Vinekross Technologies Limited

Lagos, Nigeria

RC1883948

Anti-Money Laundering Compliance Policy and Programme

1. Introduction and Purpose

Vinekross Technologies Limited ("Vinekross" or the "Company") recognizes the critical importance of protecting the integrity of the global financial system from money laundering, terrorist financing, and other financial crimes. The Company is committed to deterring customers and outside parties from using the Company as a conduit for such illegal activity and is committed to its and its bank partners' compliance with all applicable laws and regulations designed to combat such illegal activities. The Company recognizes that a strong anti-financial crime programme is essential to comply with applicable laws and regulations, and to meet the expectations of the Company's shareholders, regulators, and customers.

Vinekross designed this Anti-Money Laundering ("AML") Compliance Policy (the "Policy") and its accompanying programme (the "AML Compliance programme," or collectively the "Policy/programme") to:

- Establish a framework for protecting the Company from being used to facilitate money laundering or terrorist financing or circumvent economic sanctions;
- Institute compliance with the legal and regulatory responsibilities applicable directly to the Company and/or its business partners (including the requirements to monitor, detect, prevent, and report possible money laundering, terrorist financing, sanctions breaches, and other financial crimes);
- Set forth the governing principles and mandatory minimum standards, roles, responsibilities, specific measures, and general expectations of Vinekross personnel[1] as they conduct business; and
- Communicate the Company's clear commitment to strong compliance culture.

Money laundering is the process by which persons attempt to conceal and disguise the true origin and ownership of illegal funds. Money laundering is generally viewed as a three-stage process: placement, layering, and integration:

- Placement is the introduction of unlawful proceeds into the financial system without attracting the attention of financial institutions or law enforcement;
- Layering is the moving of funds around the financial system to create confusion and complicate the paper trail; and
- Integration is the further incorporation of unlawful proceeds in the financial system through additional transactions to convert illicit funds into apparently legitimate business earnings.

Money launderers, terrorists, and other bad actors use many different types of financial products and services to support their activities. In response, Finansinspektionen and Swedish government has passed laws that make money laundering a crime and has imposed affirmative obligations

1Vinekross "personnel" includes all Vinekross employees, officers, temporary staff, contractors, and service providers, including any parent company staff involved in the operations of Vinekross.

and related AML and anti-terrorist financing laws and regulations and guidelines (collectively, "AML") on the Company and/or its business partners to detect, prevent, and report possible money laundering, financial crimes, and terrorist financing.
Government bodies and international organizations relevant to Vinekross' operations administer and enforce economic and trade sanctions based on various factors, including foreign policy concerns, terrorism, international narcotics trafficking, and the proliferation of weapons of mass destruction.

Policy Statement

It is the policy of Vinekross, its board of directors (the "Board"), and its executive management ("Executive Management") to comply fully and continuously with all applicable AML laws and related regulations. Vinekross personnel must not conduct any business activity in which he or she knowingly violates or circumvents such laws and regulations
It is also the policy of Vinekross, its Board, and Executive Management to comply fully and continuously with all the laws, regulations, and orders regarding doing business with, maintaining accounts for, or handling transactions or monetary transfers for foreign countries or foreign nationals listed under applicable sanctions programmes. Vinekross personnel must not conduct any business activity in which he or she knowingly violates or circumvents legally applicable sanctions. If Vinekross finds that it has an account for or a customer of Vinekross is included in applicable sanctions programmes, all accounts of such customer shall be blocked. Personnel must not conduct any business activity in which personnel knowingly violate legally applicable sanctions. The Board and Executive Management recognize that Vinekross requires sanctions controls in order to ensure compliance with sanctions as well as remain aligned to the Company's risk tolerance.

2. Policy/programme Scope

This Policy/programme applies to the Board, all Vinekross personnel, and all Vinekross business activities.
Appendix B lists all documents related to this Policy/programme.

3. Policy/programme Requirements

This Policy/programme requires that the Board adopt the programme and that Vinekross implement and adhere to the Policy/programme, which includes the following components:

- Designation of an AML Officer;
- Governance structure for the Policy/programme;
- Internal controls designed to ensure ongoing compliance with AML requirements applicable to the Company and its bank partners, including:
    - AML compliance risk assessment processes;
    - Risk-based frameworks for a "Know Your Customer" ("KYC") and customer due diligence programme that provides, collects, and verifies, as needed, customer information;
    - Controls to ensure compliance with sanctions laws;
    - Risk-based transaction monitoring and suspicious activity reporting, including to bank partners as appropriate;

- Regulatory reporting and record-keeping;
- Information sharing with law enforcement and other financial institutions; and
- Mechanisms designed to monitor ongoing compliance (e.g., quality assurance and audit);
- Ongoing training and development for personnel whose routine activities are relevant to AML controls; and
- Periodic independent Policy/programme review by a qualified third party to test and assess the implementation and effectiveness of the Company's Policy/programme and the adequacy of its controls over AML compliance risk.

Vinekross will document its efforts to carry out all activities pursuant to this Policy/programme. Vinekross will comply with bank partner requirements at all times, and this Policy/programme will not be construed to contradict any bank partner requirements.

3.1. Governance Structure, Roles, and Responsibilities

The Board designates the AML Officer,[2] who has responsibility for day-to-day oversight of the Company's AML compliance and execution of this Policy/programme. The AML Officer reports directly to the Vinekross chief executive office ("CEO") and has direct accountability, and access, to the Board as needed.[3]

The AML Officer and his/her team are independent of the Company's other teams and have the authority to cross departmental lines. They will have unrestricted access to any business records, IT systems, or any other business locations to which they require access in order to fulfil their responsibilities.

The following table summarizes roles and responsibilities for development, implementation, oversight, and review of this Policy/programme.[4] As Vinekross' operations mature, its full-target operating model will be achieved; as such, short-term coverage of certain responsibilities may be provided by identified individuals.

Responsible Party	Role/Responsibility
Board of Directors (or a delegated committee thereof)	• Designate a AML Officer (Policy/programme Owner) and a Backup Policy/programme Owner; • Review and approve this Policy/programme and adopt revisions as necessary, at least annually; • Review, approve, and oversee Company-wide initiatives related to this Policy/programme; • Review escalated issues related to this Policy/programme and resolve them; • Review compliance reports related to this Policy/programme and act on them as needed; • Ensure that the AML Officer (Policy/programme Owner) has

2Unless determined otherwise by the Board, the Chief Compliance Officer serves as the AML Officer.

3As Vinekross' business and management structure expands, it may implement management-level executive committee(s) responsible for overseeing the Policy/programme, as appropriate.

4Vinekross will at least initially be a small organization that does not have multiple layers of management. As and when Vinekross grows, the AML Officer will amend this Policy/programme to clarify the responsibilities in relation to the Policy/ programme.

Responsible Party	Role/Responsibility
	sufficient authority to carry out his or her duties; • Oversee the Policy/programme, assessing its effectiveness via an independent test by a qualified third party at least annually; • Approve the AML compliance risk assessment required by this Policy/programme; and • As applicable, review feedback from regulatory examinations or correspondence relating to the Policy/programme and receive reports on any remedial action necessary.
Executive Management	• Promote a strong culture of compliance at Vinekross; • Ensure that the AML Officer (Policy/programme Owner) has sufficient authority to carry out all duties related to this Policy/programme; • Ensure that the Company has sufficient resources, including personnel and systems, to implement and meet the objectives of this Policy/programme; • Hold management and all stakeholders accountable for resolution of corrective actions related to this Policy/programme; • Communicate this Policy/programme and its requirements to Vinekross personnel within their area of responsibility; • Implement this Policy/programme and other applicable policies and procedures within their area of responsibility; • Ensure that employees under their supervision receive appropriate compliance training on this Policy/programme; • Review and approve with the AML Officer any Policy/programme exceptions; • Ratify lowering a monitoring threshold or imposing a new threshold; • Review the AML compliance risk assessment required by this Policy/programme; • Review the results of independent testing; • Review the AML Officer's recommended Policy/programme revisions; and • As applicable, review feedback from regulatory examinations or correspondence relating to the Policy/programme and receive reports on any remedial action necessary.
General Counsel[5]	• Interpret laws and regulations; • Provide advice and counsel regarding the requirements of applicable laws, regulations, and Company policies to all stakeholders; • Review and approve all customer-facing documents, and new or significantly revised products, services, geographies, and business practices; and

5Vinekross may initially consult outside legal counsel while it expands its management structure to include a General Counsel.

Responsible Party	Role/Responsibility
	• Keep Financial Crimes Enforcement Network ("FinCEN") registration and relevant state licenses current.
Policy/programme Owner (AML Officer)	• Develop and present this Policy/programme for Executive Management review and for Board review and approval, initially and going forward at least annually; • Implement and maintain this Policy/programme and related procedures; • Maintain sufficient staffing, in both numbers and qualifications, to implement the Policy/programme effectively, and request additional resources from Executive Management as needed. • Communicate this Policy/programme to business and other functional areas; • Ensure all Vinekross personnel receive appropriate training on this Policy/programme and that Vinekross documents such training and attendance; • Review and provide guidance, including through engaging outside legal counsel as appropriate, the requirements of applicable laws, regulations, and Company policies, to all stakeholders; • Maintain systems, procedures, reports, and other controls used to support efforts to comply with this Policy/programme, including ensuring that each function conducts on-going monitoring of the effectiveness of its compliance controls, and promptly alerts Executive Management and the Board on any material deficiencies or weaknesses or non-compliance. Institute and monitor corrective action to remedy any deficiencies found; • Review any changes to AML compliance- and sanctions-related laws, regulations, guidance, or regulatory expectations and ensure that the Company implements processes to remain fully in compliance with its AML obligations and regulatory expectations; • Perform the necessary analysis to determine the ongoing effectiveness of the Policy/programme, and review and refresh the Policy/programme, at least annually and more frequently as circumstances require, and ensure that this takes into account applicable law and supervisory or relevant third-party input; • Make recommendations for addressing weaknesses or new requirements to the Board, and report them to Executive Management; • Approve exceptions to this Policy/programme and maintain a written record of exceptions, including reasons for granting them; • Conduct an AML compliance risk assessment prior to or within three (3) months of operations commencing, and continue to update it annually;

Responsible Party	Role/Responsibility
	• Update the AML compliance risk assessment in light of any issues raised during independent testing; • Set transaction monitoring thresholds and adjust them as needed in response to emerging patterns of activity, documenting the rationale for all threshold changes; • Ensure that the Company fully meets AML reporting and OFAC requirements in a timely fashion applicable to its operations or to its business partners, including designing appropriate controls, conducting testing of their effectiveness, and preparing annual reports to OFAC on the total of blocked funds; • Establish systems and procedures to receive, document, respond to, and evaluate information sharing requests; • Review the AML implications of any new or significantly revised products, services, distribution channels, geographies, initiatives or business practices, and advise Executive Management on necessary steps to mitigate the money laundering and/or sanctions risk; • Provide input into the performance of key employees in meeting their responsibilities under this Policy/programme; • Provide periodic reports to the Board and Executive Management, at least annually, on the state of AML compliance, testing and monitoring reports, and any significant emerging issues; • Provide annual reports to Vinekross' bank partners on the state of AML compliance, testing and monitoring reports, reports on complaint trends, and any significant emerging issues; • Report potentially suspicious activity to Vinekross' bank partners on an on-going basis, and alert law enforcement as needed; • Establish a regular quality assurance programme and ensure that the Company's approach to testing AML compliance is consistent with the overarching compliance testing approach; • Ensure adequate staffing of critical programme functions; • Oversee all service providers whose activities impact the Policy/programme; • In conjunction with legal counsel, approve contracts and agreements with affiliated and third-party service providers that impact the implementation of this Policy/programme to ensure that every contract clearly identifies the service provider's roles, responsibilities, performance standards, reporting obligations, and liabilities; and • As needed, liaise with regulators on AML compliance issues.
Backup Policy/programme Owner (Deputy	• Perform AML Officer's responsibilities under this Policy/programme in the event that he or she cannot do so (or otherwise delegates to the Deputy AML Officer responsibility for

Responsible Party	Role/Responsibility
AML Officer)[6]	a specific action contemplated by this Policy/programme).
Vinekross Personnel (All Employees and Third-Party Service Providers)	• Promote a strong culture of compliance at Vinekross; • Know their responsibilities under this Policy/programme and ensure they remain in compliance; • Ensure they complete required AML compliance training; • Ensure they implement the Policy/programme within their sphere of responsibility and deliver compliance outcomes; • Notify and seek the approval of the AML Officer (Policy/programme Owner) in advance of all proposals for new or modified products, services, geographies, distribution channels, or initiatives that might affect money laundering and sanctions risk; • Identify compliance weaknesses within their areas of responsibility related to this Policy/programme, and promptly alert relevant executive leaders and the Policy/programme Owner; • Report unusual or suspicious activity to the AML Officer; • Grant the Policy/programme Owner, or designee, unrestricted access to business records, systems, or locations necessary to fulfil the duties described in this Policy/programme; and • For leaders of business areas: submit plans for any new or substantially modified policies, procedures, or controls for review and approval by the Policy/programme Owner.

3.2. Risk Tolerance Statement and Business Decisions

The Company understands that transactions and withdrawals pose a potential risk for money laundering and/or terrorist financing and sanctions breaches. The Company's risk tolerance for money laundering risk is low; the Company's has zero tolerance for any breach of this Policy/programme's sanctions compliance requirements. The Company will not accept either natural person or legal entities as customers (both existing and new customers) if they are Specially Designated Nationals ("SDNs"). Therefore the Company requires a robust control environment with low error rates for due diligence after applying internal controls. As a result, the AML Officer will participate in business decisions that affect the Company's AML compliance risk, such as changes to permissible customer types, etc. The Company will adhere to certain standards to limit these risks.

Vinekross sets appropriate limits on the customer types accepted and the number of permitted accounts and their usage, commensurate with the Company's money laundering and sanctions risk in its activities. At a minimum, Vinekross limits customer accounts to the following, unless otherwise approved by the AML Officer:

- Customers who are verified other than those residing in Burma, Côte d'Ivoire, Democratic People's Republic of North Korea, Democratic Republic of the Congo, Eritrea, Former Federal Republic of Yugoslavia, Iran, Iraq, Lebanon, Liberia, Libya, Japan, United States of America, Somalia, Sudan, Syria, and Zimbabwe;

6The Board may designate the CEO as the Deputy AML Compliance Officer.

- Customers who are established and reputable foreign entities, excluding those established in Burma, Côte d'Ivoire, Democratic People's Republic of North Korea, Democratic Republic of the Congo, Eritrea, Former Federal Republic of Yugoslavia, Iran, Iraq, Lebanon, Liberia, Libya, Japan, New Zealand, United States of America, Somalia, Sudan, Syria, and Zimbabwe or having principals residing therein;
- Transactions in USD, EUR, GBP, SEK, AUD, CAD, CHF, JPY, NZD, NOK, TRY, XAG, XAU;
- Source of funds allowed: ACH, wire, debit card, credit card;
- Withdrawals are first credited back to the Vinekross account holder's original source of funding. Thereafter, withdrawals are processed via wire transfer; and

3.3. Internal Controls and Establishment of AML Compliance programme

Vinekross will maintain controls as necessary to mitigate the AML risks presented by its customers, products and services, and operating geographies to an acceptable level.
Vinekross may rely on a third party to operate particular compliance controls or systems. Vinekross and the AML Officer ultimately remain responsible for satisfying regulatory obligations and should establish effective oversight processes for any outsourced tasks.
The AML Officer oversees the development and implementation of internal controls sufficient to ensure compliance with this Policy/programme, including the following.

3.3.1. Know Your Customer programme

The Company's risk-based KYC programme has three components: a customer identification programme ("CIP") that allows the Company to identify and verify the identity of its customers with reasonable assurance; a customer due diligence ("CDD") programme; and an enhanced due diligence ("EDD") programme for customers with indicators of heightened risk.

3.3.1.1. Customer Identification programme

Vinekross' CIP is a fundamental control in preventing the Company from becoming involved in money laundering, terrorist financing, or sanctions breaches. The Company's policy is to ensure that it has a reasonable belief that it knows the true identity of its customers at account opening. This means that identification information has been obtained for each customer and that independent means have been used to verify some or all of the identification information.
This Policy/programme covers all Vinekross customers.[7] Customers include anyone that opens an account, including individuals and corporations and other legal entities.
Vinekross' policy is to collect the following identity information online or on a mobile application for all of its customers at account opening before allowing the customer to deposit funds or conduct transactions:
Individuals

- Full legal name;
- Date of birth;
- Government identification number or Individual Tax Identification Number ("ITIN"));
- Current physical street address;
- E-mail address;
- Mobile telephone number; and

7"An individual, a corporation, a partnership, a trust or estate, a joint stock company, an association, a syndicate, joint venture, or other unincorporated organization or group.

- Valid payment method information, which is the customer's bank account information (financial institution, account type, routing number, and account number).

Legal Entities

- Full legal name;
- Government identification number (such as the tax identification number ("TIN")); and
- Current physical street address;
- Email address;
- Telephone number;
- Principal account holder's[8] full legal name. The legal entity's principal account holder is also required to complete CIP, as described above; and
- Valid payment method information, which is the customer's bank account information (financial institution, account type, routing number, and account number).

3.3.1.1.1. Verification

The Company[9] verifies at the time of account opening the identity of each customer, including their name, government identification number, and address, through documentary verification methods of customer information collected. Documentary means of verification of customer identification refers to methods that rely on the customer presenting documentation that shows existence of the entity.

Individuals

Documents that evidence the existence of an individual are original government-issued, or agencies thereof, documents with a photograph, which contain the name and either an identification number or date of birth. When accounts are applied for, the document must always be sighted; the documents must be sighted through live connection or screenshots/photos. Such documents may include:

- Valid passport;
- Current driver's license;
- Current Visa;
- Current non-driver photo ID card;
- Current armed forces identification; and
- Current permanent resident card.

Additionally, the customer's address needs to be verified. This may be through documents such as the following:

8The principal account holder is the key decision-making party for the product or service with whom Vinekross is engaged.

9Vinekross may contract an SLA with a third party to organize and review customer information. The service provider would be subject to the Oversight of Outsourced Service Providers requirements specified in this Policy/programme.

- Third-party data bases, such as LexisNexis;
- TIN Notification;
- Government websites;
- Copy of correspondence between the customer and the governmental authority;
- Copy of customer's utility bill (dated within the past three months);
- Copy of current bank statement (dated within past three months);
- Google or other search engines;
- Copy of Title to Property;
- Copy of executed note and mortgage; or
- Copy of executed lease agreement.

Legal Entities

Documents that evidence the existence of an entity other than an individual are required. Documents for entities are original documents issued by governments or agencies thereof bearing the seal of the issuing government body or certified by the government body and include:

- Certificate of good standing;
- Government-issued business license;
- Certified formation documents;
- Articles of incorporation;
- Articles of organization
- Articles of association;
- Signed limited partnership agreement;
- Signed general partnership agreement;
- Certificate of trade or business name;
- Trade extracts; and
- Trust instrument.

3.3.1.1.1.1. Record-Keeping

Vinekross will make and maintain records with regard to the verification of customer identity. Vinekross will retain the original of any application form and all relevant records received. A record must be made of the description of any documents relied upon to verify the identity of a customer, including the document's type, identification number, place and date of issuance, and expiration date; a copy of the document(s) satisfies the requirement.

Vinekross will electronically retain all CIP information for at least five years after the date of the customer's most recent transaction or transaction attempt.

3.3.1.1.1.2. Exceptions, Extensions, and Lack of Verification[10]

In limited circumstances, the AML Officer may grant an exception to the CIP requirements including determining whether account activity must be restricted or transactions monitored. The AML Officer and at least one member of Executive Management is required to review and confirm/approve any such exceptions. These restrictions remain in place until the verification process is complete or the account or relationship is terminated.

The Company must ensure that proper verification of customer identification for each customer is performed before a new account is opened. However, the AML Officer may grant a temporary extension of thirty (30) calendar days for completing the CIP process. These exceptions must be monitored for aging and completion purposes and reported to Executive Management.

Vinekross will not allow customers awaiting identity verification to deposit funds or conduct transactions of any kind. Vinekross' policy is to not permit individuals or legal entities who fail customer verification to maintain accounts of any kind. In the event that: the customer cannot or will not provide the CIP information requested; or the customer's identity cannot be verified with the information provided and the customer cannot subsequently provide sufficient proof of identity; or there are anonymous accounts or accounts under fictitious names; or the customer has provided information that is false or contains significant inconsistencies that cannot be resolved after further investigation, then the Company will suspend the due diligence and on-boarding process, notify the AML Officer, and the Company will not enter a relationship with the customer or open the account, or the Company will exit the existing relationship within thirty (30) calendar days. If appropriate, the AML Officer may escalate such customers for potential investigation of suspicious activity if Vinekross identifies reportable suspicious activity identified in the due diligence processes.

10Pending authentication or failure of the authentication process is grounds for not permitting customer activity or the opening of the customer account.

3.3.1.2. Customer Due Diligence

3.3.1.2.1. Customer Due Diligence Requirements

Vinekross performs CDD and collects additional customer information for all customers, as follows: Individuals

- Source of funds;
- Annual income;
- Expected product usage (e.g., wallet, trading, or both);
- Account activity (expected monthly dollar amounts for wallet balances, number of monthly exchange transactions, and number of wallet digital asset transfers);[11] and
- Occupation.

Legal Entities

- Source of funds;
- Most recent audited financial statements, if they exist;
- Expected product usage and account activity;
- Industry; and

Politically Exposed Persons (PEP)

- Source of Funds
- Source of Wealth
- Bank Statement (for account activities)
- Most recent audited financial statements
- The AML Officer will go through the docs manually and verify financial statements from the financial institution and business sources mentioned.

11After on-boarding the customer, Vinekross will continue to keep this information updated on a periodic and risk-based basis.

- Legal entity ownership structure.
    - The Company requires, for all legal entity customers, collection of information on the customer's ownership structure and the identification of beneficial owners and the ultimate parent. A "beneficial owner" is a legal entity or individual that directly or indirectly owns or controls 25% or more of a customer. A customer can have any number of beneficial owners or the customer may have none. An "ultimate beneficial owner" ("UBO") is an individual or legal entity that directly or indirectly owns or controls 25% or more of a customer and does not itself have any individual or legal entity with a controlling interest of 25% or more. The UBO is at the top of the ownership structure (e.g., "top of the house"). A customer might have up to four UBOs or the customer may have none. For Politically Exposed Persons ("PEPs"), the threshold for determining a UBO is 10% or more.
    - An "ultimate parent" is a legal entity, not an individual, who directly or indirectly owns or controls more than 50% of a customer and does not itself have a legal entity with a controlling interest of more than 50%. A customer usually has one ultimate parent but in rare circumstances will have none. This situation would occur when Vinekross has a customer that is the "top of the house" entity.
    - As part of documenting the ownership structure of a customer, all beneficial owners (e.g., 25% or more ownership) must be identified including the full legal name and the percentage ownership.

In addition, since account applications occur online or through a mobile application, Vinekross may at account opening or during the CDD process collect information for other purposes that will deepen its understanding of customer identity and help further assess risk, including telephone usage, IP address and location information, and social networking and public record information. Vinekross will collect this information online using a web browser or mobile application.

Prior to the completion of CDD, Vinekross will not allow customers to deposit funds or conduct transactions of any kind. Vinekross' policy is to not permit individuals or legal entities who fail required CDD to maintain accounts of any kind. In the event that: CDD measures cannot be applied; the customer cannot or will not provide the CDD information requested; and/or the customer has provided information that is false or contains significant inconsistencies that cannot be resolved after further investigation, then then the Company will suspend the due diligence and on-boarding process, notify the AML Officer, and the Company will not enter a relationship with the customer or open the account, or the Company will exit the existing relationship within thirty (30) calendar days. If appropriate, the AML Officer may escalate such customers for potential investigation of suspicious activity if Vinekross identifies reportable suspicious activity identified in the due diligence processes.

3.3.1.3. Enhanced Due Diligence

Vinekross conducts EDD to assess the risks associated with its users and expected transaction activity on a risk-based basis. Customers subject to additional due diligence include:

- Any customer identified as a Higher-Risk Customer type (in the section below); and

- Any customer with gross fiat currency deposits or withdrawals of $50,000[12] or more over the previous twelve (12) months; and

3.3.1.3.1. Low, Medium , High Risk Customer types

The Company has identified certain customer types as presenting a greater likelihood of money laundering and sanctions risks.

Low risk customer type:

- Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile.
- Government Departments and Government-owned companies, regulators and statutory bodies etc.

Medium risk customer type:

- Persons in business/industry or trading activity where the area of his residence or place of business has a scope or history of unlawful trading/business activity.
- Where the client profile of the person/s opening the account, according to the perception of the Company is uncertain and/or doubtful/dubious

High Risk Customer Type:

- Customers identified as PEPs;
- Embassy, foreign consulate, and foreign consulate employee customers;
- Customers subject to a sanctions Voluntary Self-Disclosure;
- Foreign bank customers operating under:
    - An offshore banking license;
    - A banking license issued by a foreign country designated as non-cooperative; or
    - A banking license issued by a country that has been designated by the U.S. Secretary of the Treasury as warranting Special Measures.
- For-profit religious or spiritual organizations;
- Dealers in precious metals and stones;
- Charities, not-for-profit organizations ("NPOs"), and non-governmental organizations ("NGOs") that are either unregistered, or located or operating in high risk jurisdictions;
- Customers organized, domiciled, or doing business in high risk jurisdictions;
- Legal entity customers for whom ultimate beneficial ownership information or information regarding the legal entity's directors, managing partners, trustees, settlors, and beneficiaries, cannot be obtained or its accuracy reasonably confirmed;
- Customers subject to significant negative news, as identified through screening and due diligence activities.

The Higher-Risk Customer Types list is maintained by the AML Officer and is reviewed at least annually.

3.3.1.3.2. EDD Requirements

As defined in its procedures, EDD will include some or all of the following, conducted upon the customer being identified as Higher-Risk:

- Negative news and internet searches of the customer, and for legal entities also the controlling principal, beneficial owners, and ultimate parent;
- Collection of additional ID document;
- Collection of additional information about the customer;
- Collection of information on the customer's banking relationship with other institutions;

12

- Collection of information on the purpose of transactions;
- Meeting with Vinekross personnel;
- Assessment of expected transactional activity;
- Review of actual transactional activity against expected activity; and
- Collection of information for legal entity customers, including:
    - Legal formation number assigned by the formation entity and formation documents for corporate entities;
    - Legal entity's AML programme information, if applicable;
    - The legal entity's beneficial owners, controllers, and signatories of legal entity customers.

At a minimum, review and written approval by the AML Officer is required prior to account opening for the following higher-risk customer types, with all such approvals to be reported to the Board.

Vinekross will not allow customers awaiting completion of EDD to deposit funds or conduct transactions of any kind. Vinekross' policy is to not permit individuals or legal entities who fail required EDD to maintain accounts of any kind. In the event that: EDD measures cannot be applied; the customer cannot or will not provide the EDD information requested; and/or the customer has provided information that is false or contains significant inconsistencies that cannot be resolved after further investigation, then then the Company will suspend the due diligence and on-boarding process, notify the AML Officer, and the Company will not enter a relationship with the customer or open the account, or the Company will exit the existing relationship within thirty (30) calendar days. If appropriate, the AML Officer may escalate such customers for potential investigation of suspicious activity if Vinekross identifies reportable suspicious activity identified in the due diligence processes.

3.3.1.4. Prohibited Customer Types

The process of the customer identification programme and due diligence enables the business to determine whether a potential customer is a "prohibited customer" who is prohibited from using the Company's products and services ("Prohibited Customers"). Prohibited Customers are individual or legal entity customers that appear to be involved in activity that may be illegal or poses potential legal, regulatory, reputational, or sanctions risk or penalties that exceed the Company's risk appetite. Specifically, it is the Company's policy to prohibit the following types of individuals and legal entities from using the Company's products and services:

- Individuals and legal entities whose wealth or funding appears to be accumulated through corruption or activities that are illegal in the United States or in the country of origin;
- Bearer share accounts or entities that issue shares in bearer form;
- Payable-through-accounts and nested accounts;
- Non-traditional financial services companies (unless expressly approved by the AML Officer) including casas de cambio, exchange houses, check cashers, and currency dealers or exchangers);

- Individuals and legal entities who are designated under OFAC or who are in OFAC-sanctioned countries, without first obtaining the appropriate OFAC license;
- Individuals and legal entities whose wealth or funding appears to be accumulated through corruption or activities that are illegal in Sweden or in the country of origin;
- Individuals and legal entities whose identities are not known or cannot be verified as per the CIP and due diligence sections above;
- Individuals and legal entities included in Vinekross' internal watch list;
- Individuals and legal entities whose accounts were previously closed and the relationship terminated by the Company for AML, sanctions, or other anti-financial crime compliance reasons; and
- Individuals or legal entities who AML Officer or designee deems to pose unacceptable money laundering or sanctions risk.

The specific types listed above are representative, but not exhaustive. The Company reviews and updates this designation at least annually.
In the event that it is unclear whether a party is a Prohibited Customer, the decision must be escalated to a higher, qualified authority (e.g., the AML Officer) who shall take into consideration the elements of the Company's reputational risk policies and practices. If the Company finds that an individual or legal entity should be classified as a Prohibited Customer, the Company will suspend the due diligence and on-boarding process, notify the AML Officer, and the Company will not enter a relationship with the customer or open the account, or the Company will exit the existing relationship within thirty (30) calendar days. Prohibited Customers may also be escalated for potential investigation of suspicious activity, as appropriate.

3.3.1.5. Periodic Reviews

Throughout the course of a customer relationship, certain occurrences or changes in a customer's profile or activity may impact or raise concerns regarding the money laundering and sanctions risk of that customer. Vinekross will ensure on a risk-based approach that customer information is maintained, updated, and refreshed after account opening, and that transactional activity is incorporated into the Company's understanding of the customer's risk, on an on-going basis. All customers identified as higher risk and subject to EDD, including a customer who has a change in profile, or who requested activity or modified terms of service (such as increasing transaction limits), will be reviewed after account opening as appropriate and at least every twelve (12) months, and all other customers are reviewed at least every twenty-four (24) months. The scope of the review includes:

- Confirming that CIP was performed and all CDD and EDD information in a customer's file is current;
- Incorporating any new or additional information on the customer since the last review;
- Including information regarding the transactional activities of the customer; and
- Considering the results of transaction monitoring and case investigations, as relevant.

The Company will record the steps taken and the results of the review.

3.3.2. Transaction Monitoring and Suspicious Activity Reporting

Vinekross monitors customer activity to detect unusual or suspicious transactions.[13] Vinekross' policy is to take a conservative approach to monitoring by setting low dollar monitoring thresholds commensurate with the Company's high money laundering and sanctions risk in its activities. The Company will deny accounts that exceed set limits or display unusual activity. At a minimum, the Company will monitor all transactions, including fiat currency and digital asset transactions, at the customer and account levels, for:

- Fraudulent applications;
- Customers who appear to be structuring to avoid certain financial reporting.
- Groups/patterns of transactions indicative of smurfing (i.e., the use of multiple individuals and/or transactions to break large transactions into smaller transactions for the purpose of avoiding detection);
- Unusually large transactions:
- Customers who change linked bank accounts frequently;
- Multiple accounts or transactions assigned to one ITIN or TIN, address, or telephone number;
- Transactions with high-risk geographies;
- Customers for whom increased monitoring would be appropriate, including those considered to be higher risk and those on an internal Vinekross watch list; and
- Dormant accounts.

The AML Officer will ensure that his or her staff review alerts in a timely fashion. In addition, the Company requires all personnel to report any unusual customer or transactional activity they observe to the AML Officer. The AML Officer will ensure that all employees receive training on how to report unusual activity as part of the AML compliance training programme (see below).
The AML Officer will set transaction monitoring thresholds. The AML Officer reviews the sufficiency and calibration of the thresholds no less than annually will have authority to make changes including as needed in response to emerging patterns of activity. The AML Officer will document and retain the rationale for raising or eliminating a monitoring threshold and report that to Executive Management for approval. Executive Management must also ratify lowering a monitoring threshold or imposing a new threshold. However, in the event that new patterns of suspicious activity emerge prior to Executive Management approving such a change, the AML Officer is authorized to impose new thresholds pending Executive Management's approval. The AML Officer will ensure that the rationale for all changes in thresholds is documented and retained.

When a suspicious transaction is identified or reported to the AML officer, the AML officer reports such transactions to the Nigerian Financial Intelligence Unit (NFIU).
The AML Officer oversees the timely review and documentation of investigations and determines whether the Company needs to take actions, including but not limited to closure of the account, that meets any of the following criteria:

13 Vinekross also monitors against the limits set forth in *Section 4.2*.

- Involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity;
- Is designed to evade the requirements of AML laws and regulations to which Vinekross is subject, whether through structuring or other means;
- Serves no business or apparent lawful purpose, and the reporting business knows of no reasonable explanation for the transaction after examining all available facts; and/or
- Involves the use of the Company to facilitate criminal activity.

3.3.3. Suspension, Termination, and Cancellation of Customer Accounts

The AML Officer is permitted to suspend, restrict, or terminate a customer's access to any or all of Vinekross' services, or deactivate or cancel accounts that have been identified as posing unacceptable money laundering or sanctions risk to the Company. This includes accounts for which:

- Vinekross is so required by a facially valid subpoena, court order, or binding order of a government authority;
- Vinekross reasonably suspects the customer of using its Vinekross Account in connection with a prohibited business or practice that violates this Policy/programme;
- Use of an Vinekross Account is subject to any pending litigation, investigation, or government proceeding and/or the Company perceives a heightened risk of legal or regulatory non-compliance associated with account activity;
- The Company's service partners are unable to support the account use; or
- The customer takes any action that Vinekross deems as circumventing Vinekross' controls, including, but not limited to, opening multiple Vinekross Accounts or abusing promotions which Vinekross may offer from time to time.

If Vinekross suspends or closes an account, or terminates use of Vinekross services for any reason, it will provide the customer with notice of the Company's actions unless a court order or other legal process prohibits Vinekross from providing such notice.

3.3.4. Other Regulatory Reporting and Recordkeeping

3.3.4.1. Purchase and Sale of Monetary Instruments Recordkeeping

The Company has no plans to purchase or sell monetary instruments.

If in the future the Company develops plans to do so, the AML Officer will amend this Policy/programme and ensure that the Company develops recordkeeping procedures in accordance with the relevant regulations in advance of commencing the activity.

3.3.4.2. Funds Transfer Recordkeeping

The Company collects and maintains records of all funds transmittals valued at $3,000 or more in aggregate on the same day. The following information is included for each such transaction record:

- Name of the transmitter and, if the payment is ordered from an account, the account number;
- Address of the transmitter;

- Amount of the transmittal order;
- Date of the transmittal order;
- Identity of the recipient's financial institutions; and
- As many of the following items as possible:
    - Name and address of recipient;
    - Account number of the recipient; and
    - Any other specific identifier of the recipient; and
- Either the name and address or the numerical identifier of the transmitter's financial institution.

Vinekross maintains required records for a period of at least five years in a form that allows prompt retrieval in response to regulatory or law enforcement requests.

3.3.4.3. Reports of International Transportation of Currency or Monetary Instruments ("CMIRs")

The Company does not plan to undertake any activities that would involve transporting, mailing, or shipping monetary instruments out of or into the United States in any amount. Thus, the CMIRs requirements do not currently apply to Vinekross.

If in future the Company develops plans to allow other types of funds transfers, the AML Officer will amend this Policy/programme and ensure that the Company develops reporting procedures in accordance with the relevant regulations in advance of the activity commencing.

3.3.5. Information Sharing

The Company will cooperate fully with federal government authorities, law enforcement authorities, and financial institution partners on AML compliance investigations to the extent allowable under applicable privacy and other laws.

The AML Officer will establish systems and procedures to ensure that the Company:

- Establishes a central process for receiving, documenting, and responding to requests for information sharing and subpoenas and National Security Letters ("NSLs"), and ensuring that these procedures include notification of the AML Officer to allow for the review of customer activity;
- Promptly evaluates all information sharing requests received, including those from its bank partners, and provides timely responses with all information that Vinekross is legally allowed to share.

Other than these processes, the Company does not disclose information relating to its transaction monitoring activities to third parties except with the written consent of the AML Officer. The Company prohibits employees from disclosing information about its AML compliance activities or Policy/programme without receiving written permission from the AML Officer.

3.3.6. Oversight of Outsourced Service Providers

Vinekross may outsource specified systems and controls to service providers, which the Company defines to include affiliates as well as third parties. However, in all cases the Company retains

full responsibility for complying with AML laws and regulations, as well as ensuring the full implementation of the Policy/programme. The AML Officer, in conjunction with Executive Management and legal counsel, is responsible for approving contracts and agreements with affiliated and third-party service providers that impact the implementation of the Policy/programme to ensure that every contract clearly identifies the service provider's roles, responsibilities, performance standards, reporting obligations, and liabilities. These agreements include the service provider's obligations to provide documentation on customer information and investigations, and clearly detail the Company's requirements for internal controls, audit reviews, and the conditions for the termination of the affiliate or supplier relationship.
The AML Officer oversees all service providers that perform risk management and control processes whose activities significantly impact Vinekross' Policy/programme. This oversight includes:

- Conducting due diligence on capabilities ahead of approving the decision to outsource;
- Establishing SLAs setting standards the service provider must meet;
- Requiring the service provider to provide training to applicable employees that is broadly equivalent to the training that a Company employee would receive to fulfill the same role;
- Requiring reporting on performance against SLAs; and
- Performing periodic testing of service providers' performance as per SLA requirements.

3.3.7. Sanctions and Adverse Media Compliance

The AML Officer will establish and maintain controls to ensure that Vinekross complies with sanctions regulations to enforce economic and trade sanctions, including OFAC. These controls will apply to all parties with which the Company does business, including, but not limited to, customers, other transaction parties, and Vinekross personnel. The AML Officer will establish and oversee systems and procedures to ensure that the Company:

- Fully incorporates sanctions risk within its AML risk assessment;
- Screens each customer and other transaction party14 subject to CIP against OFAC sanctions programmes at account opening and prior to processing any transaction;
- Screens Vinekross personnel prior to doing business with them;
- Updates internal OFAC and other applicable lists in a timely fashion when OFAC announces changes to sanctions programmes;
- Prevents all customers under review for a potential OFAC hit from conducting transactions;
- Reviews all transactions identified through screening as potential OFAC violations;
- Documents rationale for clearing all false-positive OFAC hits;
- Blocks or rejects transactions as appropriate under Swedish sanctions law;
- Also Adverse Media Screening is carried out to identify potential criminal entities by analysing negative news from credible sources. The types of adverse media we look out for include: Financial Crime, Human and Drug Trafficking, Terrorists Associations, Property Crime, Digital Fraud.

We source for info for our sanctions and adverse media screenings from sources such as: print and online newspapers, sanctions lists chartered by governments, Sanction lists issued by the OFAC (Office of Foreign National Control), HMT financial watchlists, Lists compiled and consolidated by the United Nations (UN), Sanction lists chartered by the European Union, International Database (IDB) by the U.S. Census Bureau etc.

14Includes known beneficiaries of paymeTrafficking, Terrorists Associations, Property Crime, Digital Fraud. nts (including as permitted in digital asset transactions) and associated parties such as beneficial owners and controllers of accounts identified by CIP and CDD.

- Blocks internet protocol addresses of countries subject to broad OFAC sanctions, and any countries subject to narrower OFAC sanctions where the AML Officer thinks internet protocol blocking is necessary to mitigate the risk of a sanction violation;
- Reports blocked and rejected items to OFAC and prepares annual reports to OFAC on the total of blocked funds; and
- Establishes similar controls in relation to U.N. sanctions lists and other applicable sanctions programmes.

3.3.8. Mechanisms Designed to Monitor Ongoing Compliance

3.3.8.1. Staffing

The AML Officer will ensure that he or she has adequate staffing, both in numbers and qualifications, to implement the Policy/programme effectively, or request additional resources from Executive Management as needed. At least annually, the AML Officer will present his or her approach to staffing to Executive Management for approval and will ensure that all activities performed on behalf of the Company comply with Company policies and procedures and all applicable regulatory requirements regardless of the personnel performing the tasks.

3.3.8.2. Reporting

To ensure effective Executive Management and Board oversight of the Policy/programme, the AML Officer reports at least quarterly on the status of the programme to Executive Management and the Board. The reporting is compiled by the AML Officer, and may include:

- Overall AML compliance risk levels against the targeted risk level;
- Progress in implementation of the Policy/programme, such as:
    - KYC metrics;
    - Suspicious activity monitoring (transactions processed, cases generated);
    - Training sessions scheduled and completed; and
    - QA reviews and results.
- AML compliance trends;
- Material Policy/programme compliance issues and/or escalated issues;
- Emerging AML compliance issues, which the Company will need to address.
- Status of Policy/programme corrective actions; and
- Independent testing findings, bank partner concerns, and/or regulatory concerns.

No less than annually, the AML Officer will provide a report on the state of Policy/programme compliance and any significant emerging issues that will assist Executive Management and the Board in evaluating any Policy/programme changes that may be appropriate.

3.3.8.3. Quality Assurance and Testing[15]

A quality assurance testing helps to ensure that the Company maintains a high quality programme by implementing monitoring processes to promptly identify systematic errors and control deficiencies. Quality assurance testing may review the Company's:

- KYC programme;
- Transaction monitoring;
- Regulatory reporting, to the extend applicable in the previous year;
- Referrals to bank partners;
- Information sharing;
- Sanctions screening;
- Record-keeping; and
- Training.

The AML Officer is responsible for overseeing quality assurance testing, taking necessary corrective action to remediate findings, and reporting such information to Executive Management and the Board.

3.3.8.4. New Products or Business Practices

All new or modified products or services, distribution channels, geographies, and business initiatives or practices require, among other things, sign-off by the AML Officer. The AML Officer evaluates from a compliance perspective the risks to ensure that any such risks are appropriately identified and mitigated. The AML Officer updates the AML risk assessment when such practices are introduced and ensures the Company implements any needed additional controls before adopting the new or modified product or practice.

3.3.8.5. Training and Development

The Company requires that the Board and all Vinekross personnel whose jobs impact the Company's AML compliance receive AML compliance training appropriate to their roles and responsibilities at least on an annual basis. In addition, orientation for all new personnel contains an overview of the requirements of AML compliance and this Policy/ programme.

The goals of Vinekross' AML compliance training programme are to:

- Ensure that the Board and Executive Management are knowledgeable regarding Vinekross' obligations and responsibilities under AML law;
- Ensure Vinekross personnel are familiar with relevant AML compliance requirements pertaining to their specific job functions and that they receive the most current information available;
- Ensure that Executive Management and the Board are knowledgeable regarding Vinekross' obligations and responsibilities under AML law;

15As the programme scales to involve more Vinekross personnel, the AML Officer may put in place a quality assurance programme.

- Inculcate an understanding of the significance of Vinekross' AML efforts and help develop a strong culture of AML compliance across the Company; and
- Develop a cadre of personnel and managers throughout Vinekross to detect, escalate, and manage AML compliance-related risks as and when they arise.

Consistent with the Company's Compliance Policy, the AML Officer is responsible for ensuring that a risk-based AML compliance training programme is developed; that it is presented to Executive Management for approval; and that employees in need of advanced training receive such training and that records of training attendance are maintained.

3.3.8.6. Independent Testing

The Board oversees the completion, at least annually, of an independent review and test of Vinekross' AML compliance by a qualified third party, for the purpose of assessing the implementation and effectiveness of the Policy/programme and the adequacy of its controls over AML compliance risk. The AML Officer is responsible for updating Vinekross' AML compliance risk assessment in light of any issues raised during the independent testing and taking necessary corrective action to remediate findings.

4. Policy/programme Administration

4.1. Development, Review, and Approval

This Policy/programme is presented to the Board, or a designated Board committee, for review and approval at least annually or upon any request for significant modifications to this Policy/programme.

The AML Officer is responsible for the custody and issuance of this Policy/programme. Under the direction of the AML Officer, this Policy/programme and related procedures are required to be reviewed and reaffirmed, or appropriate updates to it will be recommended to the Board, at least annually or more frequently as appropriate. The review includes consideration of current and changes in applicable laws, regulations, or regulatory guidance; current and changes in the Company's products and services or operating geographic locations; feedback on the effectiveness of the Policy/programme; and any supervisory and/or audit input. The AML Officer, if necessary, may consult legal counsel.

The AML Officer may make minor modifications or supplement this Policy/programme without Board approval, so long as these changes are within the principles and limits of this Policy/programme and do not have the effect of reducing them. The AML Officer ensures that development and any revision of this Policy/programme includes circulating a draft to all relevant stakeholders (including Executive Management) for review and feedback, and reflecting the consideration of any applicable law and supervisory or relevant third-party input.

4.2. Compliance

4.2.1. Variances

No part of this Policy/programme or its supporting procedures should be interpreted as contravening or superseding other legal and regulatory requirements imposed upon Vinekross, including bank partner requirements.

Any conflicts between this Policy/programme and other legal obligations must be submitted immediately to the AML Officer for further evaluation. The AML Officer, if necessary, will consult outside legal counsel, and if appropriate will report the conflict and its resolution to Executive Management and the Board. All variances to this Policy/programme must be approved by the AML Officer and one member of Executive Management.

4.2.2. Exceptions

All exceptions to this Policy/programme require the approval of the AML Officer and the Board. The business must apply for an exception to this Policy/programme by contacting the AML Officer in writing and the AML Officer must inform Executive Management, report the exception request and recommendation to the Board, and take additional measures to effectively handle money laundering and/or sanctions risk. Additionally, the AML Officer will review the conditions that led to the exception, evaluate corrective actions, and identify an appropriate action plan to either return to compliance with this Policy/programme or seek modification to the Policy/programme. Action plans to cure exceptions to this Policy/programme will be presented to the Board for review and approval or review and rejection, as appropriate. Questions or suggestions about this Policy/programme should be directed to the AML Officer.

4.2.3. Breaches

The Policy/programme prohibits Company personnel from participating in any activity that facilitates money laundering or terrorist financing, or knowingly violates legally applicable sanctions. The Company does not tolerate: any conscious avoidance of facts; a failure to resolve indicators of potentially suspicious activity or possible violations of law, or other significant inconsistencies that arise in review of a customer's due diligence or transaction activity; or negligence on the part of its personnel. This Policy/programme prohibits advising or providing any other assistance to individuals for the purposes of circumventing financial crime laws or regulations or Company internal procedures.

Company personnel are required to promptly report any breach of or non-compliance with this Policy/programme to the AML Officer. The AML Officer ensures Vinekross personnel can report violations of this Policy/programme anonymously by phone and/or email. The AML Officer further ensures that this mechanism is well-publicized to all employees and takes all possible steps to ensure reports of potential violations remain anonymous and confidential. Vinekross never tolerates retaliation of any type against an employee who reports a potential violation of the Policy/programme. Any employee who commits such retaliation will be subject to subject to the Consequences of Non-Compliance section of this Policy/ programme. The AML Officer, or designee, must track the remediation and disposition of an identified Policy/programme breach. The AML Officer, if necessary, will consult outside legal counsel. Where appropriate, the AML Officer is responsible for informing the relevant authorities.

Any Company personnel who violates this Policy/programme are subject to the Consequences of Non-Compliance requirements of this Policy/programme.

4.2.4. Consequences of Non-Compliance

Vinekross recognizes that if it the Company fails to comply with this Policy/programme and applicable AML laws and related regulations, it could result in significant adverse legal, reputation, and financial impact on the Company.

All Company personnel are responsible for assisting in Vinekross' compliance with applicable AML laws and related regulations. All Company personnel are responsible for understanding this Policy/programme and undertaking any specified responsibility assigned to them. Compliance with the requirements of this Policy/programme and applicable AML laws and related regulations must be included as applicable in the job descriptions and performance evaluations of Company personnel. The AML Officer, at his or her discretion, may provide input into any employee's performance evaluation. Personnel who fail to comply with this Policy/programme will be held accountable for their performance and may be subject to disciplinary action up to, and including, termination of employment in appropriate cases.

Individuals who fail to comply with the applicable AML laws and related regulations can also be subject to personal liability such as civil and/or criminal penalties and imprisonment, and as such may be referred to law enforcement or regulatory authorities in accordance with the requirements of the requisite government authority.

4.3. Communication Plan and Contact

Upon the Policy/programme's approval, the AML Officer is responsible for communicating this Policy/programme through the following channels:

- Sending an email to stakeholders detailing material updates; and
- Publishing the Policy/programme and related documentation to the location as agreed by the stakeholders.

The AML Officer is available for consultation on the interpretation and administration of this Policy/programme.

5. Appendices

5.1. Appendix A: Definitions

For purposes of this Policy/programme, these terms are defined as follows:

Agent	An independent entity that seeks to add specific MSB services to its existing products and services. For example, a corner store that offers remittance services through Western Union. FinCEN requires that MSBs provide their list of agents to FinCEN.
AML	Anti-money laundering
Beneficial Owner	A legal entity or individual that directly or indirectly owns or controls 25% or more of a customer
Board	Vinekross Board of Directors
AML Officer	Vinekross officer reporting to the CEO and Board, and who is designated to execute the Policy/programme
AML Compliance Risk	The risk of legal or regulatory sanctions, material financial loss, or loss to reputation that the Company may suffer as a result of failure to comply with AML- and sanctions-related laws, rules, and regulatory guidance

CCO	Vinekross Chief Compliance Officer
CDD	Customer Due Diligence
CEO	Vinekross Chief Executive Officer
CIP	Customer Identification programme
CMIR	Reports of International Transportation of Currency or Monetary Instruments
Currency	Currency is defined as coin and paper money of the United States or any other country that is designated as legal tender, circulates, and is customarily accepted as a medium of in the country of issuance
Customer	Anyone that opens an account, including corporations and other legal entities
EDD	Enhanced due diligence
Executive Management	The senior management-level executives, including the CEO, that oversee risk management at the Company
Integration	The incorporation of unlawful proceeds into the financial system to convert illicit funds into apparently legitimate business earnings
Vinekross or the Company	Vinekross Technologies Limited
Layering	The moving of funds around the financial system to create confusion and complicate the paper trail
Monetary Instruments	Includes: Currency; traveler's checks in any form; all negotiable instruments (including personal checks, business checks, official bank checks, cashier's checks, third-party checks, promissory notes (as that term is defined in the Uniform Commercial Code), and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including personal checks, business checks, official bank checks, cashier's checks, third-party checks, promissory notes, and money orders) signed but with the payee's name omitted; and securities or stock in bearer form or otherwise in such form that title thereto passes upon delivery. Monetary instruments do not include warehouse receipts or bills of lading
Money Laundering	The process by which persons attempt to conceal and disguise the true origin and ownership of illegal funds. Money laundering is generally viewed as a three-stage process: placement, layering, and integration
NGO	Non-governmental organization
NPO	Not-for-profit organization
NSL	National Security Letter
OFAC	Office of Foreign Assets Control
PEP	Politically Exposed Person
Personnel	Vinekross' employees, officers, temporary staff, contractors, and service providers, including any parent company staff involved

	in the operations of Vinekross
Placement	The introduction of unlawful proceeds into the financial system without attracting the attention of financial institutions or law enforcement
Policy/programme	Vinekross' AML Compliance Policy and programme
Sanctions	Sanctions laws are instruments used by government bodies and international organizations to advance objectives relating to national security, foreign policy, human rights, or prevention of drug trafficking or other illegal activity
SDN List	Specially Designated Nationals and Blocked Persons List
SLA	Service level agreement
Ultimate Beneficial Owner (or UBO)	An individual or legal entity that directly or indirectly owns or controls 25% or more of a customer and does not itself have any individual or legal entity with a controlling interest of 25% or more
Ultimate Parent	A legal entity, not an individual, who directly or indirectly owns or controls more than 50% of a customer and does not itself have a legal entity with a controlling interest of more than 50%
VSD	Voluntary Self-Disclosure