Xtream Markets

ANTI-MONEY LAUNDERING AND SANCTIONS POLICY

support@xtrememarkets.com

www.xtrememarkets.com

Table of Contents

1. INTRODUCTION & POLICY PURPOSE

1.1 **Xtream Markets LTD,** hereinafter referred to as **Xtream Markets LTD**, is dedicated to preventing its business operations, along with those of its related entities, affiliates and associates (collectively, "the Company"), from being exploited for financial crimes such as money laundering, terrorist financing, and violations of applicable sanctions laws and regulations across all jurisdictions where the Company operates.

1.2 The Company has voluntarily adopted this risk-based Anti-Money Laundering ("AML") and Sanctions Policy ("the Policy") to safeguard itself, its directors, and employees to the fullest extent possible against involvement in money laundering, terrorist financing, breaches of economic sanctions, and other financial crimes.

1.3 All actions, operations, transactions, and dealings conducted in the course of the Company's business activities adhere strictly to the ethical principles and conduct rules outlined in this Policy and the Company's AML Manual. Additionally, the Policy should be interpreted in conjunction with other pertinent policies.

2. SCOPE OF APPLICATION

2.1 This Policy applies to all directors, officers, and individuals within the Company and its subsidiaries (including related entities, affiliates, and associates1) who perform roles in representation, administration, management, or exercise management and control. It also extends to all employees and representatives of the Company (e.g., freelance consultants, suppliers, agents, distributors, representatives, brokers, etc.) (hereinafter collectively referred to as "Persons Covered by this Policy").

2.2 Persons Covered by this Policy must familiarize themselves with its provisions, and employees of Company entities are expected to actively ensure compliance. To facilitate this, the Company commits to widespread distribution of this Policy and its integration into employee training programs to enhance awareness.

2.3 All Persons Covered by this Policy are responsible for reading and comprehending its contents. Engaging in activities that contravene this Policy or any AML or sanctions requirements is strictly prohibited. Any inquiries regarding the Policy or its application to specific business areas should be directed to the Company's AML Compliance Officer (compliance@xtrememarkets.com).

3. PERSONS RESPONSIBLE FOR APPROVAL AND IMPLEMENTATION OF THIS POLICY

3.1 The Compliance Officer ("CO") is responsible for overseeing the company's adherence to the Policy.

3.2 The Policy emphasizes compliance with Anti-Money Laundering (AML) and sanctions laws and regulations imposed by the United States (the "U.S.") and the European Union (the "EU"). However, the Company must also ensure compliance with all applicable laws and regulations in every jurisdiction where it operates. The CO will develop local monitoring mech anisms, generally in consultation with local legal departments, to ensure compliance with any additional local anti-mon ey laundering requirements in each territory where the Company does business.

3.3 To accurately reflect changes in the Company's business, the Policy will be regularly reviewed and updated in response to evolving risks. Based on the changing risk profile of the Company's operations (including products, services, business lines, customers, and geographic locations), the Company will periodically conduct appropriate risk assessments. These assessments will identify potential vulnerabilities to violations of relevant statutes, guidelines, and standards, including the risk of abuse by criminals and other bad actors. The results will inform updates to the Company's overall AML and sanctions risk profiles. The CO will work with various business areas to identify high-risk areas, establish appropriate pro cedures and mitigating controls, and respond to any questions about the Policy. The risk assessment will be updated to address the root causes of any identified violations or systemic deficiencies. This assessment will consider resource allo cation to higher-risk areas and potential changes to the Policy. The CO will conduct these risk assessments at least once every three years.

3.4 The CO will undertake periodic AML and sanctions compliance reviews or audits to test and monitor the ongoing effectiveness of the Policy and its application to the Company's businesses.

3.5 The CO will ensure the proper retention of AML- and sanctions-related records, in accordance with the Company's record retention policy.

3.6 The CO will provide or arrange training for employees at least annually. Certain employees will be identified and trained by the CO to perform customer due diligence (CDD) and sanctions compliance screening for customers and counterparties (collectively, "customers") and other third parties such as agents, consultants, distributors, licensees, resellers, suppliers, and others who operate on behalf of the Company (collectively, "third parties") in compliance with the Policy. AML and sanctions compliance will be incorporated into the job descriptions and performance evaluations of employees, as appropriate.

3.7 The CO may periodically amend and recirculate the Policy with the consent of the Board of Directors. The CO will periodically report to the Audit Committee on the status of processes and procedures to prevent sanctions and money laundering-related violations.

4. LEGAL FRAMEWORK FOR MONEY LAUNDERING

4.1 The Company is committed to complying with all applicable anti-money laundering (AML) laws, regulations, conventions, and similar authorities in all jurisdictions where it operates.

Definition of Money Laundering: Money laundering generally involves acts designed to conceal or disguise the origins of proceeds derived from criminal activity, making it appear that the proceeds are from a legitimate source. These proceeds may include profits from drug trafficking, embezzlement, corruption, fraud, or other criminal offenses at the federal, state, or foreign levels. Money laundering can involve cash transactions, non-cash transactions (such as wire transfers or credit card purchases), foreign exchange transactions, and real estate transactions. It typically consists of three fundamental components: placement, layering, and integration.

- **Placement:**

At the placement stage, cash from criminal proceeds enters the financial system. This can involve depositing cash into a bank or other financial institution or converting it into negotiable monetary instruments, such as money orders or trav eler's checks. To disguise criminal activity, cash may also be routed through a "front" business, such as a check-cashing service.

- **Layering :**

AThe layering stage involves creating complex or multiple layers of transactions to break the audit trail from the illegal source, further separating the funds from their criminal origin. Funds can be transferred to other accounts, financial insti tutions, or shell companies, or disguised as proceeds from legitimate business activities. Layering may also involve trans ferring funds to countries with strict bank secrecy laws, such as the Cayman Islands, the Bahamas, and Panama. These laws, combined with the high daily volume of wire transfers, can make it difficult for law enforcement to trace these transactions. Once deposited in a foreign bank, the funds can be moved through accounts of "shell" corporations esta lished solely for money laundering purposes.

- **Integration:**

At this stage, the funds are re-introduced into the financial system and made to appear as if they were derived from le gitimate sources. This process, known as integration, allows the laundered money to be used to purchase legitimate assets or to fund other criminal activities. By understanding these components, the Company can better identify and pre vent money laundering activities, ensuring compliance with all relevant AML laws and regulations. Examples include making loan repayments, creating a new business with the laundered money, and mixing laundered money with income from other legitimate income or assets. Other examples include trade-based money laundering schemes, which involve the deposit of criminal proceeds into a U.S. or EU bank account(s) that are then transferred to a business to purchase goods, which are then shipped to foreign countries for sale, with the sale proceeds being transferred to the criminal orga nization, making the funds obtained illicitly in the U.S. or EU look as though they are legitimate.

5. LEGAL FRAMEWORK FOR SANCTIONS

a) Sanctions are typically imposed by a government or an international organization to achieve various foreign policy or national security objectives. These sanctions generally restrict an entity's or individual's ability to engage in certain com mercial activities and financial dealings with targeted entities or individuals. Sanctions measures can range from com prehensive restrictions—prohibiting trade with a target country and freezing the assets of its government, corporate en tities, and residents—to targeted asset freezes on specific entities or individuals. The Company will conduct its activities in compliance with the sanction's requirements of the U.S., EU, and any other jurisdictions as determined by the Compa ny's Compliance Officer.

b) Certain entities and individuals targeted by sanctions are identified on lists issued by the U.S., EU, United Nations, and other governments or international organizations, which are published on publicly available websites ("Sanctions Lists"). Sanctions also target certain entities and individuals not included on these Sanctions Lists, including entities owned or controlled by those on such lists.

c) Failure to comply with sanctions can lead to severe civil and criminal penalties for the business and individual employ ees, officers, and directors, as well as significant reputational damage to the Company.

d) As a rule, employees and representatives of the Company are not permitted to engage in any transactions or dealings with a party that is the target of applicable sanctions, such as those imposed by the U.S. or the EU, or any jurisdiction sub ject to comprehensive sanctions. This does not mean all transactions involving a jurisdiction targeted by any sanc tions are prohibited; some jurisdictions are subject to more nuanced sanctions where certain transactions and dealings may be permissible, although caution is warranted. The relevant sanctions programs and targets, as well as guidance on identifying and understanding the scope of these sanctions, will be specified by the Company's Compliance Officer ("Relevant Sanctions Programs"). All questions regarding the scope of coverage should be directed to the Company's Compliance Officer.

5.1 U.S. SANCTIONS (OFAC Sanctions Compliance)

The U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") administers and enforces U.S.-based economic and trade sanctions programs ("OFAC Sanctions Programs"), which are based on U.S. foreign policy and national security goals, as well as United Nations and other international mandates. OFAC publishes lists of individuals, companies, and entities, such as terrorists and narcotics traffickers, which are targets of the OFAC Sanctions Programs. These lists include the Specially Designated Nationals ("SDNs") and Blocked Persons List (the "SDN List").

a) Applicability of U.S. Sanctions:

U.S. sanctions apply to:

- U.S. companies and their overseas branches (and, for certain sanctions, non-U.S . subsidiaries of U.S. companies) in relation to their activities anywhere in the world.
- U.S. citizens and permanent resident aliens (i.e., "green card" holders) in relation to their activities anywhere in the world.
- Certain non-U.S. companies and non-U.S. nationals concerning their activities in the U.S. and any business conducted wholly or partly in the United States.

U.S. sanctions can also be applied to transactions that involve the United States, including those that utilize the U.S. financial system (e.g., dollar-denominated transactions) and those that involve U.S. companies, individuals, or U.S.-origin items.

b) Secondary Sanctions:

The United States has also implemented "secondary sanctions" that target companies and individuals engaging in specific kinds of transactions and dealings, generally in sanctioned countries such as Iran, even if the transaction or dealing does not have a direct U.S. jurisdictional nexus. These secondary sanctions aim to exclude or restrict the non-U.S. person engaging in the conduct from U.S. economic activity.

Understanding and adhering to these sanctions is crucial for ensuring compliance with U.S. and international laws and avoiding severe penalties and reputational damage.

5.2 EU SANCTIONS

a) The Council of the European Union takes decisions on the adoption of EU sanctions. The European Commission implements these decisions into EU law through proposals for regulations, which are then adopted by the Council. However, there is no central EU enforcement body; enforcement of EU sanctions is managed by individual Member States.

6. SCOPE AND APPLICATION OF EU SANCTIONS:

6.1 EU sanctions comprise a range of financial and trade measures. The main financial sanctions involve designating individuals or legal entities, leading to asset freezes and prohibitions on making funds or economic resources available to them. The EU maintains a consolidated list of individuals and entities subject to financial sanctions. Entities that are majority-owned or controlled by a listed person or entity are treated as if they are also on the list. EU trade restrictions vary by country but can include prohibitions on the import or export of a wide range of goods and technology, including luxury goods.

Applicability of EU Sanctions:

EU sanctions apply to:

- EU companies and EU nationals in relation to activities anywhere in the world, even if an EU national is employed by a non-EU company.
- Non-EU companies and non-EU nationals concerning activities in the EU and any business conducted wholly or partly within the EU.

Unlike the U.S., the EU does not impose secondary sanctions.

Understanding and complying with EU sanctions is critical for avoiding legal penalties and maintaining the Company's reputation.

7. AML AND SANCTIONS COMPLIANCE PROGRAM

The Company has voluntarily adopted this Policy to combat money laundering, terrorist financing, violations of economic sanctions, and other financial crimes (the "Program"). The elements of the Program are detailed in the following sections:

7.1 SCREENING

a) **Xtream Markets LTD** employs a robust screening process facilitated through advanced tools provided by Sum sub, leveraging the Comply Advantage database for enhanced efficacy. This screening process is conducted at 2 critical stages: prior to onboarding &. before establishing a business relationship, and on an ongoing daily basis thereafter.

b) All clients, irrespective of their risk-based level, undergo comprehensive screening. Clients are screened daily, and any matches detected are promptly reviewed and assessed by the CO. This screening continues throughout the duration of the business relationship with the client. The same rigorous screening process applies uniformly to sanctions and Politi-cally Exposed Persons (PEP) checks, ensuring compliance with regulatory standards and mitigating potential risks asso-ciated with financial crime.

7.2 EMPLOYEE AWARENESS AND TRAINING

a) All employees are responsible for reading and having access to the Policy. Upon joining the Company, all employees will receive compulsory Policy training, followed by refresher training at least annually. The Company's Compliance Officer (CO) and other employees responsible for administering Customer Due Diligence (CDD) or engaging in CDD functions will receive specialized training on the appropriate processes and tools necessary for their duties. Dates and names of at-tendees at the training sessions will be recorded, and training materials and records will be kept for the required retention period.

b) The training will cover factors that employees who handle or supervise the handling of customers, transactions, and/or funds should be aware of, particularly those that may involve suspicious activity. The training will also cover, at a mini-mum, the following:

- The employees' responsibilities under the Policy include obtaining sufficient CDD and identifying and escalating suspi cious activity to the CO.
- Red flags and signs of money laundering, terrorist financing, and other financial crimes that may arise during the course of the employee's duties.
- The identity and responsibilities of the CO.
- The potential consequences for employee non-compliance with applicable OFAC laws and regulations, including disci plinary action by the Company and civil and criminal penalties.
- The Company's record retention policy in relation to the Policy.

c) The Company, in conjunction with the CO, will review its business areas to determine if certain employees require additional or more specific training. This training will be recorded and retained in the same manner as the Company-wide Policy training. Additionally, senior management will receive high-level training and awareness designed to foster the Company's top-level commitment to complying with the Policy.

7.3 AUDIT

a) The Compliance Officer ("CO") will conduct periodic AML and sanctions compliance reviews or audits to test and monitor the ongoing effectiveness of the Program and its application within the Company. When deemed useful and appropriate, the CO will arrange for external audits performed by a third-party provider to conduct gap analyses and test the adequa-cy of the Company's controls in light of its risk profile. If such external audits are undertaken, the CO will work with the ex-ternal auditor to define the scope of the audit.

7.4 CUSTOMER DUE DILIGENCE

a) The Customer Due Diligence (CDD) process is crucial for the Company to gain comprehensive insights into parties involved in its transactions, forming an essential part of its arsenal to detect, prevent, and when necessary, report instances of money laundering, terrorist financing, and other illicit activities. coo also ensures the Company's compliance with ap-plicable AML laws and sanctions.

b) As a standard practice, the Company adopts a risk-based approach to AML and sanctions compliance. Only counterpar-ties and transactions exhibiting identified risk factors undergo further scrutiny to assess their implications for applicable AML laws or sanctions. Any uncertainties should be promptly referred to the Compliance Officer at (compliance@xtrememarkets.com).

c) Although referred to as "customer due diligence," the scope of CDD extends beyond retail customers. The Company conducts CDD on customers and transaction parties such as suppliers, distributors, wholesalers, marketing representatives, and other counterparties based on thorough risk assessments. Responsibility for identifying and independently verifying the identity of such parties, and where applicable, their owners, controlling parties, and potential connections to sanctioned jurisdictions or individuals varies according to circumstances. CO typically oversees reviews at the Company level, while local personnel handle relationships locally, guided by the CO as necessary.

d) Based on the Company's risk assessments, the CO determines appropriate screening, customer declarations, and other measures aligned with the Company's risk profile to conduct effective CDD. Enhanced due diligence is typically applied to high-risk counterparties, including Politically Exposed Persons ("PEPs"). For low-risk and standard-risk customers or infrequent retail store customers, limited due diligence may suffice, considering the transactional expectations.

e) Examples of "red flags" requiring further scrutiny include:

- A retail customer who is a PEP making unusually large purchases relative to their reported income.
- A retail customer making rapid transactions with mismatched credit card information or experiencing frequent card rejections.
- A wholesaler with distributors in sanctioned jurisdictions soliciting business from the Company.
- A supplier with suspicious identification details and incongruent business activities, such as large textile purchases and unverifiable contact information.

f) Identification and verification requirements vary across the Company's business lines, with responsibility for completing the CDD process resting with employees, third-party operators, or contracted specialists.

g) Any business transactions indicating potential AML violations or links to sanctioned entities must be promptly reported to the CO. The CO will maintain detailed records and, in consultation with external counsel as needed, determine whether to report the activity to relevant authorities or block/reject the transaction in compliance with applicable Sanctions Programs.

h) Any business transactions indicating potential AML violations or links to sanctioned entities must be promptly reported to the CO. The CO will maintain detailed records and, in consultation with external counsel as needed, determine whether to report the activity to relevant authorities or block/reject the transaction in compliance with applicable Sanctions Programs.

i) As part of the CDD process, the Company will consider including relevant contractual provisions ensuring third-party compliance with applicable AML laws and Sanctions Programs before establishing relationships with customers or third parties such as suppliers, licensors, distributors, and service providers.

j) Additionally, the Company will conduct periodic screening of its customer base to detect any associations with Sanctions Programs. Screening frequency aligns with the Company's evolving risk profile and occurs as needed, with an annual review of the entire customer base.

8. PROVISION OF CUSTOMER DUE DILIGENCE (CDD) / ULTIMATE BENEFICIAL OWNER (UBO) INFORMATION REGARDING THE COMPANY

8.1 In specific circumstances, the Company may receive requests to provide Customer Due Diligence (CDD) or Ultimate Beneficial Owner (UBO) information about itself. Financial institutions, for instance, often require this information as part of their Anti-Money Laundering (AML) and sanctions compliance protocols. To ensure consistency and proper handling of such inquiries, any request received by a member or employee of the Company should be directed to the CO. The CO will oversee the provision of necessary and relevant information on behalf of the Company, tailored to the specific requirements of the relationship in question.

9. RETENTION OF RECORDS

9.1 If a customer becomes subject to investigation by authorities for activities related to Anti-Money Laundering (AML) or sanctions compliance, the Company is obligated to maintain a clear audit trail documenting the processes conducted in accordance with its Policy. Employees within the Company's Compliance & Risk Management Function, including the CO, who are responsible for AML and sanctions compliance, must adhere to the Company's record retention policies concerning the Policy. This includes retaining all AML and sanctions-related due diligence records on customers, including their identities, transactions, and any Company reports on such customers and transactions.

9.2 Specific records to be retained include:

- Documentation obtained during the Customer Due Diligence (CDD) process, including copies of identity evidence or records indicating where such copies can be accessed.
- Records of actions taken, or reports submitted concerning the internal and external reporting of suspicious activities.
- Records pertaining to the Company's screening processes for sanctions compliance concerning its customers.
- Logs documenting the dates and subjects covered in Policy training sessions.
- Copies of any reports produced by the Company's Compliance Officer regarding exemptions from or waivers of Policy requirements.
- Other relevant books and records as mandated by the Company's record retention policies.

These records are crucial for demonstrating compliance with regulatory requirements and ensuring transparency in the Company's efforts to combat financial crime. Employees of the Company, particularly those under the supervision of the Compliance Officer, must maintain complete and accurate records throughout the duration of customer relationships and for at least five years after the relationship ends.

Specifically, all records related to matches or hits on relevant Sanctions Lists, as well as records pertaining to blocked property or rejected transactions, will be retained for a minimum of five years. In cases where property is blocked, records related to such blocked assets will be kept for five years after the property is unblocked.

Records associated with ongoing investigations or disclosed activities pending approval by authorities for disposal should also be retained until authorized for destruction. This retention period ensures compliance with regulatory standards and facilitates thorough oversight of the Company's AML and sanctions compliance efforts.

10. OBLIGATIONS OF PERSONS SUBJECT TO THIS POLICY

10.1 Persons subject to this Policy, irrespective of their location or role, and all those acting on their behalf, must adhere to the following obligations:

- Comply with all applicable AML and sanctions laws and regulations in every jurisdiction where the Company operates.
- Familiarize themselves with this Policy, ensure its distribution, provide explanations to subordinates and third parties acting on behalf of the Company, and consistently operate in accordance with its guidelines.
- Direct any uncertainties regarding potential violations of applicable AML or sanctions laws or regulations to the Company's AML Compliance Officer.
- Maintain accurate records of all transactions, including necessary transaction details and approvals, and uphold comprehensive and accurate bookkeeping.
- Perform appropriate customer due diligence and sanctions screening before entering into business partnerships with new entities or engaging third parties to act on behalf of the Company.
- Oversee and monitor business activities carried out by third parties on behalf of the Company.
- Remain vigilant for indications or evidence of suspicious transaction activities or structuring related to the Company's operations.
- Participate in mandatory compliance training sessions related to this Policy.
- Promptly report any violations or suspected violations of this Policy or any AML or sanctions laws or regulations,

11. RED FLAGS

11.1 Be vigilant for the following "Red Flags" and consult the Compliance & Risk Management Function to address any uncertainties before proceeding with the transactions or activities in question:

- Insufficient or suspicious information provided by a customer.
- Use of suspicious identification documents that cannot be readily verified.
- Reluctance of a business to provide complete information about its nature, anticipated activities, prior banking relationships, officers, directors, or business location

- Customer background not aligning with expected business activities.
- Payments made with checks, money orders, or bank drafts not drawn from the purchaser's own account.
- Use of corporate vehicles (e.g., shell companies) to obscure ownership, source of funds, or involvement of sanctioned ju risdictions.
- Use of third parties to conceal the identity of sanctioned individuals or Politically Exposed Persons (PEPs) and the origin or ownership of funds, such as in real estate transactions.
- Use of shell companies for international wire transfers involving financial institutions in jurisdictions different from their registration.
- Attempt by a customer or company to dissuade an employee from maintaining required records.
- Customer reluctance to provide information necessary for mandatory reporting, or refusal to proceed with a transaction after being informed of reporting requirements.
- Request by a business or customer to be exempted from reporting or recordkeeping requirements.
- Purchase of goods or services by a business that does not align with its stated line of business.

12. REPORTING VIOLATIONS

12.1 It is the responsibility of all individuals associated with **Xtream Markets LTD** to promptly report any suspected violations of this Policy or any anti-money laundering or sanctions laws to the Company's AML Compliance Officer. If you believe that a violation of this Policy or any anti-money laundering or sanctions laws has occurred, you must report your suspicion immediately.

12.2 **Xtream Markets LTD** ensures that no employee will face demotion, penalties, or any other adverse consequence for making a report in good faith or for following this Policy, even if such actions result in a loss of business or other adverse consequences for the company.