+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

Version: 1.0
Effective Date: 17 September 2025

ANTI-MONEY LAUNDERING (AML), COUNTER-TERRORIST FINANCING (CFT) & KYC POLICY MANUAL

INTRODUCTION

Veyron Markets adopts a strict zero-tolerance approach toward money laundering, terrorist financing, fraud, corruption, and any form of financial crime. The Company recognizes that financial institutions, including trading and brokerage platforms, are inherently exposed to risks of misuse by criminal elements seeking to disguise the origin of illicit funds or to channel funds for unlawful purposes.

This Anti-Money Laundering (AML), Counter-Terrorist Financing (CFT), and Know Your Customer (KYC) Policy Manual (the "Policy") establishes a comprehensive, risk-based compliance framework designed to effectively prevent, detect, and report suspicious activities. The framework aligns with internationally recognized standards, including the recommendations of the Financial Action Task Force (FATF), and is structured to meet regulatory expectations across multiple jurisdictions.

The purpose of this Policy is to ensure that the Company:

- Maintains robust systems and controls to mitigate the risks of money laundering and terrorist financing
- Implements effective customer identification and verification procedures (KYC/CDD)
- Continuously monitors customer transactions and behavior for unusual or suspicious activity
- Identifies and assesses risks associated with customers, products, services, and geographic exposure
- Ensures timely reporting of suspicious activities to relevant regulatory authorities
- Maintains accurate and secure records for regulatory and audit purposes

Veyron Markets applies a risk-based approach (RBA), which allows the Company to allocate resources efficiently and apply enhanced scrutiny to higher-risk areas while maintaining proportionate controls for lower-risk relationships. This approach ensures that AML/CFT measures are dynamic, scalable, and responsive to evolving risks.

The Company is committed to fostering a strong culture of compliance across all levels of the organization.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

Senior management and the Board of Directors actively support AML/CFT initiatives and ensure that adequate resources, systems, and training are provided to implement this Policy effectively. All employees, regardless of role, share responsibility for compliance and are required to understand and adhere to the procedures outlined in this manual.

This Policy applies to all business activities, customers (both individuals and legal entities), employees, and third-party relationships associated with the Company. It covers the entire customer lifecycle—from onboarding and verification to ongoing monitoring, reporting, and record retention.

Failure to comply with this Policy may expose the Company to significant regulatory, financial, and reputational risks. Accordingly, strict adherence is mandatory, and any breaches may result in disciplinary action, including termination of employment or contractual relationships, and potential legal consequences.

This document is subject to periodic review and updates to ensure ongoing alignment with regulatory developments, emerging risks, and industry best practices.

POLICY STATEMENT

Veyron Markets is firmly committed to maintaining the highest standards of integrity, transparency, and regulatory compliance in all its operations. The Company adopts a zero-tolerance approach toward money laundering, terrorist financing, fraud, corruption, and any other form of financial crime.

This Policy establishes the Company's commitment to implementing effective Anti-Money Laundering (AML), Counter-Terrorist Financing (CFT), and Know Your Customer (KYC) controls designed to prevent the misuse of its services and systems. The Company recognizes its responsibility as a financial service provider to safeguard the financial system from abuse and to support global efforts in combating illicit financial activities.

To achieve this, Veyron Markets has implemented a comprehensive, risk-based AML/CFT framework that includes:

- Robust customer identification and verification procedures prior to establishing any business relationship
- Ongoing monitoring of customer transactions and behavior to detect unusual or suspicious activity
- Risk assessment mechanisms to identify, evaluate, and mitigate potential exposure to financial crime

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

- Timely reporting of suspicious transactions to relevant regulatory and law enforcement authorities
- Maintenance of accurate, complete, and secure records in accordance with legal requirements

The Company ensures that AML/CFT compliance is embedded into its corporate governance structure. Senior management and the Board of Directors are actively responsible for overseeing the effectiveness of AML controls and ensuring that adequate resources, systems, and personnel are in place.

All employees of the Company are required to:

- Adhere strictly to this Policy and all related procedures
- Exercise due diligence in performing their roles
- Remain vigilant to potential indicators of suspicious activity
- Report any concerns promptly to the AML Compliance Officer

The Company strictly prohibits the establishment or continuation of business relationships with:

- Individuals or entities involved in criminal activities
- Sanctioned persons or organizations
- Customers who fail to provide adequate identification or verification documentation
- Anonymous or fictitious accounts

Failure to comply with this Policy may expose the Company to significant legal, regulatory, and reputational risks. Accordingly, any breach of this Policy will be treated seriously and may result in disciplinary action, including termination of employment, as well as potential legal consequences.

This Policy is subject to periodic review and updates to ensure its continued effectiveness and alignment with evolving regulatory requirements, industry best practices, and emerging risks. Through this Policy, Veyron Markets reaffirms its commitment to operating with integrity and contributing to the global fight against financial crime.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

OBJECTIVES

The primary objective of this Anti-Money Laundering (AML), Counter-Terrorist Financing (CFT), and Know Your Customer (KYC) Policy is to establish a robust and comprehensive framework that enables Veyron Markets to effectively prevent, detect, and respond to risks associated with financial crime. The Company recognizes that a strong AML/CFT framework is essential not only for regulatory compliance but also for maintaining trust, safeguarding its operations, and contributing to the integrity of the global financial system.

This Policy is designed to achieve the following key objectives:

1. Prevention of Financial Crime

The foremost objective of this Policy is to prevent the Company from being used as a vehicle for money laundering, terrorist financing, fraud, or any other illicit financial activities. The Company aims to achieve this by implementing stringent controls that deter criminals from attempting to misuse its platform.

This includes:

- Ensuring that all customers are properly identified and verified before establishing a business relationship
- Detecting attempts to use false, misleading, or stolen identities
- Preventing anonymous or fictitious accounts
- Blocking or restricting access to individuals or entities involved in illegal activities

By adopting a proactive approach, the Company seeks to minimize the risk of exposure to financial crime at the earliest stage.

2. Compliance with Regulatory and Legal Requirements

The Company is committed to full compliance with all applicable AML/CFT laws, regulations, and international standards, including those set by global regulatory bodies and local authorities in the jurisdictions where it operates.

This objective includes:

- Adhering to regulatory requirements related to customer identification, verification, and monitoring
- Ensuring timely submission of Suspicious Activity Reports (SAR/STR) to relevant authorities
- Maintaining accurate and complete records in accordance with legal retention requirements
- Cooperating fully with regulatory bodies, law enforcement agencies, and financial intelligence units

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

- Compliance is treated as a fundamental obligation and is integrated into all business processes and decision-making frameworks.

3. Implementation of a Risk-Based Approach

The Company aims to implement and maintain a dynamic Risk-Based Approach (RBA) that allows it to identify, assess, and mitigate risks efficiently. This ensures that resources are allocated proportionately, focusing more on high-risk areas while maintaining appropriate controls across all customer segments.

Key aspects include:

- Assessing risks associated with customers, geographic locations, products, and transactions
- Assigning risk ratings to customers based on predefined criteria
- Applying enhanced due diligence measures to high-risk customers
- Continuously updating risk assessments based on customer behavior and external developments

This approach ensures that the Company remains responsive to evolving threats and emerging financial crime typologies.

4. Establishment of Robust Internal Controls

Another key objective is to develop and maintain strong internal controls and procedures that support effective AML/CFT compliance.

This includes:

- Clearly defined roles and responsibilities for AML compliance across the organization
- Segregation of duties to prevent conflicts of interest and unauthorized activities
- Implementation of approval processes and escalation mechanisms
- Maintenance of audit trails and documentation for all compliance activities
- Regular internal audits and compliance reviews to assess effectiveness

These controls ensure consistency, accountability, and transparency in all AML-related processes.

5. Detection and Reporting of Suspicious Activities

The Company aims to establish efficient systems and procedures to detect, investigate, and report suspicious transactions and activities in a timely manner.

This involves:

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

- Continuous monitoring of customer transactions and behavior
- Identification of unusual patterns, inconsistencies, or red flags
- Prompt escalation of suspicious activities to the AML Compliance Officer
- Thorough investigation of alerts and flagged transactions
- Filing of Suspicious Activity Reports (SAR/STR) with relevant authorities when necessary
- The Company recognizes that timely detection and reporting are critical in combating financial crime and supporting law enforcement efforts.

6. Protection of the Company's Reputation and Integrity

Maintaining a strong reputation is a core objective of the Company. Exposure to money laundering or financial crime can result in severe reputational damage, financial losses, and regulatory penalties.

To mitigate these risks, the Company:

- Ensures strict adherence to AML/CFT policies and procedures
- Conducts due diligence on customers and business relationships
- Avoids engaging with high-risk or non-compliant entities
- Promotes ethical conduct and transparency in all operations

Protecting the Company's reputation is essential for long-term sustainability and stakeholder trust.

7. Promotion of a Strong Compliance Culture

The Company aims to foster a culture of compliance where all employees understand their responsibilities and actively contribute to AML/CFT efforts.

This includes:

- Providing regular training and awareness programs for employees
- Encouraging vigilance and proactive identification of suspicious activities
- Ensuring that employees feel responsible and accountable for compliance
- Promoting ethical behavior and zero tolerance for misconduct

A strong compliance culture ensures that AML/CFT principles are embedded across all levels of the organization.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

8. Ensuring Data Integrity and Record Maintenance

- The Company aims to maintain accurate, complete, and secure records of all customer and transaction data. Proper record-keeping supports transparency, auditability, and regulatory compliance.
- This objective includes:
- Maintaining customer identification and verification records
- Recording transaction histories and monitoring activities
- Retaining records for the required regulatory period
- Ensuring data confidentiality and protection against unauthorized access
- Effective record management enables the Company to respond to regulatory inquiries and investigations efficiently.

9. Continuous Improvement and Adaptation

The Company recognizes that financial crime risks are constantly evolving. Therefore, an important objective of this Policy is to ensure continuous improvement of AML/CFT controls. This includes:

- Regular review and updating of policies and procedures
- Incorporation of new regulatory requirements and industry best practices
- Enhancement of monitoring systems and technologies
- Learning from internal audits, regulatory feedback, and industry developments

This proactive approach ensures that the Company remains resilient against emerging risks.

10. Cooperation with Regulatory and Law Enforcement Authorities

The Company is committed to supporting global efforts in combating financial crime through active cooperation with regulators and law enforcement agencies.
This includes:

- Providing requested information in a timely and accurate manner
- Assisting in investigations where required
- Ensuring transparency in reporting and disclosures
- Maintaining open communication with regulatory bodies

Such cooperation reinforces the Company’s commitment to maintaining a secure and compliant financial environment.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

SCOPE

The scope of this Anti-Money Laundering (AML), Counter-Terrorist Financing (CFT), and Know Your Customer (KYC) Policy extends to all business activities, operations, and relationships undertaken by Veyron Markets, without exception. This Policy applies comprehensively across all jurisdictions in which the Company operates or seeks to operate, subject to applicable local laws and regulatory requirements.

This Policy is binding on all employees of the Company, including full-time staff, part-time staff, temporary employees, contractors, consultants, interns, and any other individuals engaged in activities on behalf of the Company. It applies equally to senior management, directors, and members of the Board, all of whom are required to demonstrate leadership in promoting and maintaining a strong compliance culture.

The scope of this Policy further extends to all customers of the Company, including individuals, corporate entities, partnerships, trusts, and any other legal arrangements. All customers are subject to appropriate due diligence measures, risk assessment procedures, and ongoing monitoring as defined within this Policy, regardless of their geographic location, transaction size, or account type.

In addition, this Policy applies to all products and services offered by the Company, including but not limited to trading accounts, brokerage services, financial instruments, and any related digital or financial platforms. All existing and future products must be assessed for AML/CFT risks prior to launch and continuously monitored throughout their lifecycle.

This Policy also covers all third-party relationships, including business partners, introducing brokers, payment service providers, technology vendors, liquidity providers, and any outsourced service providers. Where third parties act on behalf of or in connection with the Company, they are required to adhere to equivalent AML/CFT standards, and appropriate due diligence must be conducted prior to engagement and on an ongoing basis.

Furthermore, the scope includes all customer onboarding processes, transaction processing activities, fund transfers, deposits, withdrawals, internal transfers, and any other financial or operational activity that may expose the Company to AML/CFT risks. No activity, irrespective of value or frequency, is exempt from monitoring and compliance oversight.

This Policy applies throughout the entire lifecycle of the business relationship with the customer, from initial onboarding and verification through to account maintenance, ongoing monitoring, and eventual termination of the relationship. Even after termination, the Company continues to maintain records and fulfill regulatory obligations as required by applicable laws.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

Overall, this Policy establishes a unified compliance framework that governs all aspects of the Company's operations, ensuring that AML/CFT obligations are consistently applied, effectively enforced, and continuously monitored across all functions, departments, and jurisdictions.

Risk-Based Approach (RBA)

The Risk-Based Approach (RBA) is the foundation of the Company's AML/CFT framework and is designed to ensure that Veyron Markets allocates its resources, controls, and monitoring efforts in a manner that is proportionate to the level of risk identified in its customers, products, services, delivery channels, and geographic exposure.

Under this approach, the Company does not apply a uniform level of due diligence to all customers. Instead, it assesses and categorizes risk based on predefined criteria and applies enhanced controls where higher risks are identified. This ensures that the Company can effectively prevent and detect money laundering, terrorist financing, and other financial crimes while maintaining operational efficiency.

The Risk-Based Approach enables the Company to identify, evaluate, and understand the risks to which it is exposed and to implement appropriate mitigation measures. It is a dynamic and continuous process that evolves in response to changes in customer behavior, transaction patterns, regulatory expectations, and global financial crime trends.

The Company recognizes that financial crime risks are not static and may vary significantly depending on several internal and external factors. As such, the RBA framework is integrated into all stages of the business relationship, including customer onboarding, verification, transaction monitoring, periodic reviews, and account closure.

Risk assessment is conducted using a combination of automated systems and manual oversight. Customers are evaluated based on multiple risk indicators, including but not limited to their country of residence or incorporation, nature of business activities, source of funds, transaction behavior, and whether they are classified as Politically Exposed Persons (PEPs) or are associated with high-risk jurisdictions.

Based on this assessment, customers are assigned a risk classification, typically categorized as low, medium, or high risk. Each category determines the level of Customer Due Diligence (CDD) to be applied. Low-risk customers are subject to standard verification procedures, while medium-risk customers are subject to enhanced scrutiny in specific areas. High-risk customers are subject to Enhanced Due Diligence (EDD), which includes deeper verification of identity, source of wealth, and ongoing transaction monitoring.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

The Risk-Based Approach also extends to the Company's products and services. Certain offerings, such as high-leverage trading instruments or cross-border transactions, may inherently carry higher risk and therefore require additional controls and monitoring measures. Similarly, geographic risk is carefully assessed, with higher scrutiny applied to customers or transactions linked to jurisdictions identified as having weak AML/CFT controls or subject to international sanctions.

The Company also ensures that its Risk-Based Approach is supported by continuous monitoring and periodic review mechanisms. Customer risk profiles are not static and are reassessed regularly based on changes in behavior, transaction activity, or updated external risk intelligence. Any significant change in customer profile triggers a reassessment of risk classification and may result in the application of additional controls.

Furthermore, the Risk-Based Approach is supported by governance and oversight mechanisms to ensure its effectiveness. Senior management is responsible for approving the risk framework, while the AML Compliance Officer ensures its implementation and ongoing effectiveness. Internal audits and compliance reviews are conducted periodically to evaluate the adequacy of the RBA framework and to identify areas for improvement.

Ultimately, the Risk-Based Approach ensures that Veyron Markets remains agile, compliant, and capable of addressing emerging financial crime risks in a structured and proportionate manner, while maintaining alignment with international AML/CFT standards and best practices.

Risk Classification

The Company applies a structured Risk Classification framework to ensure that all customers are assessed, categorized, and monitored in accordance with their potential exposure to money laundering, terrorist financing, fraud, and other financial crime risks. This classification system is a core component of the Risk-Based Approach (RBA) and determines the level of Customer Due Diligence (CDD), monitoring intensity, and approval requirements applicable to each customer.

Risk classification is determined at the time of onboarding and is continuously reviewed throughout the customer relationship. It is based on a combination of quantitative and qualitative factors, including customer profile, geographic exposure, source of funds, transaction behavior, and overall relationship activity. The classification process ensures that higher-risk customers are subject to enhanced controls, while lower-risk customers are managed with standard procedures.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

The Company generally classifies customers into three primary categories: low risk, medium risk, and high risk. Each category reflects the degree of AML/CFT risk exposure and determines the level of scrutiny required.

Low-risk customers are typically individuals or entities that demonstrate transparent financial profiles, stable and consistent transaction behavior, and originate from jurisdictions with strong AML/CFT regulatory frameworks. These customers are subject to standard Customer Due Diligence procedures, including basic identity verification and ongoing periodic monitoring.

Medium-risk customers are those who present moderate levels of risk due to certain risk indicators such as increased transaction volumes, cross-border activity, complex employment structures, or limited transparency in source of funds. These customers are subject to standard CDD along with selective Enhanced Due Diligence (EDD) measures where necessary. Their transactions are monitored more frequently to identify potential anomalies or deviations from expected behavior.

High-risk customers are those who present significant exposure to AML/CFT risks. This includes Politically Exposed Persons (PEPs), customers from high-risk or sanctioned jurisdictions, entities with complex or opaque ownership structures, or customers engaged in high-volume or unusual transaction patterns. High-risk classification triggers mandatory Enhanced Due Diligence, senior management approval, and continuous enhanced monitoring of all account activity.

The risk classification framework is not static and is subject to ongoing reassessment. Any significant change in customer behavior, transaction patterns, geographic exposure, or external risk intelligence may result in reclassification. For example, a low-risk customer exhibiting unusual transaction behavior may be escalated to medium or high risk following review by the Compliance Department.

The Company also ensures that risk classification decisions are documented, justified, and retained for audit and regulatory purposes. All classifications are supported by a clear rationale and are subject to periodic internal review and independent audit to ensure consistency and effectiveness.

Ultimately, the Risk Classification framework enables the Company to apply proportionate and effective AML/CFT controls, ensuring that higher-risk customers receive enhanced scrutiny while maintaining operational efficiency for lower-risk relationships. This structured approach supports the Company’s commitment to regulatory compliance, risk mitigation, and the prevention of financial crime.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

Risk Scoring Model

The Company implements a structured Risk Scoring Model to objectively assess and quantify the money laundering and terrorist financing risk associated with each customer. This model forms an integral part of the overall Risk-Based Approach (RBA) and ensures that risk classification decisions are consistent, transparent, and evidence-based.

The Risk Scoring Model assigns numerical values to specific risk factors identified during the onboarding process and throughout the ongoing customer relationship. These risk factors are evaluated individually and collectively to produce an overall risk score, which determines the customer's risk category and the level of due diligence required.

The key risk indicators used within the scoring model include, but are not limited to, the customer's country of residence or incorporation, the nature of their occupation or business activity, the source of funds and source of wealth, transaction behavior, account usage patterns, and whether the customer is classified as a Politically Exposed Person (PEP). Additional considerations include exposure to high-risk jurisdictions, involvement in complex corporate structures, and the use of third-party payments or accounts.

Each risk factor is assigned a predefined score based on its inherent risk level. For example, jurisdictions with strong AML/CFT frameworks are assigned lower scores, while high-risk or sanctioned jurisdictions are assigned higher scores. Similarly, customers with transparent and verifiable income sources are assigned lower risk values compared to those with unclear or undocumented sources of wealth.

The cumulative score generated from all risk factors determines the overall risk rating of the customer. This rating is typically categorized into low, medium, or high risk bands. Customers with low aggregate scores are considered low risk and are subject to standard Customer Due Diligence procedures. Customers with moderate scores are classified as medium risk and may be subject to selective Enhanced Due Diligence measures. Customers with high aggregate scores are classified as high risk and are subject to mandatory Enhanced Due Diligence, increased monitoring, and senior management approval.

The Risk Scoring Model is designed to be dynamic and responsive. It is continuously updated based on changes in customer behavior, transaction activity, or new risk intelligence obtained through internal monitoring systems or external sources. Any significant change in a customer's risk profile automatically triggers a reassessment and recalculation of the risk score.

The Company ensures that the Risk Scoring Model is consistently applied across all customers to maintain fairness, objectivity, and regulatory compliance.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

All scoring outcomes are documented and stored securely for audit and regulatory inspection purposes. The methodology used for scoring is subject to periodic review to ensure its effectiveness and alignment with evolving regulatory expectations and industry best practices.
In addition, the Risk Scoring Model is supported by automated systems and manual oversight. While automated tools assist in the initial calculation and monitoring of risk scores, final assessment decisions are reviewed and validated by the Compliance Department to ensure accuracy and appropriateness.
Ultimately, the Risk Scoring Model enables the Company to proactively identify high-risk customers, allocate compliance resources efficiently, and implement appropriate risk mitigation measures in a structured and defensible manner, thereby strengthening the overall effectiveness of the AML/CFT framework.

CUSTOMER ONBOARDING PROCEDURES

The Customer Onboarding Procedures of Veyron Markets are designed to ensure that no business relationship is established without the completion of comprehensive identity verification, risk assessment, and compliance screening. These procedures form the first and most critical control point in the Company's Anti-Money Laundering (AML), Counter-Terrorist Financing (CFT), and Know Your Customer (KYC) framework, and are intended to prevent the onboarding of high-risk, fraudulent, or sanctioned individuals and entities.
The onboarding process begins at the point of customer registration, where the prospective customer is required to submit accurate personal or corporate information through the Company's official onboarding platform. The Company ensures that all information collected is sufficient to establish the identity of the customer, understand the nature of the intended relationship, and assess the associated risk exposure.
Upon submission of registration details, the customer is required to complete the KYC documentation process. This includes providing valid identification documents, proof of address, and any additional information required based on the customer type. For corporate clients, incorporation documents, ownership structure details, and Ultimate Beneficial Owner (UBO) information are mandatory. The Company ensures that all submitted documentation is clear, valid, and up to date before proceeding to the next stage of onboarding.
Once documents are received, the Company conducts a thorough verification process. This includes authentication of identity documents, validation of address proof, and cross-checking of corporate records where applicable.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

The Company may use both automated verification tools and manual review processes to ensure the authenticity and reliability of the information provided.

Simultaneously, the customer is subjected to sanctions screening, Politically Exposed Person (PEP) checks, and adverse media screening using recognized databases and compliance tools. Any potential match is escalated for further review by the Compliance Department to determine whether the relationship can proceed or requires additional due diligence measures.

Following verification and screening, the Company performs a detailed risk assessment of the customer. This includes assigning a risk score based on predefined criteria such as geographic location, source of funds, occupation, transaction expectations, and overall risk indicators. Based on this assessment, the customer is categorized into low, medium, or high risk, which determines the level of due diligence and ongoing monitoring required.

For low-risk customers, onboarding may proceed upon successful completion of standard verification procedures. Medium-risk customers may require additional clarification or selective Enhanced Due Diligence (EDD) before approval. High-risk customers are subject to mandatory EDD, including senior management approval and enhanced scrutiny of supporting documentation, before any account activation is permitted.

The Company maintains a strict policy that no trading account or business relationship is activated until all onboarding requirements have been fully satisfied and the customer has been formally approved by the Compliance function. This ensures that only verified and appropriately assessed customers are granted access to the Company's services.

Throughout the onboarding process, the Company ensures proper documentation of all steps, decisions, and approvals. All records are securely stored in accordance with regulatory retention requirements and are made available for internal audit or regulatory inspection when required.

The onboarding procedures are subject to continuous improvement and periodic review to ensure alignment with evolving regulatory expectations, technological advancements, and emerging financial crime risks. Any changes to onboarding requirements are implemented promptly and communicated to relevant stakeholders to ensure consistent application across the organization.

Ultimately, the Customer Onboarding Procedures serve as a critical control mechanism that enables Veyron Markets to establish legitimate business relationships, prevent exposure to illicit activities, and maintain the integrity of its financial ecosystem.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

CUSTOMER DUE DILIGENCE

Customer Due Diligence (CDD) is a fundamental pillar of the Company's Anti-Money Laundering (AML), Counter-Terrorist Financing (CFT), and Know Your Customer (KYC) framework. It refers to the set of procedures and controls implemented by Veyron Markets to identify, verify, and understand its customers and the nature of their financial activities before and throughout the business relationship.

The primary objective of Customer Due Diligence is to ensure that the Company has a reasonable level of certainty regarding the identity of its customers, the legitimacy of their funds, and the purpose of their engagement with the Company. CDD also enables the Company to assess the risk posed by each customer and apply appropriate monitoring and control measures in line with the Risk-Based Approach (RBA).

The Company performs Customer Due Diligence at the onboarding stage and continues it on an ongoing basis throughout the lifecycle of the business relationship. CDD is not a one-time exercise but a continuous process that is updated whenever there is a change in customer behavior, risk profile, or supporting information.

At a minimum, CDD requires the Company to verify the identity of the customer using reliable and independent documentation, data, or information. For individual customers, this includes verification of full name, date of birth, nationality, residential address, occupation, and source of funds. For corporate or legal entity customers, CDD includes verification of company registration details, ownership structure, directors, shareholders, and Ultimate Beneficial Owners (UBOs).

An essential component of CDD is the identification and verification of the Ultimate Beneficial Owner (UBO). The Company is required to take reasonable measures to identify the natural person(s) who ultimately own or control the customer entity, particularly where ownership exceeds the defined threshold or where control is exercised through other means. This ensures transparency in ownership structures and reduces the risk of concealment of illicit funds through complex corporate arrangements.

The Company also assesses and understands the purpose and intended nature of the business relationship. This involves evaluating the expected account activity, nature of transactions, and anticipated volume of trading or fund flows. This information is used to establish a baseline against which actual customer behavior is monitored over time.

Customer Due Diligence further includes the verification of the source of funds and, where necessary, the source of wealth. The Company takes reasonable steps to ensure that funds used in transactions are derived from legitimate sources and are consistent with the customer's known financial profile and declared economic activity.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

In cases where standard CDD is not sufficient to adequately assess risk, the Company applies Enhanced Due Diligence (EDD) measures. This may include obtaining additional documentation, conducting deeper verification of financial background, increasing the frequency of monitoring, and requiring senior management approval before establishing or continuing the business relationship.

Conversely, in limited and low-risk scenarios where permitted by applicable regulations, the Company may apply Simplified Due Diligence (SDD), provided that sufficient justification exists and the risk of money laundering or terrorist financing is demonstrably low.

The Company ensures that all CDD information is properly documented, verified, and securely stored in accordance with applicable data protection and record-keeping requirements. Any discrepancies, inconsistencies, or concerns identified during the CDD process are escalated to the AML Compliance Officer for further review and action.

Ongoing Customer Due Diligence is an integral part of the Company's monitoring framework. Customer profiles are periodically reviewed and updated based on changes in risk classification, transaction behavior, regulatory requirements, or new information obtained through monitoring systems or external sources.

Ultimately, Customer Due Diligence enables Veyron Markets to maintain a clear understanding of its customers, mitigate exposure to financial crime risks, and ensure compliance with applicable AML/CFT regulations and international best practices.

KYC REQUIREMENTS

Know Your Customer (KYC) Requirements form a critical component of the Company's Anti-Money Laundering (AML), Counter-Terrorist Financing (CFT), and Customer Due Diligence (CDD) framework. These requirements are designed to ensure that Veyron Markets establishes and maintains verified, accurate, and up-to-date information about all customers prior to and throughout the course of the business relationship.

The primary purpose of KYC requirements is to confirm the identity of customers, assess their risk profile, and ensure that the Company is not knowingly or unknowingly facilitating illicit financial activity. The KYC process ensures transparency, accountability, and regulatory compliance across all customer interactions.

All customers are required to provide complete, accurate, and verifiable information during the onboarding process. The Company does not permit the opening or activation of any account unless all mandatory KYC requirements have been satisfactorily fulfilled and verified.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

For individual customers, KYC requirements include the collection of essential personal and financial information. This includes full legal name, date of birth, nationality, residential address, contact details, occupation, employment details, and source of funds. In addition, customers are required to disclose information regarding the nature of their financial activity and expected transaction behavior to enable proper risk assessment.

For corporate or institutional customers, the KYC requirements extend to the collection of detailed company information, including registered company name, registration number, incorporation date, country of incorporation, registered office address, business activities, and corporate structure. The Company also requires disclosure of all directors, shareholders, and Ultimate Beneficial Owners (UBOs), along with appropriate supporting documentation to verify ownership and control.

The KYC process also requires submission of valid identification documents issued by recognized authorities. For individuals, acceptable documents include a valid passport, national identity card, or driving license. These documents must be current, legible, and contain a clear photograph of the individual. Proof of residential address is also required and may include recent utility bills, bank statements, or government-issued correspondence, typically not older than three months.

For corporate customers, required documentation includes the Certificate of Incorporation, Memorandum and Articles of Association, Certificate of Good Standing (where applicable), board resolutions authorizing account opening, and documentation evidencing the ownership structure and control chain. Additional supporting documents may be requested depending on the complexity and risk profile of the entity.

The Company ensures that all KYC documents are subject to verification procedures, which may include automated validation tools, manual review, and cross-referencing against reliable third-party databases. Any inconsistencies, discrepancies, or signs of document tampering are escalated to the Compliance Department for further investigation.

KYC requirements are not limited to the onboarding stage. The Company maintains an ongoing obligation to ensure that customer information remains accurate and up to date. Customers may be required to periodically resubmit documentation or provide updated information in the event of changes to their personal details, corporate structure, or financial activity.

Failure to comply with KYC requirements, or the provision of false, incomplete, or misleading information, may result in the rejection of the application, suspension of account access, or termination of the business relationship.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

In cases of suspected fraud or financial crime, the matter may be escalated to relevant regulatory or law enforcement authorities.
The Company ensures that all KYC data is stored securely and handled in accordance with applicable data protection and confidentiality requirements. Access to KYC information is strictly limited to authorized personnel for compliance and regulatory purposes only.
Ultimately, the KYC Requirements framework ensures that Veyron Markets maintains a high standard of customer integrity, reduces exposure to financial crime risks, and complies with global AML/CFT regulatory expectations.

For Legal Entities

For legal entity customers, the Know Your Customer (KYC) requirements are more extensive due to the increased complexity of corporate structures and the higher potential risk of misuse for money laundering, terrorist financing, tax evasion, or other financial crimes. Veyron Markets applies enhanced scrutiny to all corporate onboarding processes to ensure full transparency of ownership, control, and source of funds.
All legal entities are required to provide complete identification and incorporation details to establish their legal existence. This includes the official registered company name, trading name (if applicable), company registration number, date of incorporation, country of incorporation, registered office address, and principal place of business. The Company may also request additional licensing or regulatory information where the entity operates in a regulated sector.
To understand the nature of the business relationship, the legal entity must disclose its core business activities, industry sector, expected transaction behavior, and purpose of account usage. This information is used to assess whether the expected activity is consistent with the Company's risk appetite and operational profile.
A critical component of corporate KYC is the verification of the ownership and control structure of the entity. The Company requires a complete ownership chart or structure diagram that clearly identifies all direct and indirect shareholders. All individuals or entities holding significant ownership interest (typically 25% or more, or as defined by applicable regulations) must be disclosed as Ultimate Beneficial Owners (UBOs). Where no individual meets the ownership threshold, the natural person(s) exercising control through other means must be identified and verified.
For each UBO, the Company requires full KYC documentation equivalent to that required for individual customers, including valid identification documents and proof of address. This ensures transparency in the chain of ownership and prevents concealment of illicit funds

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

through complex corporate arrangements or nominee structures.

In addition to UBO identification, the Company requires details of all directors, partners, authorized signatories, and individuals who exercise control over the management of the entity. These individuals must be properly identified and verified, and their authority to act on behalf of the entity must be supported by appropriate corporate resolutions or legal documents.

Corporate customers are required to submit official incorporation documents, including the Certificate of Incorporation, Memorandum and Articles of Association, and any amendments thereto. Where applicable, the Company may also request a Certificate of Good Standing or equivalent document issued by the relevant regulatory authority to confirm the ongoing legal status of the entity.

A board resolution or equivalent governing document authorizing the opening of the account and designating authorized signatories is mandatory. This ensures that the account is being opened with proper corporate approval and governance oversight.

Depending on the risk classification of the entity, the Company may request additional supporting documentation, such as financial statements, audited reports, tax identification numbers, or bank references. These documents assist in verifying the legitimacy of the entity's financial position and assessing its source of funds and source of wealth.

All documents submitted by legal entities are subject to verification through manual review and, where applicable, independent third-party validation. Any inconsistencies, missing information, or indications of elevated risk will result in escalation to the Compliance Department and may trigger Enhanced Due Diligence (EDD) procedures.

Legal entity customers are also subject to ongoing monitoring throughout the business relationship. Any changes in ownership structure, directors, business activity, or control must be promptly communicated to the Company and may require re-verification of KYC information.

Failure to comply with corporate KYC requirements, or the submission of false or misleading information, may result in account rejection, suspension, or termination of the business relationship. Where necessary, suspicious cases will be escalated to the AML Compliance Officer and relevant authorities.

Through these requirements, Veyron Markets ensures full transparency of corporate clients, mitigates the risks associated with complex ownership structures, and maintains compliance with international AML/CFT standards.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

DOCUMENT VERIFICATION

Document verification is a critical control within the Company's Anti-Money Laundering (AML), Counter-Terrorist Financing (CFT), and Know Your Customer (KYC) framework. It is designed to ensure that all customer-submitted documents are authentic, valid, accurate, and consistent with the information provided during the onboarding process.

The objective of document verification is to prevent the use of forged, altered, expired, or fraudulent documents for the purpose of opening or maintaining an account with Veyron Markets. This process ensures that the Company only establishes business relationships with verified and legitimate individuals or legal entities.

All documents submitted by customers, whether individuals or legal entities, are subject to systematic review and validation. The verification process may include a combination of automated tools, manual assessment, and cross-referencing with reliable third-party databases or official registries, depending on the risk classification of the customer.

For individual customers, document verification primarily focuses on identity and address confirmation. Identity documents such as passports, national identity cards, or driving licenses are reviewed to ensure they are valid, unexpired, and issued by recognized authorities. Key security features, including photograph matching, document integrity, and consistency of personal details, are carefully assessed. Proof of address documents such as utility bills or bank statements are also verified to confirm residential details and ensure they are recent, typically issued within the last three months.

For corporate customers, document verification involves a more detailed review of incorporation and ownership-related documents. The Company verifies the authenticity of incorporation certificates, constitutional documents, and corporate filings to confirm the legal existence of the entity. Ownership structure documents are reviewed to ensure transparency of Ultimate Beneficial Ownership (UBO), and all relevant individuals are properly identified and verified.

The verification process also includes checks for document integrity and fraud indicators. These may include inconsistencies in formatting, signs of digital manipulation, mismatched fonts, missing security features, or discrepancies between submitted information and supporting records. Any such irregularities are treated as potential red flags and are escalated to the Compliance Department for further investigation.

Where necessary, the Company may independently verify submitted information using third-party verification systems, government databases, corporate registries, or credit reference agencies.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

This helps ensure that the information provided by the customer is accurate and corresponds with external reliable sources.

Document verification is closely integrated with the Company's sanctions screening and risk assessment processes. Any discrepancies identified during verification may impact the customer's risk rating and could trigger Enhanced Due Diligence (EDD) measures or result in rejection of the onboarding application.

In cases where documentation is incomplete, unclear, expired, or otherwise insufficient, the customer will be requested to provide additional or updated documentation. Failure to comply with such requests within a reasonable timeframe may result in suspension or rejection of the application or restriction of account access.

All verified documents are securely stored in accordance with the Company's data protection and record-keeping policies. Access to such documents is strictly limited to authorized personnel for compliance, audit, and regulatory purposes only.

The Company ensures that document verification is an ongoing process and not limited to the initial onboarding stage. Customers may be required to resubmit documentation periodically or upon request, particularly where changes in personal details, corporate structure, or risk profile occur.

Ultimately, document verification ensures that Veyron Markets maintains a secure onboarding environment, prevents identity fraud, and complies with applicable AML/CFT regulatory requirements and international best practices.

Entities

For legal entity customers, the term "Entities" refers to all non-individual clients, including but not limited to companies, corporations, partnerships, trusts, foundations, associations, and any other form of incorporated or unincorporated organization establishing a business relationship with Veyron Markets.

All entities are subject to enhanced Know Your Customer (KYC) and Customer Due Diligence (CDD) requirements due to the increased complexity of their ownership structures and the potential for misuse in concealing beneficial ownership or layering illicit funds. The Company applies a fully transparent approach to ensure that the true ownership, control, and purpose of each entity is clearly identified and verified prior to account activation.

Each entity is required to provide complete identification details, including its legal name, trading name (if applicable), registration number, date of incorporation or formation, country of establishment, registered office address, and principal place of business.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

This information is verified against official corporate registries or equivalent authoritative sources where available.

In addition to basic identification, entities must disclose the nature of their business activities, operational structure, industry sector, and expected transactional behavior. This enables the Company to assess whether the entity's intended use of services is consistent with its declared business profile and risk appetite.

A fundamental requirement for all entities is the disclosure and verification of ownership and control structures. The Company requires a detailed ownership chart that identifies all direct and indirect shareholders, as well as any individuals or entities exercising significant control over the organization. All Ultimate Beneficial Owners (UBOs), typically defined as natural persons holding 25% or more ownership or control, must be clearly identified and verified.

Where ownership is distributed in a complex or layered structure, the Company will require full transparency of each layer until all natural persons exercising ultimate control are identified. This ensures that no anonymity is maintained through intermediary companies, trusts, or nominee arrangements.

All UBOs, directors, partners, and authorized signatories associated with the entity are required to undergo individual KYC verification. This includes submission of valid identification documents, proof of address, and any additional information necessary to assess their role, authority, and risk exposure.

Entities are also required to provide supporting corporate documentation, including but not limited to the Certificate of Incorporation, Memorandum and Articles of Association, partnership agreements (where applicable), and any amendments or updates to governing documents. A board resolution or equivalent authorization document confirming the decision to open an account with the Company and identifying authorized signatories is mandatory.

Depending on the risk profile of the entity, additional documentation may be required, such as financial statements, audited reports, tax identification numbers, business licenses, or bank references. These documents assist in validating the legitimacy, financial standing, and operational authenticity of the entity.

The Company performs thorough verification of all submitted entity documentation using manual review processes and, where necessary, independent validation through corporate registries, regulatory databases, or third-party verification systems. Any inconsistencies, missing information, or indicators of heightened risk are escalated to the Compliance Department for further assessment.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

Entities are continuously subject to ongoing monitoring throughout the business relationship. Any changes in ownership structure, management, business activity, or control must be immediately disclosed to the Company and may trigger re-verification of KYC and risk assessment procedures.

Failure by an entity to provide accurate, complete, or verifiable information, or the identification of suspicious or inconsistent data, may result in rejection of onboarding, suspension of account access, or termination of the business relationship. Where required, such cases may be reported to relevant regulatory or law enforcement authorities.

Through these measures, Veyron Markets ensures that all entities engaging with the Company are legitimate, transparent, and compliant with applicable AML/CFT standards, thereby reducing exposure to financial crime risks and maintaining the integrity of the financial system.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

Entities are continuously subject to ongoing monitoring throughout the business relationship. Any changes in ownership structure, management, business activity, or control must be immediately disclosed to the Company and may trigger re-verification of KYC and risk assessment procedures.

Failure by an entity to provide accurate, complete, or verifiable information, or the identification of suspicious or inconsistent data, may result in rejection of onboarding, suspension of account access, or termination of the business relationship. Where required, such cases may be reported to relevant regulatory or law enforcement authorities.

Through these measures, Veyron Markets ensures that all entities engaging with the Company are legitimate, transparent, and compliant with applicable AML/CFT standards, thereby reducing exposure to financial crime risks and maintaining the integrity of the financial system.

ENHANCED DUE DILIGENCE (EDD)

Enhanced Due Diligence (EDD) is an advanced level of Customer Due Diligence applied by Veyron Markets to customers, transactions, and business relationships that present a higher risk of money laundering, terrorist financing, fraud, or other financial crimes. EDD is designed to provide a deeper and more comprehensive understanding of the customer's identity, financial profile, and transactional behavior, beyond the standard KYC and CDD requirements.

The application of EDD is mandatory in situations where the customer is identified as high-risk based on the Company's Risk-Based Approach (RBA). This includes, but is not limited to, Politically Exposed Persons (PEPs), customers originating from high-risk or sanctioned jurisdictions, entities with complex or opaque ownership structures, and customers whose transaction patterns are unusually large, inconsistent, or difficult to explain in relation to their declared profile.

The primary objective of Enhanced Due Diligence is to mitigate the increased risk exposure associated with such customers by obtaining a higher level of assurance regarding the legitimacy of their identity, source of funds, and overall business activities. EDD ensures that the Company has sufficient information to make informed decisions about whether to establish or continue a business relationship.

As part of the EDD process, the Company conducts additional verification measures beyond standard due diligence. This may include obtaining detailed information on the customer's source of wealth, including supporting documentation such as financial statements, salary certificates, business ownership records, investment portfolios, or other relevant financial evidence.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

EDD Measures

Enhanced Due Diligence (EDD) measures implemented by Veyron Markets are designed to mitigate heightened financial crime risks associated with high-risk customers, transactions, and jurisdictions. These measures ensure that the Company applies a deeper level of scrutiny, verification, and ongoing oversight than standard Customer Due Diligence procedures.

EDD measures begin with the collection of additional and more detailed information relating to the customer's identity, financial background, and business activities. The Company obtains comprehensive evidence of source of funds and, where necessary, source of wealth. This may include salary certificates, audited financial statements, tax returns, bank statements, investment records, business ownership documents, or other supporting evidence that substantiates the legitimacy of the customer's financial profile.

For corporate customers, EDD measures include a detailed review of the organizational structure, ownership chain, and control mechanisms. The Company conducts in-depth verification of all Ultimate Beneficial Owners (UBOs), directors, and key decision-makers. Where ownership structures are complex or layered, additional documentation is required to ensure full transparency and identification of all natural persons exercising control.

EDD also requires intensified screening procedures, including enhanced sanctions checks, Politically Exposed Person (PEP) identification, and adverse media monitoring. The Company utilizes multiple data sources and screening tools to ensure that no high-risk indicators are overlooked. Any potential match identified during screening is subject to immediate escalation and detailed review.

A key component of EDD is the requirement for senior management approval prior to onboarding or continuation of the business relationship. This ensures that high-risk decisions are reviewed at an appropriate governance level and that the Company's risk appetite is not exceeded without proper authorization.

In addition, customers subject to EDD are placed under enhanced ongoing monitoring. Their transactions are reviewed more frequently and in greater detail to identify unusual patterns, inconsistencies, or deviations from expected behavior. Any suspicious activity identified under enhanced monitoring is escalated to the AML Compliance Officer for further investigation and potential reporting to relevant authorities.

EDD measures also include periodic re-assessment of the customer's risk profile. Any significant changes in transaction behavior, geographic exposure, ownership structure, or external risk intelligence triggers a mandatory review and potential reclassification of risk status.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

SANCTIONS & SCREENING CONTROLS

Veyron Markets implements comprehensive and robust sanctions and screening controls as part of its overall Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) framework. These controls are designed to ensure full compliance with applicable international laws, regulatory requirements, and global financial crime prevention standards. The Company adopts a zero-tolerance approach toward sanctions breaches and strictly prohibits entering into or maintaining business relationships with any individuals, entities, or jurisdictions subject to sanctions.

To achieve this, the Company conducts systematic screening against multiple authoritative and globally recognized databases. These include international sanctions lists such as the United Nations (UN) Sanctions List, the U.S. Office of Foreign Assets Control (OFAC) sanctions lists, the UK Office of Financial Sanctions Implementation (OFSI) consolidated list, and the European Union (EU) Consolidated Sanctions List. In addition to sanctions lists, the Company screens against government-issued watchlists, Politically Exposed Person (PEP) databases, and reputable adverse media sources to identify potential reputational and financial crime risks.

The Company ensures that all sanctions data sources are regularly updated and maintained in line with the latest available information. Screening systems and tools are configured to automatically synchronize with updated sanctions data to ensure that newly designated individuals, entities, or jurisdictions are promptly identified. This ensures that the Company remains continuously aligned with evolving global sanctions regimes and regulatory expectations.

Sanctions screening is conducted at multiple stages of the customer lifecycle. This includes initial screening during the onboarding process prior to establishing any business relationship, as well as ongoing screening throughout the duration of the relationship. Additionally, screening is performed whenever there is a material change in customer information, such as changes in ownership structure, geographic location, or transaction behavior. The Company also conducts periodic rescreening of its entire customer base using automated systems to ensure continuous compliance with updated sanctions lists and emerging risk indicators.

All customers, including both natural persons and legal entities, are subject to real-time and periodic screening processes. The Company utilizes advanced screening methodologies, including name matching algorithms, fuzzy logic detection, and risk-based filtering techniques, to identify potential matches. These systems are designed to minimize false positives while maintaining a high level of accuracy and sensitivity in detecting true matches. Manual review

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

processes are also applied where necessary to validate system-generated alerts and ensure appropriate decision-making.

In the event that a potential match is identified, the case is immediately escalated to the Compliance Department for further investigation. The Compliance team conducts a detailed analysis, which may include reviewing customer identification data, transaction history, supporting documentation, and external intelligence sources. The purpose of this review is to determine whether the match is a true positive or a false positive. All findings, decisions, and supporting rationale are fully documented and retained for audit and regulatory purposes.

Where a match is confirmed, the Company takes immediate and appropriate action in accordance with applicable laws and internal policies. Such actions may include rejecting the onboarding application, freezing or restricting the customer's account, suspending transactions, or terminating the business relationship. The Company ensures that all actions taken are proportionate to the level of risk identified and are consistent with regulatory obligations.

In cases involving confirmed sanctions exposure or where there are reasonable grounds for suspicion, the Company may be required to report the matter to relevant regulatory authorities, financial intelligence units, or other competent bodies without delay. All reporting is conducted in accordance with applicable legal requirements and within prescribed timelines. The Company maintains strict confidentiality in all such matters and adheres to "no tipping-off" obligations.

The sanctions and screening framework is subject to continuous review and enhancement to ensure its effectiveness in identifying and mitigating financial crime risks. The Company regularly updates its screening tools, data providers, and internal procedures to reflect changes in international sanctions regimes, regulatory expectations, and emerging risk typologies. Internal audits and compliance reviews are conducted periodically to assess the adequacy and effectiveness of the screening framework.

Through these measures, Veyron Markets ensures that its sanctions and screening controls remain robust, responsive, and fully aligned with global best practices, thereby safeguarding the integrity of its operations and contributing to the prevention of financial crime.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

TRANSACTION MONITORING

Veyron Markets operates a comprehensive transaction monitoring system designed to detect, analyze, and prevent suspicious financial activity. The system combines automated monitoring tools with manual oversight to ensure that all customer transactions are reviewed in accordance with the Company's AML/CFT obligations.

Transaction monitoring is applied to all customer accounts on a continuous basis and covers all forms of financial activity, including deposits, withdrawals, transfers, and trading behavior. The objective is to identify transactions that are inconsistent with the customer's known profile, expected activity, or risk classification.

The monitoring system uses predefined rules, thresholds, and behavioral analytics to detect unusual or potentially suspicious activity. These may include unusually large transactions, rapid movement of funds, frequent deposits followed by immediate withdrawals, or trading patterns that lack economic rationale.

In addition, the Company monitors for specific risk indicators such as structuring transactions to avoid reporting thresholds, use of multiple accounts, third-party payments, and transactions involving high-risk jurisdictions. Any activity that triggers these alerts is automatically flagged for further review.

Once a transaction is flagged, it is reviewed by the Compliance Department, which assesses the nature and context of the activity. This review includes examination of customer history, transaction patterns, and supporting documentation. If necessary, the Company may request additional information from the customer to clarify the nature and purpose of the transaction.

Where suspicious activity is identified, the matter is escalated to the AML Compliance Officer for further investigation. If suspicion is confirmed, a Suspicious Activity Report (SAR/STR) is prepared and submitted to the relevant regulatory authority in accordance with legal obligations.

Transaction monitoring is an ongoing and dynamic process. The Company regularly reviews and updates its monitoring rules, thresholds, and detection models to ensure effectiveness against emerging financial crime typologies and evolving regulatory expectations.

All monitoring activities, alerts, investigations, and decisions are fully documented and retained for audit and regulatory purposes. This ensures transparency, accountability, and compliance with applicable AML/CFT requirements.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

MONITORING RULES / TRIGGERS

Veyron Markets implements a structured set of monitoring rules and predefined triggers within its transaction monitoring framework to identify potentially unusual, inconsistent, or suspicious customer activity. These rules are designed based on known money laundering typologies, regulatory expectations, and internal risk assessments, and are continuously reviewed to ensure effectiveness against emerging financial crime trends.

Monitoring rules are applied to all customer transactions, including deposits, withdrawals, internal transfers, and trading activity. The system evaluates transactions in real time and post-event analysis to detect deviations from expected customer behavior and profile.

Key monitoring triggers include, but are not limited to, transactions exceeding predefined monetary thresholds that are inconsistent with the customer's declared income, financial profile, or historical activity. Any sudden increase in account funding or trading volume without reasonable explanation is flagged for review.

Additional triggers include frequent deposits followed by immediate withdrawals without substantial trading activity, which may indicate layering or attempted placement of illicit funds. Patterns of structuring transactions into smaller amounts to avoid internal limits or reporting thresholds are also considered high-risk indicators.

The system also flags transactions involving third-party payments, where the funding source does not match the account holder's identity, as well as multiple accounts controlled or linked to the same individual or entity without clear justification.

Transactions involving high-risk jurisdictions, sanctioned countries, or regions with weak AML/CFT controls are automatically subject to enhanced scrutiny. Similarly, accounts that demonstrate inconsistent trading behavior, such as rapid high-volume trading followed by withdrawal of funds, are reviewed closely.

All triggered alerts are reviewed by the Compliance Department, which assesses the transaction context, customer profile, and supporting documentation before determining whether escalation is required.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

SUSPICIOUS ACTIVITY IDENTIFICATION

Suspicious activity is identified through a combination of automated alerts, manual reviews, employee observations, and external intelligence sources. The Company defines suspicious activity as any transaction, behavior, or pattern that appears inconsistent with the customer's known profile, lacks economic or legal justification, or suggests potential involvement in money laundering, terrorist financing, fraud, or other financial crimes.

Indicators of suspicious activity may include unexplained or excessive transaction volumes, inconsistent financial behavior, or activity that does not align with the customer's stated occupation, business model, or source of funds. Transactions that appear structured to evade reporting thresholds or internal controls are also treated as suspicious indicators.

The Company also considers behavioral red flags such as reluctance or refusal by a customer to provide requested information, sudden changes in transaction patterns, or frequent movement of funds through multiple accounts or jurisdictions without clear purpose.

All identified suspicious activity is documented and escalated to the AML Compliance Officer for detailed investigation. The Compliance Officer evaluates whether the activity has a legitimate explanation or whether it constitutes reasonable grounds for suspicion of financial crime.

Where suspicion is confirmed or cannot be reasonably dismissed, the Company proceeds with the filing of a Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR) in accordance with applicable regulatory requirements. The Company also assesses whether it is necessary to restrict, suspend, or terminate the customer relationship to mitigate further risk exposure.

Tipping-off the customer regarding any investigation, suspicion, or reporting activity is strictly prohibited under all circumstances. All investigations are conducted in strict confidentiality to ensure compliance with legal obligations and to preserve the integrity of ongoing reviews.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

REPORTING PROCEDURES (SAR / STR)

Veyron Markets maintains formal reporting procedures for the identification, investigation, documentation, and submission of Suspicious Activity Reports (SAR) or Suspicious Transaction Reports (STR) to relevant regulatory and financial intelligence authorities.

The reporting process begins when a transaction or customer activity is flagged as suspicious through monitoring systems, employee observations, or external alerts. Once identified, the case is immediately escalated to the AML Compliance Officer or Money Laundering Reporting Officer (MLRO) for review.

The AML Compliance Officer conducts a detailed investigation, which includes reviewing customer identification data, transaction history, risk classification, source of funds information, and any supporting documentation provided by the customer. Where necessary, additional information may be requested internally, ensuring that all analysis is properly documented.

If, after review, the Compliance Officer determines that there are reasonable grounds to suspect that the funds or activity are linked to money laundering, terrorist financing, or other financial crimes, a SAR/STR is prepared. This report includes detailed information about the customer, transaction details, reasons for suspicion, and all supporting evidence.

The SAR/STR is then submitted to the relevant financial intelligence unit or regulatory authority in accordance with applicable laws and reporting timelines. The Company ensures that all submissions are accurate, complete, and made without undue delay.

All reporting activities are strictly confidential. Employees are prohibited from disclosing any information related to suspicious activity investigations or reports to the customer or any unauthorized third party. Any breach of confidentiality or tipping-off provisions is treated as a serious disciplinary offense.

Following submission of a SAR/STR, the Company continues to monitor the customer’s activity closely and may take additional risk mitigation measures, including transaction restrictions, enhanced monitoring, or termination of the business relationship, depending on the severity of the case.

All SAR/STR records, supporting documentation, and investigation notes are securely retained in accordance with regulatory record-keeping requirements and are made available to auditors or regulators upon request.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

INVESTIGATION

The investigation process is a key control within the Company's AML/CFT framework and is designed to ensure that all alerts, escalations, and reported activities are assessed in a consistent and risk-based manner. The AML Compliance Officer is responsible for reviewing all cases using available internal information such as KYC/CDD data, transaction history, risk classification, sanctions screening results, and prior account activity.

Each investigation begins with an assessment of the customer's expected profile, including declared source of funds, occupation, and anticipated transaction behavior. This is compared against actual activity to identify any inconsistencies, unusual patterns, or red flags. Where required, additional information may be requested from internal teams or the customer to clarify the nature of transactions, while ensuring strict confidentiality and avoiding any form of tipping-off.

The AML Officer may also use external sources such as adverse media checks, sanctions lists, and corporate registry information to support the review. All findings and decisions are documented, including the rationale for either closing the case or escalating it for further action.

Investigations are conducted independently and objectively to ensure compliance decisions are not influenced by commercial considerations.

Where reasonable grounds for suspicion are identified, the matter is escalated for external reporting. If no suspicion is found, the case is closed with documented justification, and the customer continues to be monitored based on their risk profile.

EXTERNAL REPORTING

Where an investigation confirms or reasonably suggests suspicious activity, the Company submits a Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR) to the relevant regulatory or financial intelligence authority. Reporting is carried out by the AML Compliance Officer in accordance with applicable laws and regulatory timelines.

Each report includes relevant customer details, transaction information, nature of suspicion, and supporting evidence derived from internal investigations. Reports are submitted promptly once suspicion is established, ensuring accuracy and completeness of information provided to authorities.

In certain cases, the Company may restrict, suspend, or freeze account activity pending regulatory guidance. All reporting actions are strictly confidential, and no information is disclosed to the customer or unauthorized parties under any circumstances.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

CONFIDENTIALITY

All AML-related investigations and reports are treated as strictly confidential. Employees and authorized personnel are prohibited from disclosing any information regarding internal alerts, investigations, or regulatory reporting to customers or third parties.

The Company enforces a strict “no tipping-off” policy to ensure the integrity of investigations and compliance with legal obligations. Any breach of confidentiality is considered a serious violation and may result in disciplinary action, termination, and legal consequences.

Access to AML investigation data is restricted to authorized personnel only, and all related information is securely stored and protected through appropriate internal controls.

ONGOING MONITORING

The Company continuously monitors customer activity to ensure consistency with the customer’s profile and risk classification. Customer information and behavior are periodically reviewed and updated as necessary.

Risk classifications are reassessed based on changes in transaction patterns, geographic exposure, or new risk indicators. High-risk customers are subject to enhanced and more frequent monitoring to ensure early detection of suspicious activity and timely risk mitigation.

RECORD KEEPING

The Company maintains comprehensive records of all AML-related information, including customer identification documents, transaction histories, risk assessments, monitoring outputs, and SAR/STR filings.

All records are securely stored and protected against unauthorized access. The Company retains AML-related records for a minimum period of five to seven years following the termination of the business relationship, or longer where required by applicable law or regulation.

INTERNAL CONTROLS & GOVERNANCE

The AML Compliance Officer is responsible for implementing, maintaining, and overseeing the Company’s AML/CFT framework. This includes monitoring compliance effectiveness, managing investigations, and liaising with regulatory authorities.

The Company maintains strong internal controls, including segregation of duties, structured approval processes, audit trails, and compliance monitoring systems. These controls ensure accountability, transparency, and effective risk management across all operations.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

EMPLOYEE TRAINING

All employees are required to undergo AML/CFT training at the time of onboarding and on an annual basis thereafter. Training ensures that staff are aware of their obligations and able to identify and respond to potential financial crime risks.

Training covers key areas such as customer due diligence, identification of suspicious activity, internal escalation procedures, and regulatory reporting requirements.

DATA PROTECTION

The Company ensures that all customer and transactional data is securely stored and accessed only by authorized personnel for legitimate compliance purposes. Appropriate safeguards are implemented to prevent unauthorized access, loss, or misuse of sensitive information.

The Company complies with applicable data protection laws and ensures confidentiality, integrity, and security of all AML-related data.

NON-COMPLIANCE

Failure to comply with this Policy may result in disciplinary action, including termination of employment or contractual relationships. In serious cases, non-compliance may lead to legal proceedings and regulatory sanctions.

The Company maintains a zero-tolerance approach toward violations of AML/CFT obligations.

TRANSACTION VERIFICATION

The Company reserves the right to request additional verification documents at any time, including proof of payment methods, bank or card statements, and source of funds declarations. Customers must provide requested documentation in a timely manner. Failure to comply may result in account suspension, transaction restrictions, or termination of the business relationship.

RISK MITIGATION MEASURES

The Company implements a combination of automated monitoring systems, manual compliance reviews, escalation procedures, and periodic internal audits to mitigate AML/CFT risks.

These measures are designed to ensure early detection of suspicious activity, effective risk control, and continuous improvement of the compliance framework.

+44 7482 197196
www.veyronmarkets.com
support@veyronmarkets.com

EMPLOYEE TRAINING

All employees are required to undergo AML/CFT training at the time of onboarding and on an annual basis thereafter. Training ensures that staff are aware of their obligations and able to identify and respond to potential financial crime risks.

Training covers key areas such as customer due diligence, identification of suspicious activity, internal escalation procedures, and regulatory reporting requirements.

DATA PROTECTION

The Company ensures that all customer and transactional data is securely stored and accessed only by authorized personnel for legitimate compliance purposes. Appropriate safeguards are implemented to prevent unauthorized access, loss, or misuse of sensitive information.

The Company complies with applicable data protection laws and ensures confidentiality, integrity, and security of all AML-related data.

NON-COMPLIANCE

Failure to comply with this Policy may result in disciplinary action, including termination of employment or contractual relationships. In serious cases, non-compliance may lead to legal proceedings and regulatory sanctions.

The Company maintains a zero-tolerance approach toward violations of AML/CFT obligations.

TRANSACTION VERIFICATION

The Company reserves the right to request additional verification documents at any time, including proof of payment methods, bank or card statements, and source of funds declarations. Customers must provide requested documentation in a timely manner. Failure to comply may result in account suspension, transaction restrictions, or termination of the business relationship.

RISK MITIGATION MEASURES

The Company implements a combination of automated monitoring systems, manual compliance reviews, escalation procedures, and periodic internal audits to mitigate AML/CFT risks.

These measures are designed to ensure early detection of suspicious activity, effective risk control, and continuous improvement of the compliance framework.