for client type)** Ø Proof of banking details (bank issued document) Ø Agreement/application form/policy (and supporting documents), for establishing business relationship Ø SARS issued document(s) reflecting tax numbers Ø Proof of employment, source of funds, source of income and source of wealth Ø Proof of authority to act, **IF** person(s) is/are acting on behalf of client or person(s) whom client is/are acting on behalf of) (e.g. power of attorney, affidavit, court order, directors'/members'/trustees' resolution) Ø FSCA FAIS License Certificate (including Annexures), **IF** client is an FSP
High risk: South African citizens or residents (**PLUS** documents required for **ALL** high risk clients)	**South African citizens or residents (PLUS documents stated above, for ALL high risk clients)** Ø Identity documents issued by the South African governement (e.g. green bar-coded identity document, smart card, passport, driver's license, birth certificate (for minors) (note: copy of the smart card must include the front and back) ØProof of physical residential addresses (document from independent third party, with issue date not older than 3 months) (e.g. utility bill, telephone bill (landline or mobile), retail invoice, insurance policy, lease or rental agreement)
High risk: Foreign nationals (**PLUS** documents required for **ALL** high risk clients)	**Foreign nationals (PLUS documents stated above, for ALL high risk clients)** Ø Passport ØProof of physical residential addresses (document from independent third party, with issue date not older than 3 months) (e.g. utility bill, telephone bill (landline or mobile), retail invoice, insurance policy, lease or rental agreement)
High risk: Companies/close corporations (**PLUS** documents required for **ALL** high risk clients)	**Companies/close corporations (PLUS documents stated above, for ALL high risk clients)** Ø Founding documents (registration certificate, amended registration certificate, notice of incorporation, amendment to company information, name change certificate) ØSARS issued document (to verify Trading Name, if applicable) Ø Proof of physical business addresses (document from independent third party, with issue date not older than 3 months) Ø Share register (reflecting current shareholders and ownership details) Ø Shareholding structure (e.g. organogram) and founding documents of majority shareholders (according to person type) ØFor each individual who is a beneficial owner, director/member, person authorised to act, documents required for South African citizens or residents OR Foreign nationals (according to person type)
High risk: Trusts (**PLUS** documents required for **ALL** high risk clients)	**Trusts (PLUS documents stated above, for ALL high risk clients)** Ø Founding documents (trust deed, amendments to trust deed) Ø Authorisation letter from the Master of the High Court (latest letter, which reflects list of current trustees) ØFor each founder/doner, trustee, beneficiary, person authorised to act, documents required for South African citizens or residents OR Foreign nationals (according to person type)

High risk: Retirement funds/medical schemes (**PLUS** documents required for **ALL** high risk clients)	**Retirement funds/medical schemes (PLUS documents stated above, for ALL high risk clients)** Ø Founding documents (registration certificate, amended registration certificate, rules of the fund) ØSARS issued registration document (if applicable) Ø Proof of physical business addresses (document from independent third party, with issue date not older than 3 months) ØFor each individual who is a trustee, principal officer, person authorised to act, documents required for South African citizens or residents OR Foreign nationals (according to person type)
High risk: Partnerships (**PLUS** documents required for **ALL** high risk clients)	**Partnerships (PLUS documents stated above, for ALL high risk clients)** Ø Founding documents (partnership agreement) Ø Proof of physical business addresses (document from independent third party, with issue date not older than 3 months) ØFor each individual who is a partner, person exercising control, person authorised to act, documents required for South African citizens or residents OR Foreign nationals (according to person type)
Very high risk	**Click on + sign in left margin, to view verification documents per client type.**
Very high risk: **ALL** clients (**PLUS** relevant documents for client type)	**ALL clients (PLUS relevant documents for client type)** Ø Proof of banking details (bank issued document) Ø Agreement/application form/policy (and supporting documents), for establishing business relationship Ø SARS issued document(s) reflecting tax numbers Ø Proof of employment, source of funds, source of income and source of wealth Ø Proof of authority to act, **IF** person(s) is/are acting on behalf of client or person(s) whom client is/are acting on behalf of) (e.g. power of attorney, affidavit, court order, directors'/members'/trustees' resolution) Ø FSCA FAIS License Certificate (including Annexures), **IF** client is an FSP
Very high risk: South African citizens or residents (**PLUS** documents required for **ALL** very high risk clients)	**South African citizens or residents (PLUS documents stated above, for ALL very high risk clients)** Ø Identity documents issued by the South African governement (e.g. green bar-coded identity document, smart card, passport, driver's license, birth certificate (for minors) (note: copy of the smart card must include the front and back) ØProof of physical residential addresses (document from independent third party, with issue date not older than 3 months) (e.g. utility bill, telephone bill (landline or mobile), retail invoice, insurance policy, lease or rental agreement)
Very high risk: Foreign nationals (**PLUS** documents required for **ALL** very high risk clients)	**Foreign nationals (PLUS documents stated above, for ALL very high risk clients)** Ø Passport ØProof of physical residential addresses (document from independent third party, with issue date not older than 3 months) (e.g. utility bill, telephone bill (landline or mobile), retail invoice, insurance policy, lease or rental agreement)
Very high risk: Companies/close corporations (**PLUS** documents required for **ALL** very high risk clients)	**Companies/close corporations (PLUS documents stated above, for ALL very high risk clients)** Ø Founding documents (registration certificate, amended registration certificate, notice of incorporation, amendment to company information, name change certificate) ØSARS issued document (to verify Trading Name, if applicable) Ø Proof of physical business addresses (document from independent third party, with issue date not older than 3 months) Ø Share register (reflecting current shareholders and ownership details) Ø Shareholding structure (e.g. organogram) and founding documents of majority shareholders (according to person type) ØFor each individual who is a beneficial owner, director/member, person authorised to act, documents required for South African citizens or residents OR Foreign nationals (according to person type)
Very high risk: Trusts (**PLUS** documents required for **ALL** very high risk clients)	**Trusts (PLUS documents stated above, for ALL very high risk clients)** Ø Founding documents (trust deed, amendments to trust deed) Ø Authorisation letter from the Master of the High Court (latest letter, which reflects list of current trustees) ØFor each founder/doner, trustee, beneficiary, person authorised to act, documents required for South African citizens or residents OR Foreign nationals (according to person type)

Very high risk: Retirement funds/medical schemes (**PLUS** documents required for **ALL** very high risk clients)	**Retirement funds/medical schemes (PLUS documents stated above, for ALL very high risk clients)** Ø Founding documents (registration certificate, amended registration certificate, rules of the fund) ØSARS issued registration document (if applicable) Ø Proof of physical business addresses (document from independent third party, with issue date not older than 3 months) ØFor each individual who is a trustee, principal officer, person authorised to act, documents required for South African citizens or residents OR Foreign nationals (according to person type)
Very high risk: Partnerships (**PLUS** documents required for **ALL** very high risk clients)	**Partnerships (PLUS documents stated above, for ALL very high risk clients)** Ø Founding documents (partnership agreement) Ø Proof of physical business addresses (document from independent third party, with issue date not older than 3 months) ØFor each individual who is a partner, person exercising control, person authorised to act, documents required for South African citizens or residents OR Foreign nationals (according to person type)

Signed by financial adviser/intermediary to complete (person interacting with client)	
I confirm that I have accurately and fully completed Part 1 of this form	
Full name	
ID number	
Signature	
Date	

Customer due diligence form	
Client	**0**

Part 2: Screening & overall risk rating (to be completed by compliance officer or similar)

Information	**Client (each person)**	**Acting for (each person)**	**Beneficial owners (each person)**	**Trust parties (each person)**	**Partners (each person)**
UNSC targeted financial sanctions list	N/A	N/A	N/A	N/A	N/A
UNSC terrorist & related activities list	N/A	N/A	N/A	N/A	N/A
Foreign prominent public official (or closely associated with FPPO)	N/A	N/A	N/A	N/A	N/A
Source of funds of FPPO	N/A	N/A	N/A	N/A	N/A
Source of wealth of FPPO (activities that generated total net worth, produced funds & property)	N/A	N/A	N/A	N/A	N/A
Domestic prominent influential person (or closely associated with DPIP)	N/A	N/A	N/A	N/A	N/A
Source of funds of DPIP	N/A	N/A	N/A	N/A	N/A
Source of wealth of DPIP (activities that generated total net worth, produced funds & property)	N/A	N/A	N/A	N/A	N/A
Risk rating (after screening & compliance review)	Moderate risk				

Business relationship/single transaction permitted	YES
Signed by compliance officer (or similar)	
I confirm that Part 1 and Part 2 has been fully completed, reviewed, information has been verified, and populated on the customer due diligence information register	
Full name	
ID number	
Signature	
Date	
Senior management approval to establish high risk or very high risk business relationships or single transactions	N/A
Full name	
Designation	
Signature	
Date	

ANNEXURE 8: CUSTOMER DUE DILIGENCE PROCESS

1. Application

1.1. The initial customer due diligence process is followed for every prospective client, regardless of whether it relates to a single transaction, or a business relationship.

1.2. The ongoing customer due diligence process is followed for every existing client.

1.3. **Where possible, the AI will apply automated, or electronic, methods, to make the processes more efficient, and to replace some, or all, of the specified manual methods.**
- **The manual methods should be used, if the AI is unable to apply automated, or electronic, methods, and if the default methods are not functioning.**

2. Risk rating

2.1. The Company determines the **risk rating of the client, the financial product/service, the nature of the business relationship, with the aggregate thereof determining the overall risk rating of the business relationship**, or single transaction.

2.2. The Company applies a risk-based approach to determine the risk rating of the client, the financial product/service, the nature of the business relationship, with the aggregate thereof determining the overall risk rating of the business relationship, or single transaction.

2.3. The **information and documents required to establish and verify the identity of the client**, and the other people involved in the business relationship, or single transaction**, differs, depending on the overall risk rating of the business relationship, or the single transaction, and the client type**.

2.4. **For the alternative manual customer due diligence process**, if automated, or electronic methods are not functioning, Part 1 of the **customer due diligence form** reflects the information and documents required, to be able to know the client (and involved persons), and to determine the risk rating of the client, the financial product/service, and the nature of the business relationship.

3. Initial customer due diligence process

3.1. Employees must perform the customer due diligence process, to establish, and verify, the identity of the client, **and other people involved in the business relationship**, or single transaction, according to the risk-based approach, and **must use the customer due diligence forms, if automated, or electronic, methods have not been created**.

3.2. The **alternative manual customer due diligence forms** are used as the business continuity, and disaster recovery, process, if automated, or electronic, methods are not functioning.

3.3. A prospective new client **signs up (expresses an interest to invest), either on the AI's website/portal/mobile application, or using manual application forms**. At this point, the prospective new client provides the minimum information that is needed to identify, verify, and contact, the prospective new client, and to determine the risk rating of the prospective new client, namely:
- Full name
- Identity number
- Birth date
- Nationalities
- Physical address
- Telephone numbers
- Email address
- Profession/Occupation
- Employer
- Tax numbers (if applicable)
- Tax countries (if applicable)
- Banking details (if applicable, otherwise at the time they are required)
- Purpose of business relationship
- Nature of business relationship
- Source of funds (activity that generated funds for this investment)
- Source of funds (expected activity that generates funds for transacting during this business relationship)
- Source of wealth (activities that generated total net worth, produced funds & property)

3.4. Generally, if clients are natural persons (individuals), there are NO other people involved in the business relationship, or single transaction.

3.5. **For the alternative manual customer due diligence process**, if automated, or electronic methods are not functioning, Part 1 of the customer due diligence forms must be completed by the person interacting with the client (i.e. financial adviser/intermediary/administrator).

- Go to the "FICA customer due diligence form" template (CDD form).
- Create a version of the CDD form for the proposed new client.
- Complete all fields in Part 1 of the proposed new client's CDD form.

3.6. **For the alternative manual customer due diligence process**, if automated, or electronic methods are not functioning, the person completing Part 1 of the customer due diligence forms **must obtain all the required documents from the client** (i.e. according to the "*Documents to be provided by client (and other people involved in business relationship or single transaction), to verify information*" section of Part 1 of the customer due diligence form), **according to the calculated risk rating (before screening)** of the business relationship, or the single transaction, and the client type.

3.7. The proposed new client uploads a copy of their identity document, together with a clear photograph of them holding the identity document.

3.8. The proposed new client uploads a proof of residence.

3.9. The person interacting with the client **must verify the information provided by the prospective new client**.

3.10. Verification may be performed in two ways:

- **Manual verification**, by comparing the information provided by the prospective new client, with the documents provided by the client.
- The manual verification process is used as the business continuity, and disaster recovery, process, if automated, or electronic, methods are not functioning.
  - **For prospective new clients WITHOUT a South African identity number**, the **manual verification process** is performed.
- **Automated, or electronic, verification**, directly with the relevant regulator (for example, South African Department of Home Affairs (Home Affairs); Companies and Intellectual Properties Commission (CIPC); South African Revenue Service (SARS), or through a recognised third party verification service provider.
- **For prospective new clients WITH a South African identity number**, **ThisIsMe, Refinitiv, or another similar independent verification service provider**, is used to verify:
  - Full name
  - Identity number
  - Birth date
  - Nationalities
  - Physical address
  - Telephone numbers
  - Email address
  - Profession/Occupation
  - Employer
- **If the ThisIsMe, Refinitiv, or other similar independent verification service provider, verification process fails, the manual verification process must be performed**.

3.11. If the employee suspects that the prospective new client, or other persons associated with the client, in respect of the business relationship, or the single transaction, has provided a false, or fictitious, name, the employee will:

- not communicate his/her suspicion to the proposed new client, or other people involved in the proposed business relationship, or single transaction
- try to complete the **relevant customer due diligence forms**, as completely as possible
- terminate the proposed transaction, and **WILL NOT** establish a business relationship with the proposed new client

- report his/her suspicion **immediately** to the person responsible for reporting to the Centre, or his/her alternatives, if the responsible person is not available.
- The person responsible for reporting to the Centre (or his/her alternatives, if the responsible person is not available) will investigate reports received from employees, and consider **submitting an SAR to the Centre, within 15 days of becoming aware**.

3.12. **For the alternative manual customer due diligence process**, if automated, or electronic methods are not functioning, after completing, and signing, Part 1 of the customer due diligence form must be sent to the compliance function, or another similar function, for assessing, finalising, and approving.

- Part 1 of the customer due diligence form must be assessed by the compliance function, or another similar function.
- Part 2 of the customer due diligence form must be completed by the compliance function, or another similar function.

3.13. **For the alternative manual customer due diligence process**, if automated, or electronic methods are not functioning, the compliance function, or another similar function, must search the terrorist and related activities list (consolidated list), to determine whether the proposed new client (and other people) appears on the list, by using the online search facility provided by the UN, on the UN website (https://www.un.org/securitycouncil/content/un-sc-consolidated-list). Search for the surname, identity number, and date of birth (YYYY/MM/DD), of the person. Assess the results, and indicate whether they are false positives, or real positives.

- Make screenshots of the searches, as evidence that you performed the searches for the proposed new client, and save the evidence in the proposed new client's file.
- **Note: The UN consolidated list INCLUDES the information reflected on the targeted financial sanctions list (TFS list), available on the FIC website (https://www.fic.gov.za/International/sanctions/Pages/search.aspx). Therefore, separate searches against the TFS list should NOT be necessary.**

3.14. **For the alternative manual customer due diligence process**, if automated, or electronic methods are not functioning, the compliance function, or another similar function, must go back to the proposed new client's CDD form, to the "UNSC targeted financial sanctions list", and the "UNSC terrorist & related activities list", sections. If the proposed new client (or other person) DOES appear on the consolidated list, for being sanctioned, select "UNSC targeted financial sanctions list" from the drop-down list. If the proposed new client DOES NOT appear on the consolidated list, for being sanctioned, select "N/A" from the drop-down list. If the proposed new client DOES appear on the consolidated list, for terrorist & related activities, select "UNSC terrorist & related activities list" from the drop-down list. If the proposed new client DOES NOT appear on the consolidated list, for terrorist & related activities, select "N/A" from the drop-down list.

3.15. **For the alternative manual customer due diligence process**, if automated, or electronic methods are not functioning, the compliance function, or another similar function, must search the internet (Google searches) for adverse media about the proposed new client (or other person). If results are found, go back to the CDD form, and insert the relevant information into the "Notes by financial adviser/intermediary (including whether the individual acted suspiciously)" section.

3.16. **For the alternative manual customer due diligence process**, if automated, or electronic methods are not functioning, the compliance function, or another similar function, must determine whether the proposed new client is a Foreign prominent public official (or is closely associated with an FPPO), by checking whether their "Profession/Occupation", held at their "Employer", is considered to be one of the examples listed on the "FPPO" sheet of the "FICA customer due diligence form" document, or "Annexure 3: Foreign prominent public officials (FPPO)" of the FICA RMCP. **Internet (Google and LinkedIn) searches may be performed, to assist in determining the person's profession/occupation and/or employer**.

3.17. **For the alternative manual customer due diligence process**, if automated, or electronic methods are not functioning, the compliance function, or another similar function, must go back to the proposed new client's CDD form, to the "Foreign prominent public official (or closely associated with FPPO)" section. If the existing client IS an FPPO, select "Foreign prominent public official (or closely associated with FPPO)" from the drop-down list. If the proposed new client IS NOT an FPPO, select "N/A" from the drop-down list. **If the proposed new client is an FPPO, then obtain the source of funds, and the source of wealth, from the client, and complete the relevant fields on the CDD form**.

3.18. The compliance function, or another similar function, must determine whether the proposed new client is a Domestic prominent influential person (or closely associated with DPIP), by checking whether their "Profession/Occupation", held at their "Employer", is considered to be one of the examples listed on the "DPIP" sheet of the "FICA customer due diligence form" document, or "Annexure 2: Domestic prominent influential person" of the FICA RMCP. **Internet (Google and LinkedIn) searches may be performed, to assist in determining the person's profession/occupation and/or employer**.

3.19. **For the alternative manual customer due diligence process**, if automated, or electronic methods are not functioning, the compliance function, or another similar function, must go back to the prospective new client's CDD form, to the "Domestic prominent influential person (or closely associated with DPIP)" section. If the prospective new client IS a DPIP, select "Domestic prominent influential person (or closely associated with DPIP)" from the drop-down list. If the prospective new client IS NOT a DPIP, select "N/A" from the drop-down list. **If the proposed new client is a DPIP, then obtain the source of funds, and the source of wealth, from the client, and complete the relevant fields on the CDD form**.

3.20. The compliance function, or another similar function, must sign Part 2 of the fully completed CDD form.

3.21. **If the "Risk rating (after screening & compliance review)" is calculated to be "High risk", then the compliance function, or another similar function, must send the proposed new client's completed, and signed, CDD form to senior management, who must sign Part 2 of the form, approving, or declining, the risky business relationship. If senior management declines the risky business relationship, the person interacting with the client must notify the client that the AI will be terminating the business relationship.**

3.22. All forms, documents, and evidence of searches performed, must be saved in the proposed new client's file.

3.23. **For the alternative manual customer due diligence process**, if automated, or electronic methods are not functioning, when assessing Part 1, and completing Part 2, of the customer due diligence forms, the compliance function, or another similar function, must ensure that Part 1, and Part 2, has been fully completed, reviewed, and signed.

3.24. The compliance function, or another similar function, must populate all the information of the proposed new client onto the "FICA customer due diligence information register" (master client list), which is the master client list, to assist with determining the timing of performing the ongoing due diligence reviews**, IF the AI enters into a business relationship with the proposed new client**.

3.25. **For the alternative manual customer due diligence process**, if automated, or electronic methods are not functioning, whenever information about the client (or other person), or other aspects of the business relationship (for example, financial products/services), the CDD form, and the master client list, must be updated. The customer due diligence information register reflects all the customer due diligence information, and risk ratings, for each business relationship (i.e. customer due diligence information for all existing clients).

3.26. **For prospective clients, business relationships, or single transactions, MUST NOT be established until the full customer due diligence process has been completed. NO business relationship, or single transaction, may be established, if the full customer due diligence process has not been completed.**

- **The FICA customer due diligence process is only finished when all the required documents and information have been received, the customer due diligence form has been fully completed, signed, and dated, the scanning checks have been completed, the business relationship has been risk rated, AND the business relationship has been accepted by the AI.**
- If the employee cannot fully perform the customer due diligence process, the employee must reflect this information in the comments section of Part 1 of the CDD form, and must clearly state the dates, and related details, of each attempt to obtain the outstanding information from the client, before sending the form to the compliance function, or another similar function.
- The first attempt to complete the process is made 1 business day after the prospective new client has signed-up, with further attempts being made 4 business days after the 1st attempt, and 3 business days after the 2nd attempt.

- Attempts will be stopped after 2 weeks.
- If unsuccessful, senior management must sign Part 2 of the CDD form, **declining establishing the business relationship**, or single transaction.
- The person interacting with the client must notify the client that the AI will not be proceeding with the proposed business relationship, or single transaction.
    - **If the customer due diligence process was followed correctly, there would have been no transfer of funds, or assets, to the AI. If there was a transfer of funds, or assets, then the client's account must be frozen, until the client provides the outstanding information, because the AI may not conclude a transaction during a business relationship, or perform any act relating to a single transaction.**
    - **The employee must consider, through the person responsible for reporting to the Centre (or his/her alternatives, if the responsible person is not available), submitting an SAR, or STR, to the Centre, within 15 days of becoming aware**.

3.27. **Flow of funds: ONLY** once the Company has accepted the business relationship, will the client be notified thereof, and the client's online administration account with the Company will be activated, and be flagged as being "KYC verified".

- As part of this activation process, the client will be provided with their **unique client reference number**, and can view the banking details of the escrow (held in trust) bank account (held at Standard Bank) that is dedicated for funds collected, received, held, or in any other way, dealt with, on behalf of clients, product suppliers, or products.
- Thereafter, the client may transact, by **making an electronic transfer of ZAR into the dedicated bank account**, and inserting their unique client reference number as the transaction reference. **Cash transactions ARE NOT permitted.**
- The ZAR deposit is moved into the Luno digital wallet, held by the Company on behalf of it's clients.
- The Company buys BTC, to the value of the ZAR deposit.
- If the client is buying the EC10 bundle, the BTC is transferred from Luno, into an international crypto exchange, and the Company buys the other 9 cryptocurrencies comprising the EC10 bundle, in their relevant weightings, according to market capitalisation.
- The cryptocurrencies are transferred to deep cold storage (custody crypro in industry standard cold storage methods, for example, Ledger and Trezor).
- When the client requests a withdrawal, the above process is reversed.
- The **client provides the Company with their banking details, which the Company verifies, using ThisIsMe, or directly with the client's bank**.
- Withdrawals are only paid into the client's ZAR denominated bank account. **No foreign currency payments, and no third party payments, are permitted**.
- The client receives ZAR, paid to the client from the escrow (held in trust) bank account (held at Standard Bank).
- If the client sells the EC10 bundle, they may select to receive BTC, instead of ZAR.
- Fees earned by the Company, for the services provided, are earned as BTC. For the fees process, the Company has an "Admin" account, which is treated as a client, and earns the fees as BTC. The fees earned BTC is sold on Luno, for ZAR, which is transferred into the Company's bank account (held at Standard Bank) (the expense account).
- EasyEquities, an authorised financial services provider, is a corporate client of the Company. EasyEquities buys EC10 bundles, and sells them to its underlying clients, via its administrative platform. EasyEquities performs its own FICA customer due diligence process for its underlying clients, in terms of its RMCP.

4. Ongoing customer due diligence process

4.1. **For existing clients, no transactions are permitted during the business relationship(s), across all accounts for the client, if the full customer due diligence process has not been completed, i.e. transactions must not be permitted, and systems must indicate that the client is non-compliant.**

4.2. The Company must ensure that it has determined the **risk rating of the existing client, the financial product/service, the nature of the business relationship, with the aggregate thereof determining the overall risk rating of the existing business relationship**, or single transaction.

- The risk rating process for existing clients is performed in the same way as the initial customer due diligence process.

- The search of the consolidated list may be performed as a batch/bulk automated search process, by comparing the master client list against a downloaded version of the consolidated list.
- If the employee cannot fully perform the customer due diligence process for an existing client, the process for existing clients is performed in the same way as the initial customer due diligence process.
    - The business relationship with the existing client must be terminated, **by freezing the client's account**.
    - Attempts will be stopped 2 weeks after the first attempt has been made.
    - If unsuccessful, senior management must sign Part 2 of the form, **declining the continuation of the existing business relationship**, or single transaction.
    - The person interacting with the client must notify the client that the Company will be terminating the existing business relationship, or single transaction.
    - **The client's account must be frozen, until the client provides the outstanding information, because the Company may not conclude a transaction during a business relationship, or perform any act relating to a single transaction**.

4.3. The company will perform ongoing due diligence of all existing business relationships with clients, including:

- monitoring transactions during the business relationship, including (where necessary):
    - the source of funds, to ensure that the transactions are consistent with the Company's knowledge of the client, the client's business, and risk profile; and
    - the background, and purpose, of all complex, unusual, large transactions, and all unusual patterns of transactions, which have no apparent business, or lawful, purpose; and
- keeping information, and documents, updated, which was obtained during the customer due diligence process, to establish, and verify, the identity of the client.
- **The frequency of performing scheduled ongoing due diligence will differ, according to the overall risk rating of the business relationship. Compliance officers will perform scheduled sample monitoring.**
    - 1 Very low risk (3-year monitoring cycle)
    - 2 Low risk (3-year monitoring cycle)
    - 3 Moderate risk (2-year monitoring cycle)
    - 4 High risk (1-year monitoring cycle)
    - 5 Very high risk (1-year monitoring cycle)

4.4. While performing scheduled ongoing due diligence, the compliance function must refer to the summary of information about the client and the business relationship, reflected in the relevant **customer due diligence information register** (master client list), to assist them during the ongoing due diligence process.

4.5. Additionally, the person interacting with the existing client (i.e. financial adviser/intermediary/administrator), will regularly monitor transactions, and keep information updated, according to the overall risk rating of the business relationship.

4.6. During the transaction monitoring process, if the employee, or compliance officer, suspects that the transactions are inconsistent with his/her knowledge of the client, the client's business and/or risk profile, and if complex, unusual, large transactions, seem to have no apparent business, or lawful, purpose, the employee will:

- not communicate his/her suspicion to the client, or other people involved in the business relationship, or single transaction;
- report his/her suspicion to the person responsible for reporting to the Centre, of his/her alternatives, if the responsible person is not available.
- The person responsible for reporting to the Centre (or his/her alternatives, if the responsible person is not available) will investigate reports received from employees, and consider **submitting an STR to the Centre, within 15 days of becoming aware**.

5. Reliance agreements

5.1. The Company has established a reliance agreement with Rexsolom Proprietary Limited (Rexsolom). In the reliance arrangement with Rexsolom, the Company is the first party accountable institution, and Rexsolom

is the third party accountable institution. The reliance agreement sets out the duties and obligations of both parties. The process is summarised below.

5.2. From the effective date, Rexsolom will provide the Company with the shared client information, via electronic means, for existing shared clients, and new shared clients.

5.3. Rexsolom will provide the Company with the shared client information for each shared client as soon as reasonably possible, via electronic means.

5.4. Rexsolom will provide the Company with its RMCP, so the Company can determine, and understand, the CDD standards applied by Rexsolom.

5.5. For the shared clients, each party is responsible, on their own, for:

- assessing, and determining, their risk, and associated risk rating assigned to a shared client, according to its initial customer due diligence process, and ongoing due diligence process
- performing screening on each shared client, according to its initial customer due diligence process, and ongoing due diligence process
- conducting their own ongoing CDD on each shared client, according to its ongoing due diligence process
- complying with any reporting obligations in terms of FICA.

5.6. For the reliance arrangement between the Company and Rexsolom, there is no fee payable by either party.

6. Monitoring

6.1. The compliance officers will perform scheduled sample monitoring of the customer due diligence process, according to the compliance monitoring plan.