ZoraFX Global Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) Policy

Preamble: A Note on ZoraFX's Global Compliance Posture

ZoraFX operates as a global brokerage and proprietary trading firm, providing clients from around the world with access to forex and cryptocurrency markets.[1] In recognition of our global client base and the cross-jurisdictional nature of modern financial markets, ZoraFX has adopted a unified, global compliance framework. This framework is not predicated on the requirements of a single jurisdiction. Instead, it is proactively designed to meet and, where appropriate, exceed the highest international standards for combating financial crime.

By synthesizing the most stringent principles from leading regulatory regimes and international bodies, ZoraFX ensures a consistent and robust standard of compliance across all its operations. This approach demonstrates our unwavering commitment to protecting the integrity of our platform and the broader financial ecosystem. This document outlines the policies and procedures that form the bedrock of this commitment.

Section 1: Introduction and Overarching Policy Statement

1.1. Commitment to Combating Financial crime

ZoraFX maintains a zero-tolerance policy for money laundering (ML), the financing of terrorism (CFT), and all other forms of illicit financial activity. The firm is unequivocally committed to preventing the use of its products and services for criminal purposes. This policy establishes the framework of controls, systems, and procedures designed to ensure that ZoraFX, its employees, and its clients operate with the highest degree of integrity and in full compliance with applicable legal and regulatory obligations.

1.2. Policy Objective

The primary objective of this Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) Policy is to protect the ZoraFX platform, its clients, and the global financial system from the risks associated with financial crime.[3] This is achieved through a comprehensive and risk-based program designed to:

- **Prevent:** Prohibit and actively obstruct any attempts to use the ZoraFX platform for illicit purposes.

- **Detect:** Identify and scrutinize activities that may be indicative of money laundering, terrorist financing, or other financial crimes.
- **Report:** Report suspicious activities to the appropriate Financial Intelligence Units (FIUs) and law enforcement agencies in a timely and confidential manner.[4]

1.3. Scope of Application

This policy is universally applicable and binding upon all ZoraFX officers, directors, employees, and any agents acting on behalf of the firm. It governs all aspects of the business relationship with clients, including account opening, transactions, and ongoing monitoring across all offered products and services, which encompass forex and cryptocurrency trading.[1] Adherence to this policy is a mandatory condition of employment with ZoraFX and of maintaining a client relationship with the firm.

1.4. Definition of Terms

To ensure clarity and consistent interpretation, the following definitions apply throughout this policy:

- **AML (Anti-Money Laundering):** A comprehensive set of laws, regulations, and procedures designed to prevent criminals from disguising illegally obtained funds as legitimate income.[3]
- **CFT (Counter-Financing of Terrorism):** Measures and efforts aimed at preventing the financing of terrorists, terrorist acts, and terrorist organizations.
- **FATF (Financial Action Task Force):** An independent, inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction.[6]
- **FIU (Financial Intelligence Unit):** A central, national agency responsible for receiving, analyzing, and disseminating disclosures of financial information, particularly concerning suspected proceeds of crime and potential financing of terrorism.
- **KYC (Know Your Customer):** The process a business uses to verify the identity of its clients and assess their suitability, along with the potential risks of illegal intentions for the business relationship.[3] KYC is the cornerstone of any effective AML program.

- **MLRO (Money Laundering Reporting Officer):** A senior individual within the firm designated with the responsibility for overseeing the AML/CFT framework and reporting suspicious activity.[7]
- **PEP (Politically Exposed Person):** An individual who is or has been entrusted with a prominent public function. Due to their position and influence, PEPs are recognized as presenting a higher risk for potential involvement in bribery and corruption.[4] This definition extends to their family members and close associates.
- **RBA (Risk-Based Approach):** The principle that firms should identify, assess, and understand the ML/TF risks to which they are exposed and apply AML/CFT measures that are commensurate with those risks.[9]
- **SAR (Suspicious Activity Report):** A report filed with the relevant FIU by a financial institution regarding a transaction or activity that is suspected to be related to financial crime.[5]
- **UBO (Ultimate Beneficial Owner):** The natural person(s) who ultimately owns or controls a corporate entity or legal arrangement, or on whose behalf a transaction is being conducted.[10]

Section 2: The ZoraFX AML/CFT Regulatory and Compliance Framework

2.1. Foundation on International Standards

ZoraFX's AML/CFT framework is fundamentally built upon the 40 Recommendations published by the Financial Action Task Force (FATF). These recommendations are recognized globally as the international standard for combating money laundering and the financing of terrorism and proliferation.[6] By anchoring our policy to the FATF standards, ZoraFX ensures its controls are aligned with a comprehensive and consistent framework that has been endorsed by over 180 countries.[6] This provides a robust, internationally recognized foundation for all our compliance efforts.

2.2. Synthesis of Leading Jurisdictional Requirements

To construct a compliance program that is effective in a global context, ZoraFX has synthesized the most stringent and advanced requirements from the world's leading regulatory regimes. This approach ensures our controls are not only comprehensive but also adapted to the evolving nature of financial crime and technology. Our framework specifically incorporates key principles from:

- **The European Union's Anti-Money Laundering Directives (AMLDs):** ZoraFX pays close attention to the evolution of the EU's AML framework, particularly the 4th, 5th, and 6th AMLDs. These directives have progressively strengthened compliance obligations. The 4th AMLD aligned the EU with FATF standards and introduced a stronger risk-based approach and central registers for beneficial ownership.[8] The 5th AMLD extended the scope of regulation to include virtual asset service providers (VASPs) and prepaid cards, and enhanced due diligence requirements for Politically Exposed Persons (PEPs).[13] The 6th AMLD is particularly relevant as it harmonized the definition of money laundering predicate offenses across the EU, adding cybercrime and environmental crime, and extended criminal liability to legal persons (i.e., corporations), making companies directly responsible for the criminal actions of their employees.[13] By incorporating these advanced provisions, ZoraFX ensures its policy is equipped to handle the specific risks of its forex and crypto offerings.
- **The United States' Bank Secrecy Act (BSA) and FINRA Rules:** We align with the principles of the U.S. BSA, which requires financial institutions to assist government agencies in detecting and preventing money laundering.[4] The structure of our AML program is modeled on the clear and comprehensive framework mandated by the Financial Industry Regulatory Authority (FINRA) Rule 3310. This rule provides a blueprint for a well-organized and auditable AML program.[16]

2.3. The Five Pillars of ZoraFX's Compliance Program

Modeled after the robust requirements of FINRA Rule 3310 and global best practices, ZoraFX's AML/CFT program is built upon five essential pillars, ensuring a comprehensive and resilient compliance structure.[17]

1. **A System of Internal Controls:** ZoraFX has established and will maintain a system of written policies, procedures, and internal controls designed to detect and report suspicious activity. This entire AML/CFT policy, and its supporting internal procedures, are approved in writing by senior management.
2. **Independent Testing:** The firm is committed to conducting an independent test of its AML program at least annually (on a calendar-year basis). This testing will be performed by a qualified party—either internal personnel independent of the functions being tested or a qualified external third party—to assess the program's effectiveness and ensure its continued compliance with regulatory standards.[16]
3. **Designated Compliance Personnel:** ZoraFX has appointed a qualified and experienced Money Laundering Reporting Officer (MLRO) who is responsible for the

day-to-day implementation and oversight of the AML program. The MLRO's role and responsibilities are detailed further in Section 3.

4. **Ongoing Employee Training:** ZoraFX provides a comprehensive, ongoing training program for all appropriate personnel. This ensures that every relevant employee understands their responsibilities under the AML/CFT framework and can effectively identify potential red flags. This program is detailed in Section 10.
5. **Risk-Based Customer Due Diligence (CDD):** ZoraFX has implemented a robust, risk-based program for conducting customer due diligence. This includes a Customer Identification Program (CIP) to verify the identity of every client, procedures to identify beneficial owners, and ongoing monitoring to develop a customer risk profile and detect suspicious transactions. This pillar is detailed in Sections 4, 5, and 6.

This five-pillar structure provides a clear, logical, and auditable framework that ensures all critical aspects of AML/CFT compliance are systematically addressed and managed.

Section 3: Governance and the Money Laundering Reporting Officer (MLRO)

3.1. Designation and Seniority

ZoraFX recognizes that effective AML/CFT governance requires strong leadership and clear lines of responsibility. To this end, ZoraFX has appointed a Money Laundering Reporting Officer (MLRO). The MLRO is a senior-level employee who possesses the requisite experience, expertise, and authority to oversee the firm's financial crime prevention framework.[7] To ensure the MLRO's independence and influence, they have a direct reporting line to the firm's senior management and/or Board of Directors, allowing for unfiltered communication on compliance matters.[21] The MLRO function is a controlled function requiring a high degree of integrity and competence.

3.2. Core Responsibilities of the MLRO

The MLRO serves as the central point of contact and oversight for all AML/CFT-related activities within ZoraFX. Their responsibilities are comprehensive and critical to the integrity of the firm's operations. These duties include, but are not limited to:

- **Policy and Procedure Management:** Developing, implementing, maintaining, and regularly reviewing ZoraFX's AML/CFT policies and procedures to ensure they remain current with evolving laws, regulations, and international best practices.[22]

- **Suspicious Activity Reporting:** Receiving and investigating internal suspicious activity reports (SARs) submitted by employees. The MLRO is responsible for analyzing these reports, conducting further investigation as necessary, and making the final determination on whether a transaction or activity warrants the filing of an external SAR with the relevant Financial Intelligence Unit (FIU).[7]
- **Regulatory Liaison:** Acting as the primary liaison between ZoraFX and all relevant supervisory authorities, law enforcement agencies, and FIUs on matters related to money laundering and terrorist financing.[20]
- **Employee Training and Awareness:** Overseeing the firm's AML/CFT training program to ensure that all relevant employees and management are aware of their legal obligations and are equipped to identify and report suspicious activity. This includes both initial and ongoing training.[22]
- **Senior Management Reporting:** Preparing and presenting a formal report to senior management at least annually. This report assesses the effectiveness of the firm's AML/CFT systems and controls, summarizes SAR activity, highlights emerging risks, and provides recommendations for enhancement.[21]
- **Risk Advisory:** Advising senior management on the financial crime risks associated with new products, services, technologies, or expansion into new geographic markets, ensuring that AML/CFT considerations are embedded in strategic decision-making.[20]
- **Day-to-Day Oversight:** Monitoring the day-to-day operation of the firm's AML systems, including customer onboarding checks and transaction monitoring, to ensure they are functioning effectively.[21]

3.3. Resources and Authority

ZoraFX is committed to empowering the MLRO to fulfill their duties effectively and without impediment. The firm ensures that the MLRO is provided with:

- **Sufficient Resources:** This includes adequate time, budget, and support staff necessary to manage the compliance function effectively.[21]
- **Technological Support:** Access to necessary compliance technology, such as automated screening tools, transaction monitoring systems, and blockchain analytics software, to enhance the efficiency and effectiveness of the AML/CFT program.[7]

- **Unrestricted Access:** Full and timely access to all relevant client data, transaction records, and any other information required to perform their investigative and oversight functions.[23]
- **Independence and Authority:** The MLRO operates with the necessary independence to make objective decisions, free from commercial or other conflicts of interest. They have the authority to challenge business decisions that pose an unacceptable level of financial crime risk.[23]

By enshrining the MLRO's seniority, comprehensive responsibilities, and operational authority within this policy, ZoraFX ensures that its compliance function is not merely a procedural requirement but a central and influential component of its corporate governance.

Section 4: Risk-Based Approach (RBA)

4.1. The Core Principle

The cornerstone of ZoraFX's AML/CFT program is the Risk-Based Approach (RBA), as advocated by the FATF and leading global regulators.[9] The RBA is a dynamic and intelligent framework that moves beyond a one-size-fits-all, "tick-box" exercise. It requires ZoraFX to identify, assess, and understand the specific money laundering and terrorist financing risks it faces, and then to apply compliance measures that are proportionate to those risks. This ensures that resources are focused most effectively on the areas of greatest concern, leading to a more efficient and impactful AML/CFT program.

4.2. Firm-Wide Risk Assessment

ZoraFX conducts and maintains a comprehensive, documented firm-wide ML/TF risk assessment. This assessment is the foundation of our RBA and informs the design of all our AML/CFT controls.[25] The risk assessment is a continuous process, formally reviewed and updated at least annually, or more frequently in the event of:

- Significant changes to our business model, such as the introduction of new products or services.
- Expansion into new geographic markets.
- The emergence of new financial crime threats or typologies.
- Significant changes in our client base.
- Findings from internal audits, independent testing, or regulatory examinations.[26]

4.3. Risk Factor Categories

In assessing the ML/TF risk posed by a client relationship, ZoraFX considers a holistic range of factors. A client's overall risk rating is determined by analyzing the interplay between these categories, not by any single factor in isolation. The primary risk categories include:

- **Client Risk:** This involves assessing the risk inherent in the client themselves. Factors considered include:
    - The client's legal structure (e.g., individual, corporation, trust).
    - The client's occupation or the industry in which their business operates.
    - The transparency and complexity of a corporate client's ownership structure.
    - The client's stated source of wealth and the source of funds for the account.
    - Whether the client, or their beneficial owner, is identified as a Politically Exposed Person (PEP).
- **Geographic Risk:** This category assesses the risks associated with the client's location and the jurisdictions they transact with. Heightened scrutiny is applied to clients who are resident in, have citizenship from, or conduct significant transactions with jurisdictions that are:
    - Identified by the FATF as having strategic AML/CFT deficiencies (i.e., the "grey" and "black" lists).[10]
    - Known to have high levels of corruption, organized crime, or terrorist activity.
    - Subject to international sanctions or embargoes.
    - Considered to be tax havens or have weak financial regulatory oversight.[5]
- **Product/Service Risk:** This evaluates the ML/TF risks inherent in the products and services used by the client. ZoraFX recognizes that certain products may be more attractive to money launderers. This includes:
    - The high-speed, high-volume nature of forex trading.[1]
    - The potential for anonymity and rapid cross-border transfers associated with certain cryptocurrencies.[13]
    - Services that allow for rapid deposit and withdrawal of funds.

- **Transactional Risk:** This involves analyzing the client's transactional behavior for patterns that may indicate risk. Factors include:
    - The size, frequency, and complexity of transactions.
    - The use of cash or cash equivalents for deposits.
    - Transactions that have no apparent economic or lawful purpose.
    - The velocity of funds through the account (i.e., how quickly funds are deposited and then withdrawn).

4.4. Application of the RBA

The output of this multi-faceted risk assessment is a risk rating for each client (e.g., Low, Medium, High). This rating is not static and is subject to change based on ongoing monitoring. The risk rating directly dictates the level and intensity of customer due diligence that will be applied, as detailed in Section 6. This ensures that clients presenting a lower risk are subject to standard procedures, while high-risk clients receive a proportionately greater level of scrutiny through Enhanced Due Diligence (EDD).

Section 5: Customer Identification and Verification Program (CIP)

5.1. Prohibition of Illegitimate Accounts

ZoraFX maintains a strict and absolute prohibition on certain types of accounts to prevent the most basic forms of financial crime. It is forbidden to open or maintain:

- **Anonymous Accounts:** All accounts must be associated with a clearly identified and verified natural person or legal entity.
- **Accounts in Fictitious Names:** Accounts must be opened in the client's true legal name.
- **Accounts for Shell Banks:** ZoraFX will not establish or maintain any relationship with a "shell bank," which is defined as a bank that has no physical presence in the jurisdiction in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group.[30]

5.2. Timing of Verification

The verification of a client's identity is a critical control point in the onboarding process. ZoraFX will not establish a business relationship, permit any trading activity, or process any fund movements until the identity of the client (and, where applicable, their beneficial owners) has been satisfactorily verified in accordance with the procedures outlined in this

section.[32] This front-loaded approach ensures that ZoraFX knows who its clients are before they can access its services.

5.3. Digital and Documentary Verification

Recognizing the need for both security and efficiency in a digital-first environment, ZoraFX employs a hybrid approach to identity verification. This methodology aligns with the FATF's guidance on Digital Identity, which acknowledges that non-face-to-face onboarding can be standard or even lower risk when robust technologies are used.[33] Our verification process combines:

- **Digital Verification:** We leverage modern identity verification technologies to establish a high level of confidence in a client's identity remotely. This may include:
    - **Biometric Verification:** Using facial recognition technology to match a live selfie of the client against the photograph on their government-issued ID.
    - **Liveness Detection:** Employing advanced checks to ensure the person providing the selfie is physically present and not using a photo, video, or mask.
    - **NFC Chip Reading:** Using Near Field Communication (NFC) technology on a client's mobile device to read the data directly from the chip embedded in modern passports and ID cards, providing a highly secure method of data extraction.
    - **Database Checks:** Cross-referencing provided information against trusted and independent databases to confirm its validity.[35]
- **Documentary Verification:** We require clients to submit clear, legible, and unexpired copies of official identification documents. These documents are carefully reviewed for authenticity and to corroborate the information provided by the client during the application process.

This dual approach allows ZoraFX to achieve a high level of identity assurance, combatting fraud and impersonation while providing a streamlined onboarding experience for legitimate clients.

5.4. Table 1: Required Information and Documentation for Account Opening

To ensure transparency and manage client expectations, the following table outlines the minimum information and documentation required to open an account with ZoraFX. ZoraFX reserves the right to request additional information or documentation at any time based on its risk assessment.

Account Type	Information to be Collected	Acceptable Verification Documents (Non-Exhaustive List)
Individual Accounts	- Full Legal Name - Permanent Residential Address - Date of Birth - Nationality / Country of Citizenship - Occupation and Employment Status - Stated Source of Funds and Source of Wealth - Tax Identification Number (TIN) or equivalent, where applicable 36	Proof of Identity: - Government-issued Passport (international clients) - National Identity Card - Driver's License Proof of Address (must be dated within the last 3 months): - Utility Bill (e.g., electricity, water, gas, internet) - Bank or Credit Card Statement from a recognized financial institution - Government-issued correspondence (e.g., tax assessment) 36
Corporate / Institutional Accounts	- Full Legal Name of the Entity - Company Registration Number - Date and Country of Incorporation - Registered Address and Principal Place of Business - Detailed Description of Business Activities - Stated Source of Funds and Source of Wealth	Entity Documents: - Certificate of Incorporation or Registration - Memorandum and Articles of Association (or equivalent constitutional documents) - A recent (e.g., within 12 months) Certificate of Incumbency or similar official document listing current directors and shareholders - Register of Directors and Register of Shareholders/Members - Proof of Business Address (e.g., corporate bank statement, utility bill) 30

	- Full identification details for all Directors - Full identification details for all Ultimate Beneficial Owners (UBOs) with 25% or more ownership or control 3	
Individual Documents (for each Director and UBO)	- The same Proof of Identity and Proof of Address documents as required for Individual Accounts.	

Section 6: Customer Due Diligence (CDD) and Ongoing Monitoring

Customer Due Diligence is the process through which ZoraFX develops an understanding of its clients to effectively manage ML/TF risks. It extends beyond the initial identity verification (CIP) and continues throughout the entire client relationship. The intensity of CDD is determined by the client's risk profile, as established by our Risk-Based Approach.

6.1. Standard Due Diligence (SDD)

Standard Due Diligence is the baseline level of scrutiny applied to all clients upon establishing a business relationship. SDD encompasses:

- The full Customer Identification and Verification Program (CIP) as detailed in Section 5.
- Understanding the nature and intended purpose of the business relationship. This involves gathering information on the client's expected trading activity, transaction volumes, and the primary purpose for opening the account (e.g., speculation, hedging).
- This information is used to establish a baseline customer risk profile, against which future activity will be monitored for consistency.[17]

6.2. Enhanced Due Diligence (EDD)

Enhanced Due Diligence (EDD) is a more rigorous and intrusive set of measures applied to clients who are identified as presenting a higher risk of involvement in money laundering or

terrorist financing.[3] The purpose of EDD is to gain a deeper understanding of the client and their activities to mitigate the heightened risk.

- **Triggers for EDD:** EDD measures are automatically and mandatorily applied when a client is identified as, or a situation involves:
    - A Politically Exposed Person (PEP), their family member, or a close associate.
    - A client residing in or having significant business dealings with a jurisdiction identified by the FATF or ZoraFX's internal assessment as high-risk.
    - A corporate structure that is unnecessarily complex or opaque, particularly involving shell companies, bearer shares, or nominees where the ultimate beneficial owner is difficult to ascertain.
    - A client operating in a business sector known to be at high risk for money laundering (e.g., cash-intensive businesses, dealers in high-value goods).
    - Any other instance where the cumulative risk factors from the firm's risk assessment indicate a high-risk profile.[4]
- **EDD Measures:** The specific measures taken under EDD are proportionate to the risk identified and may include, but are not limited to:
    - **Senior Management Approval:** Obtaining approval from senior management within ZoraFX to commence or continue the business relationship.[25]
    - **Source of Wealth (SoW) and Source of Funds (SoF) Verification:** Taking reasonable and documented measures to establish the client's source of wealth (the origin of their total net worth) and the source of the specific funds being deposited into their ZoraFX account. This may require obtaining supporting evidence such as tax returns, audited financial statements, pay stubs, or legal documents related to inheritance or asset sales.[5]
    - **Intensified Ongoing Monitoring:** Increasing the frequency and intensity of transaction monitoring for the high-risk account, with lower thresholds for generating alerts.
    - **In-depth Purpose Inquiry:** Seeking additional information and clarification regarding the purpose and rationale behind specific transactions or patterns of activity.

6.3. Politically Exposed Persons (PEPs)

ZoraFX recognizes the higher risks associated with PEPs due to their potential susceptibility to corruption and bribery.[8]

- **Definition:** We adopt the comprehensive FATF definition of a PEP, which includes current and former senior officials in the executive, legislative, administrative, military, or judicial branches of a government, senior executives of state-owned corporations, and important political party officials. This definition also explicitly includes their immediate family members and known close associates.[4]
- **Identification:** ZoraFX utilizes reputable third-party commercial databases and public domain information to screen all new and existing clients for PEP status.
- **Management:** All relationships with PEPs are automatically classified as high-risk and are subject to the full suite of EDD measures, including senior management approval before the account can be activated.[25]

6.4. Beneficial Ownership

Transparency of ownership is a critical tool in preventing the misuse of corporate structures for illicit purposes. ZoraFX is committed to identifying the natural person(s) who ultimately own or control our corporate clients (the UBOs).[3]

- **Identification and Verification:** We take reasonable measures to identify and verify the identity of any natural person who directly or indirectly owns or controls 25% or more of the shares or voting rights in a legal entity client. This 25% threshold is in line with the standard set by the EU's AML Directives.[3]
- **Control Prong:** In addition to the ownership threshold, we seek to identify any individual who exercises ultimate effective control over the entity through other means (e.g., the power to appoint senior management).
- **Stricter Thresholds:** ZoraFX reserves the right to apply a stricter identification threshold (e.g., 10% ownership) for corporate clients deemed to be of a higher risk, based on factors such as their jurisdiction of incorporation or business sector. This flexible, risk-based application of UBO identification is a key control, mirroring best practices seen at other leading brokers.[36]

6.5. Ongoing Monitoring

Customer Due Diligence is not a one-time event at onboarding. ZoraFX conducts ongoing monitoring of all business relationships to ensure that transactions remain consistent with our knowledge of the client, their business, their risk profile, and their stated source of

funds.[5] This ongoing scrutiny allows us to detect changes in behavior or unusual activity that may require re-evaluation of the client's risk rating or further investigation. As part of this process, client information is periodically reviewed and updated to ensure it remains current and accurate.

Section 7: Sanctions Compliance

7.1. Zero-Tolerance Policy

ZoraFX maintains a strict, zero-tolerance policy towards any breach of international sanctions. It is the absolute policy of the firm not to establish or maintain any business relationship, nor to process any transaction, involving individuals, entities, or jurisdictions that are subject to sanctions imposed by major international bodies. This is a matter of strict liability and a cornerstone of our commitment to global security and financial integrity.

7.2. Screening Process

To enforce this policy, ZoraFX has implemented a robust and systematic screening process. All clients, including individual account holders, corporate entities, and their respective Ultimate Beneficial Owners (UBOs) and directors, are screened at the time of onboarding. This screening is conducted against, at a minimum, the sanctions lists published and enforced by:

- The United States Department of the Treasury's Office of Foreign Assets Control (OFAC)
- The United Nations (UN) Security Council
- The European Union (EU)
- His Majesty's Treasury (HMT) in the United Kingdom

By screening against these primary global sanctions regimes, ZoraFX ensures comprehensive coverage of the most critical and widely enforced restrictive measures.[30]

7.3. Ongoing and Transactional Screening

Sanctions compliance is a dynamic and continuous process. ZoraFX's commitment extends beyond the initial onboarding check.

- **Ongoing Screening:** Our entire client database is continuously screened against updated sanctions lists. This ensures that if an existing client becomes subject to sanctions, ZoraFX can take immediate action.

- **Transaction Screening:** All incoming and outgoing payments, including wire transfers and crypto-asset transfers, are screened in real-time. This process is designed to prevent funds from being sent to or received from sanctioned individuals, entities, or wallets, and to block transactions involving sanctioned jurisdictions.[3]

7.4. Action on Positive Matches

In the event that our screening systems identify a confirmed or "true" match to a prohibited party on a sanctions list, ZoraFX will take immediate and decisive action in accordance with applicable laws and regulations. This action will include:

1. Immediately blocking or freezing the client's account and any associated funds or assets under our control.
2. Rejecting the proposed transaction.
3. Filing a report with the relevant regulatory and law enforcement authorities (such as OFAC) without delay.
4. Strictly adhering to the prohibition against "tipping off" the client, meaning no employee will inform the client that they have been identified on a sanctions list or that a report has been filed.

These measures are executed without exception to ensure full compliance with our legal obligations and to prevent any flow of funds to sanctioned actors.

Section 8: Transaction Monitoring and Suspicious Activity Reporting

8.1. Monitoring Systems

ZoraFX employs a sophisticated, multi-layered approach to transaction monitoring, which is essential for detecting activity that may be indicative of financial crime. Our systems are designed to identify transactions that are inconsistent with a client's established risk profile and known legitimate activity. This is achieved through a combination of:

- **Automated Monitoring:** We utilize an automated, rules-based transaction monitoring system that analyzes client activity in real-time. This system is programmed with a series of rules and typologies designed to flag potentially suspicious behavior, such as structuring, unusual transaction sizes, or high-velocity movements of funds.[5]
- **Manual and Intelligence-Led Reviews:** Automated alerts are supplemented by manual reviews conducted by our trained compliance analysts. These reviews

provide human oversight and judgment, helping to distinguish between genuinely suspicious activity and legitimate but unusual behavior. This intelligence-led approach allows us to adapt to new and emerging money laundering typologies that may not yet be captured by automated rules.[25]

The parameters and rules within our monitoring systems are reviewed and calibrated regularly to ensure they remain effective and relevant to the firm's risk environment.

8.2. Table 2: Examples of Suspicious Activity Red Flags

To provide clarity on the types of behavior our monitoring program is designed to detect, the following table presents a non-exhaustive list of suspicious activity red flags. The identification of one or more of these flags will trigger an internal review. The categorization reflects the specific risks associated with ZoraFX's business model, which spans general financial activity as well as the distinct domains of forex and cryptocurrency trading.

Category	Examples of Red Flags (Non-Exhaustive List)
General Account & Transaction Activity	• Transactions that are inconsistent with the client's known financial profile, occupation, or business activity. • Sudden, unexplained, and significant increases in the volume or value of transactions compared to historical patterns. • Structuring deposits or withdrawals into multiple smaller transactions to fall just below reporting or scrutiny thresholds (i.e., "smurfing"). • Use of multiple accounts to collect and funnel funds into a single account, or vice-versa, without a clear business rationale. • Client expresses reluctance to provide required identification documents or information, or provides information that appears to be false, misleading, or forged. • Account activity originating from or connected to IP addresses in high-risk or sanctioned jurisdictions, or the use of VPNs, proxies, or other anonymizing tools to obscure location.

Forex-Specific Activity	• -Rapidly moving funds between unrelated accounts or across multiple jurisdictions with no apparent economic or legitimate business purpose. • Trading patterns that appear designed to transfer value between accounts rather than for genuine market speculation, often resulting in consistent or deliberate losses for one party. • Unusually large deposits (especially via third-party transfers) followed by immediate requests for withdrawal to a different third-party account or a high-risk jurisdiction.
Cryptocurrency-Specific Activity	• Transactions involving anonymity-enhancing technologies such as cryptocurrency mixers, tumblers, or privacy coins (e.g., Monero) designed to break the transaction trail. • "Chain hopping": The practice of rapidly moving virtual assets across different blockchains (e.g., from Bitcoin to Ethereum to another chain) to complicate tracing efforts. • Direct or indirect interaction (i.e., within a few transaction "hops") with wallet addresses known to be associated with darknet markets, ransomware demands, sanctioned entities, scams, or other illicit activities, as identified by blockchain analytics tools. • Depositing a large volume of cryptocurrency and immediately attempting to withdraw the equivalent value in fiat currency with little to no legitimate trading activity, which can indicate layering. • The use of "peel chains," where large amounts of stolen or illicit crypto are systematically siphoned off in incrementally smaller amounts to a large number of new wallets to disperse the funds.

8.3. Internal Investigation and Reporting

Any transaction or activity that is flagged by the monitoring system or identified as potentially suspicious by a ZoraFX employee must be escalated immediately to the MLRO. The employee must provide all relevant details without alerting the client. The MLRO and their team will then conduct a thorough and confidential investigation, which involves reviewing the client's profile, past activity, and any other relevant information. The entire investigation process, including the final conclusion and the rationale behind it, will be meticulously documented.[7]

8.4. Filing Suspicious Activity Reports (SARs)

If, after investigation, the MLRO concludes that there are reasonable grounds to know, suspect, or believe that a client has engaged in or is attempting to engage in money laundering, terrorist financing, or any other financial crime, a Suspicious Activity Report (SAR) will be prepared and filed. The SAR will be submitted promptly to the relevant Financial Intelligence Unit (FIU) in accordance with applicable laws and regulations.[5]

8.5. Prohibition of "Tipping Off"

ZoraFX strictly enforces the legal prohibition against "tipping off." Under no circumstances may any employee, director, or agent of ZoraFX disclose to a client or any third party that a SAR has been filed, is being considered, or that an investigation is underway. This is a criminal offense in most major jurisdictions and is critical to protecting the integrity of law enforcement investigations.[3] Any breach of this rule will result in severe disciplinary action, including immediate termination of employment, and may be reported to the authorities.

Section 9: Specific Measures for Virtual Assets (Cryptocurrencies)

9.1. Acknowledgment of Unique Risks

ZoraFX recognizes that its offering of virtual assets (cryptocurrencies) requires a specialized set of compliance controls. Virtual assets present unique ML/TF risks due to their potential for enhanced anonymity, the speed and irrevocability of their cross-border transactions, and the decentralized nature of their networks.[13] This section outlines the specific, additional measures ZoraFX has implemented to mitigate these inherent risks, demonstrating a sophisticated understanding of the virtual asset ecosystem.

9.2. Compliance with FATF "Travel Rule" (Recommendation 16)

ZoraFX is fully committed to adhering to the principles of FATF Recommendation 16 and its Interpretive Note, commonly known as the "Travel Rule" for Virtual Asset Service Providers

(VASPs). This rule is a critical global standard for preventing the misuse of virtual assets. In line with this requirement, ZoraFX has implemented policies and procedures to:

- **Obtain and Hold:** Collect and retain required and accurate originator (our client) information and required beneficiary information for virtual asset transfers.
- **Transmit:** Submit the aforementioned information to the beneficiary VASP or financial institution during or before the transfer.

This ensures that virtual asset transfers processed by ZoraFX are not anonymous and that a clear audit trail is available for regulatory and law enforcement review, aligning our crypto operations with the transparency standards of the traditional financial system.[15]

9.3. Blockchain Analytics

To effectively police transactions on public ledgers, ZoraFX utilizes advanced blockchain analytics tools. These specialized technologies provide deep insights into the transaction history of virtual assets and allow us to conduct risk-based screening of on-chain activity. Our use of blockchain analytics includes:

- **Source and Destination of Funds Analysis:** Tracing the origin of incoming crypto deposits and the destination of outgoing withdrawals to identify exposure to high-risk sources.
- **Risk Scoring:** Assigning a risk score to client wallets and transactions based on their direct or indirect links to illicit activity.
- **Screening against High-Risk Entities:** Continuously screening transactions against a comprehensive and constantly updated database of high-risk addresses and entities, including but not limited to:
    - Sanctioned wallet addresses (e.g., those designated by OFAC).
    - Darknet marketplaces.
    - Cryptocurrency mixers and tumblers designed to obfuscate transaction trails.
    - Addresses associated with known hacks, ransomware campaigns, terrorist financing, and other documented illicit activities.[29]

Any transaction that is flagged by our blockchain analytics tools as having a connection to illicit sources will be blocked, and the activity will be escalated to the MLRO for immediate investigation and potential SAR filing.

9.4. High-Risk Virtual Asset Services

In line with our Risk-Based Approach, ZoraFX applies heightened scrutiny to activities involving services or assets that are designed to obscure transparency. The firm reserves the right to restrict, subject to Enhanced Due Diligence, or prohibit transactions involving:

- **Anonymity-Enhanced Cryptocurrencies (AECs) or "Privacy Coins":** These are virtual assets that have features designed to prevent the tracing of transactions or the identification of participants.
- **Unregulated or High-Risk VASPs:** Transfers to or from virtual asset service providers that are located in high-risk jurisdictions or are known to have weak or non-existent AML/CFT controls.
- **Mixing or Tumbling Services:** Any direct or indirect interaction with services designed to break the chain of custody of funds.

This dedicated approach to virtual asset compliance demonstrates ZoraFX's commitment to staying ahead of emerging threats and maintaining a secure trading environment for all asset classes.

Section 10: Record Keeping and Employee Training

10.1. Record Keeping Policy

Meticulous and systematic record keeping is a foundational pillar of an effective and auditable AML/CFT program. ZoraFX is committed to maintaining complete and accurate records to demonstrate compliance with all applicable regulations and to assist law enforcement investigations when required.

- **Scope of Records:** ZoraFX will securely maintain all relevant records, including:
    - All documents and data obtained through the Customer Due Diligence process, including client identification and verification information (e.g., copies of passports, utility bills) and beneficial ownership details.[48]
    - Detailed records of all client transactions, including amounts, currencies, dates, and parties involved.
    - Copies of all compliance reports submitted to senior management.
    - Copies of all internal and external Suspicious Activity Reports (SARs) filed, along with the supporting documentation and analysis that informed the decision to file.

    - Records of all AML/CFT training provided to employees, including the dates, materials covered, and lists of attendees.[49]

- **Security and Accessibility:** All records will be stored securely to protect client confidentiality and prevent unauthorized access. They will be maintained in a manner that allows for timely retrieval upon request by regulators, auditors, or law enforcement agencies.
- **Retention Period:** In a commitment to upholding the highest standards, ZoraFX will retain all required records for a minimum period of **seven years** following the termination of the client relationship or the date of the relevant transaction, whichever is later. This retention period is adopted to align with the most stringent requirements among leading international jurisdictions, exceeding the five-year minimum mandated in some regions and thereby demonstrating a more conservative and robust compliance posture.[49]

10.2. Employee Training Program

The effectiveness of any AML/CFT policy ultimately depends on the employees who implement it. ZoraFX considers a well-trained and vigilant workforce to be its first line of defense against financial crime.

- **Mandatory Participation:** All ZoraFX employees whose duties bring them into contact with clients, client transactions, or the compliance function, as well as all members of senior management, are required to participate in mandatory AML/CFT training.[51]
- **Frequency:** Training is conducted for all new employees upon hiring and is refreshed for all relevant staff on an ongoing basis, at a minimum of once per calendar year. Additional, ad-hoc training is provided whenever there is a significant change in laws, regulations, or the firm's internal policies.[53]
- **Tailored Content:** The training program is not one-size-fits-all. The content is tailored to the specific roles and responsibilities of the employees attending. For example, client-facing staff receive detailed training on KYC and red flag identification at the onboarding stage, while trading operations staff receive training focused on transactional red flags.[51]
- **Core Curriculum:** The training curriculum covers, at a minimum:
    - An overview of the applicable laws and regulations governing AML and CFT.
    - A detailed review of ZoraFX's internal AML/CFT policies and procedures.

    - The employee's specific role and personal responsibilities in combating financial crime.
    - How to identify and escalate potential suspicious activity and red flags.
    - The legal consequences of non-compliance, for both the firm and the individual employee, including the strict prohibition of "tipping off."
- **Documentation:** ZoraFX maintains comprehensive records of all training sessions conducted. These records include the training materials used, the date of the session, and a list of all attendees, providing a clear and auditable trail of our commitment to employee education.[53]

Section 11: Client Cooperation and Policy Updates

11.1. Client Obligations

As a condition of opening and maintaining an account with ZoraFX, all clients are required to cooperate fully with the firm's AML/CFT compliance efforts. This obligation includes, but is not limited to:

- Providing complete, accurate, and truthful information and documentation during the onboarding process and at any subsequent time upon request.
- Promptly notifying ZoraFX of any material changes to the information provided, such as a change of address, occupation, or corporate ownership structure.
- Responding to inquiries from ZoraFX's compliance department regarding the nature or purpose of their account activity or specific transactions.

Failure to cooperate fully may result in a delay in processing transactions, suspension of account services, or termination of the business relationship.

11.2. Right to Refuse or Terminate Service

ZoraFX reserves the absolute and unconditional right to refuse to open an account for any applicant, or to suspend or terminate an existing client relationship at any time, without providing a reason. This right will be exercised if ZoraFX, in its sole and absolute discretion, determines that:

- The client has failed to comply with the requirements of this AML/CFT policy.
- The client provides false, misleading, or suspicious information.

- The client relationship poses an unacceptable level of ML/TF risk to the firm that cannot be effectively mitigated.
- Continuing the relationship would be contrary to the firm's compliance standards or risk appetite.

This right is a critical risk management tool that allows ZoraFX to protect its integrity and comply with its legal and regulatory obligations.

11.3. Policy Review and Amendment

This AML/CFT Policy is a living document, designed to adapt to a constantly changing regulatory and risk environment. The policy and its underlying procedures will be reviewed at least annually by the MLRO and senior management. It will be updated as necessary to reflect:

- Changes in applicable laws, regulations, or international standards.
- New guidance issued by regulatory bodies like the FATF.
- The emergence of new money laundering or terrorist financing typologies.
- Changes in ZoraFX's business operations, products, or client base.

The most current version of this AML/CFT Policy will always be publicly available on the ZoraFX website, ensuring full transparency with our clients and stakeholders.