SANCTIONS SCREENING POLICY

PayNox EOOD

ID number: 208071994

Legal address: Bulgaria, City of Burgas, 19 Marahydyk

St., fl. 2, office 1

TABLE OF CONTENTS

INTRODUCTION AND DEFINITIONS

"PayNox" EOOD (LLC) (may also be referred to as “the Company”, “we”, or “us” in this policy) is a legal entity duly incorporated in Bulgaria that carries out activities in the field of exchange services between virtual currencies and non-gold-backed recognized currencies and is registered in The electronic public register of entities engaged in providing services for the exchange of virtual currencies and recognized currencies without gold backing, services for the transfer or exchange of virtual assets, services for the storage and management of virtual assets, enabling control over such assets, and services related to the public offering of virtual assets, as well as providers of wallets offering custodial services. The Company understands that its activity is related to virtual assets and therefore has a higher risk of money laundering due to misuse by clients. Thus, it is a primary Company’s goal to establish and follow appropriate rules to fight against these potential risks.

In line with these regulations, this policy ensures that the Company screens all business activities, transactions, and relationships to avoid involvement with individuals, companies, or entities subject to sanctions. The policy also sets out procedures for identifying and managing risks associated with sanction violations to protect the organization from potential legal and financial repercussions. Compliance with this policy is crucial for maintaining the integrity, reputation, and legal standing of the organization in the global marketplace.

This policy applies to all employees and departments, governing their actions in screening customers, suppliers, and other business partners against the relevant sanctions lists. Regular reviews and updates are essential to ensure continued compliance with evolving legal requirements.

Definitions

Sanctions: Legal measures imposed by governments or international bodies to restrict trade, finance, and other economic activities with certain individuals, organizations, or countries. Sanctions are typically imposed to promote national security, foreign policy, or human rights goals.

Sanction Lists: Lists of individuals, organizations, or countries that are subject to restrictions due to their involvement in activities that violate international law, such as terrorism, drug trafficking, or human rights abuses. Common sanction lists include those maintained by the U.S. Office of Foreign Assets Control (OFAC), the United Nations Security Council (UNSC), and the European Union (EU).

Screening: The process of reviewing and checking individuals, organizations, transactions, or business relationships against relevant sanction lists to ensure that no prohibited entities are engaged in financial or business activities with the organization.

Sanctioned Entities: Any individual, organization, or country that has been identified on a sanction list and is therefore subject to restrictions such as asset freezes, trade prohibitions, and travel bans.

Customer Due Diligence (CDD): The process of identifying and verifying the identity of customers, partners, and other relevant parties as part of a broader effort to detect and prevent money laundering and other illegal activities. CDD includes screening for sanctions compliance.

Enhanced Due Diligence (EDD): A more thorough process for assessing the risks associated with a particular customer or transaction, often required when higher risks are identified during the screening process. EDD may involve obtaining additional information to ensure compliance with sanction regulations.

Red Flags: Indicators that suggest a possible violation of sanctions laws or potential involvement with sanctioned individuals, entities, or countries. Red flags may include unusual transactions, relationships with high-risk jurisdictions, or discrepancies in documentation.

Blocking/Freezing: The act of preventing any transactions or asset transfers involving a sanctioned entity. This includes freezing funds or other assets that are subject to sanctionsï

OFAC (Office of Foreign Assets Control): A division of the U.S. Department of the Treasury responsible for administering and enforcing economic and trade sanctions against targeted foreign countries and regimes, terrorists, international narcotics traffickers, and other entities involved in activities deemed a threat to U.S. interests

Compliance Officer: The individual or team responsible for overseeing adherence to the organization's sanction screening policy, ensuring that proper procedures are followed, and managing the escalation of potential sanctions issues.

PEP (Politically Exposed Person): An individual who holds a prominent public position, such as a government official, politician, or senior executive in a state-owned company, and who may present a higher risk of involvement in corrupt activities, including sanction violations.

Prohibited Transaction: Any transaction or business relationship involving a sanctioned entity or individual that is illegal under applicable sanctions laws, such as transferring funds, selling goods, or providing services.

These definitions help clarify key terms in the policy, ensuring everyone understands the rules and expectations.

PURPOSE AND CORE PRINCIPLE OF THE POLICY

Purpose

The purpose of this Sanction Screening Policy is to ensure that Company complies with all applicable sanctions laws and regulations, thereby mitigating risks associated with engaging with sanctioned individuals, entities, or countries. These sanctions, imposed by regulatory bodies such as the United Nations (UN), the U.S. Office of Foreign Assets Control (OFAC), the European Union (EU), and other authorities, are designed to prevent financial crimes, terrorism financing, money laundering, and other illicit activities.

By implementing a robust sanction screening process, Company's aims to:

- Adhere to international and domestic sanctions laws to avoid legal penalties, fines, and reputational damage.
- Protect the organization from financial loss or reputational harm resulting from inadvertent dealings with sanctioned entities.
- Uphold corporate integrity by preventing illicit financial activities and ensuring responsible business conduct.
- Identify, assess, and mitigate risks associated with business relationships and transactions that may involve sanctioned individuals or entities.
- Safeguard the Organization: Implement effective measures to detect and prevent business engagements that could violate sanctions regulations.

This policy serves as a foundational framework for all employees, departments, and business units to ensure that sanction screening is consistently and effectively applied across all operations.

Scope

This Screening Policy applies to all aspects of the Company's operations to ensure compliance with applicable sanctions regulations. It covers all employees, departments, business relationships, and transactions, regardless of geographic location.

This Sanction Screening Policy applies to all individuals and entities associated with the Company to ensure compliance with applicable sanctions regulations. The following groups must adhere to the policy:

- All full-time, part-time, and temporary employees.
- Independent contractors, consultants, and outsourced personnel engaged in activities on behalf of the Company.

- Employees are responsible for compliance, risk management, finance, procurement, and customer relations, as they play a critical role in screening and enforcement.
- Existing and potential customers, including individuals, corporations, and financial institutions, must be screened before engagement.
- Suppliers, vendors, and service providers are involved in business transactions with the Company.
- Third-party intermediaries such as agents, brokers, and distributors act on behalf of the organization.
- Senior leadership, including executives and board members, is responsible for overseeing compliance with sanctions laws.
- The Compliance Department is tasked with implementing and monitoring screening procedures.
- The Legal and Risk Management teams are responsible for advising on sanctions-related matters and handling potential violations.
- All subsidiaries, affiliates, and joint ventures of the Company must implement and adhere to the sanction screening process.
- Joint venture partners and associated entities must undergo due diligence to ensure compliance with this policy.
- Any banks, payment processors, or financial service providers involved in transactions with the Company must ensure compliance with relevant sanctions regulations.

Responsibility for Compliance

- All employees and stakeholders covered under this policy are required to:
- Conduct due diligence and screen relevant parties before engaging in business transactions.
- Report any potential sanctions violations to the Compliance or Legal Department.
- Follow all applicable laws and internal procedures related to sanction screening.
- Failure to comply with this policy may result in disciplinary action, termination of business relationships, or legal consequences.

This Sanction Screening Policy applies to all transactions, business relationships, and operational processes that could involve sanctioned individuals, entities, or countries. The following key areas are covered under this policy:

- All financial transactions, including payments, fund transfers, and investments, must be screened to ensure compliance with applicable sanctions laws.
- Trade transactions involving the import, export, sale, or distribution of goods and services must be verified to prevent dealings with sanctioned entities.
- New and existing customers, suppliers, vendors, and other third-party partners must be screened before and during engagement.
- Third-party intermediaries such as agents, brokers, and distributors must be vetted to mitigate the risk of indirect dealings with sanctioned entities.
- Joint ventures, mergers, and acquisitions must be assessed to ensure that no sanctioned parties are involved.
- All products and services offered by the Company must comply with relevant sanctions regulations to avoid unauthorized sales or distribution.
- Certain restricted or dual-use goods and technologies that may be subject to export controls must be carefully monitored.
- Transactions and business dealings must be reviewed to ensure compliance with regional and international sanctions lists.
- Any engagement with countries subject to comprehensive sanctions (e.g., North Korea, Iran) must be carefully assessed and approved by the Compliance Department.
- Employees and business partners must be aware of travel and trade restrictions related to sanctioned jurisdictions.
- Automated sanction screening tools must be used to verify transactions, counterparties, and payments in real time.
- Online services, e-commerce platforms, and digital transactions must be monitored to prevent dealings with sanctioned entities.
- Documentation of all sanction screenings, due diligence checks, and compliance assessments must be maintained.
- Any potential sanction matches or violations must be reported to the Compliance Officer or relevant regulatory authority.

This policy ensures that the Company remains compliant with all applicable sanctions laws and mitigates financial, legal, and reputational risks.

Core Principles of the Policy

The Sanction Screening Policy is based on the following core principles to ensure compliance with international and domestic sanctions regulations, mitigate risks, and uphold ethical business practices:

1. Compliance with Laws and Regulations

- The Company is committed to complying with all applicable sanctions laws, including those imposed by the United Nations (UN), the U.S. Office of Foreign Assets Control (OFAC), the European Union (EU), and other relevant authorities.
- The organization will implement effective measures to prevent transactions or business engagements with sanctioned individuals, entities, or countries.

2. Risk-Based Approach

- A risk-based approach will be applied to sanction screening, ensuring that high-risk transactions and business relationships receive enhanced scrutiny.
- The level of due diligence will be determined based on factors such as jurisdiction, transaction type, and the nature of the business relationship.

3. Robust Screening Mechanisms

- The organization will use automated and manual screening processes to verify customers, suppliers, partners, and transactions against global sanctions lists.
- Screening will be conducted at the onboarding stage and regularly throughout the business relationship.

4. Zero Tolerance for Violations

- The Company maintains a zero-tolerance policy for sanction violations and will take immediate action against any identified breaches.
- Employees, customers, or partners found to be engaging in activities that violate sanctions regulations may face termination of relationships and legal consequences.

5. Accountability and Oversight

- Senior management, compliance teams, and all employees are responsible for ensuring adherence to this policy.
- Clear escalation and reporting procedures will be in place for suspected sanctions violations.

6. Transparency and Ethical Conduct

- The organization is committed to conducting business with integrity and transparency, avoiding any involvement in illicit financial activities.
- Employees must act in good faith and promptly report any potential compliance concerns.

7. Continuous Monitoring and Improvement

- The sanction screening process will be continuously reviewed and updated to align with regulatory changes and evolving risks.
- Regular audits and compliance training will be conducted to ensure effectiveness and awareness.

By adhering to these core principles, the Company reinforces its commitment to compliance, risk management, and ethical business practices in all operations.

SANCTION LISTS

Sources

The Sanction Screening Policy is based on regulatory guidelines, industry best practices, and international compliance frameworks. The following sources provide the foundation for the policy:

1. International and National Sanctions Regulations

- United Nations (UN) Sanctions – Enforced by the UN Security Council to maintain international peace and security.
- U.S. Office of Foreign Assets Control (OFAC) – Administers and enforces economic and trade sanctions in the U.S.
- European Union (EU) Sanctions – Restrictive measures imposed by the EU against individuals, entities, and countries.
- UK Office of Financial Sanctions Implementation (OFSI) – Responsible for implementing financial sanctions in the United Kingdom.
- Financial Action Task Force (FATF) – Sets global standards for combating money laundering and terrorist financing.
- Other National Regulatory Bodies – Includes sanction programs enforced by individual countries where the Company operates.

2. Official Sanctions Lists

- UN Consolidated List (Security Council Sanctions)
- OFAC Specially Designated Nationals (SDN) List
- EU Consolidated Sanctions List
- UK HM Treasury Sanctions List
- World Bank and International Financial Institutions Blacklists

3. Industry Guidelines and Best Practices

- Basel Committee on Banking Supervision (BCBS) – Provides international banking compliance guidelines.
- Wolfsberg Group Principles – Best practices for financial institutions on sanctions compliance and due diligence.

- International Chamber of Commerce (ICC) Guidelines – Recommendations for trade finance compliance and sanctions screening.

4. Internal Policies and Procedures

The Company's Risk Management Framework

The Company's Anti-Money Laundering (AML) Policy

The Company's Know Your Customer (KYC) Procedures

Internal guidelines for compliance, due diligence, and reporting.

These sources ensure that the Sanction Screening Policy aligns with global regulatory standards and industry best practices.

Types of sanctions

The Company must comply with global sanctions regulations and may impose various restrictions on clients who are flagged or found to be in violation of sanctions laws. The following are the key actions a crypto exchange can take against such clients:

1. Freezing or Blocking Accounts

- Wallet Freezing: Preventing clients from withdrawing, trading, or transferring funds if they are linked to sanctioned individuals or entities.
- Account Suspension: Temporarily restricting access while further investigations are conducted.
- Permanent Account Closure: Terminating the client's account if they are found to be in violation of sanctions laws.

2. Blocking Transactions

- Wallet Address Screening: Blocking transactions from or to addresses associated with sanctioned individuals or blacklisted entities.
- Preventing Fiat On/Off Ramps: Stopping clients from depositing or withdrawing fiat currency through regulated banking channels.
- Halting Crypto Transfers: Restricting the ability to send or receive cryptocurrency if a transaction is flagged as suspicious.

3. Geographic and IP Restrictions

- Geo-Blocking Access: Preventing users from sanctioned jurisdictions (e.g., North Korea, Iran) from accessing exchange services.
- VPN and Proxy Detection: Monitoring for attempts to bypass restrictions using VPNs or other obfuscation tools.
- Device and Browser Fingerprinting: Detecting suspicious login attempts from restricted locations.

4. Reporting to Authorities

- Suspicious Activity Reports (SARs): Filing reports with financial regulators or law enforcement agencies if transactions appear linked to illicit activities.
- Cooperating with Government Requests: Providing transaction records or account details if legally required by sanctions enforcement bodies (e.g., OFAC, EU regulators).

5. Enhanced Due Diligence (EDD) on High-Risk Clients

- Requesting Additional Verification: Clients flagged for potential sanctions risks may need to provide proof of identity, source of funds, or business justification.
- Ongoing Monitoring: Continually reviewing client activity for potential links to sanctioned parties.
- Restricting Access to Certain Features: Clients under review may be limited to basic services (e.g., no margin trading, withdrawals, or staking).

6. Blacklisting of Wallet Addresses

- Tagging Known Illicit Addresses: Preventing engagement with addresses previously linked to sanctions violations, darknet markets, or ransomware payments.
- Using Blockchain Analytics Tools: Monitoring transactions for links to high-risk addresses and blocking transfers when necessary.

By enforcing these sanctions measures, the Company can ensure compliance with international regulations, mitigate financial crime risks, and protect its platform from regulatory penalties.

Regular Updates

To ensure ongoing compliance with evolving regulatory frameworks and mitigate the risk of facilitating transactions with sanctioned individuals, entities, or countries, this policy mandates the regular updating of sanction screening processes. These updates will reflect changes to sanctions lists, relevant regulations, and emerging compliance best practices.

Sanction lists from international bodies, such as the United Nations, European Union, and the U.S. Office of Foreign Assets Control (OFAC), are updated frequently. The company is committed to ensuring that screening processes reflect the most current versions of these lists. Sanction screening software or manual procedures will be updated:

- On a daily basis for high-risk jurisdictions or industries.
- Weekly for less time-sensitive updates or as new designations are added.

- In the event of urgent updates, such as a new country-wide sanction or political change, immediate updates to the screening system will be applied.

Changes to the international regulatory landscape, including new sanctions, amendments to existing sanctions, or evolving enforcement practices, are continuously monitored. Any changes to the sanctions regime will be reviewed and integrated into the screening policy, ensuring that all personnel, systems, and operations comply with the latest legal standards.

Quarterly reviews will be conducted to evaluate new or modified regulations that impact the screening process.

Immediate updates will be made to the policy if significant regulatory shifts occur.

The company's screening systems and software will be regularly updated to integrate improvements in data processing, automated matching, and exception management. Updates will also address any system bugs, errors, or vulnerabilities identified during operations.

Monthly updates will be implemented for software maintenance, including fixes for system errors and the integration of enhanced matching algorithms.

Any new technological developments in the sanctions screening space will be evaluated and integrated when deemed beneficial for operational efficiency.

Regular internal audits will be conducted to assess the effectiveness and accuracy of the sanction screening process. These reviews will identify potential gaps or inefficiencies in the screening system and allow for timely corrective actions to be implemented.

Annual audits will assess overall compliance with sanctions screening requirements.

Additional audits will be conducted quarterly to ensure high-risk areas receive additional scrutiny.

Regular updates to the sanctions screening process will be accompanied by mandatory training for all relevant staff members. This training will ensure employees are familiar with the latest sanctions lists, regulatory changes, and any adjustments made to the company's screening procedures.

Bi-annual training sessions will be held to reinforce knowledge and awareness of updated sanctions, as well as the compliance protocols that align with these updates.

Special training will be offered when significant changes occur in the regulatory or sanction landscape.

Clear communication of updates will be provided to all stakeholders involved in the sanction screening process. Any procedural changes, including modifications to the list of sanctions or system updates, will be promptly communicated through internal memos or meetings.

A feedback mechanism will be maintained to capture insights from employees and stakeholders regarding the sanction screening process, allowing for continuous improvement.

All updates made to the sanctions screening process, including changes to software, lists, and internal policies, will be meticulously documented. This documentation will serve as an audit trail for compliance purposes, ensuring full accountability and transparency.

Records of updates will be stored securely for reference during audits, inspections, or regulatory reviews.

SCREENING PROCESS

Customer Due Diligence

The Customer Due Diligence (CDD) process is a critical component of the Company's Screening Policy. It ensures that the exchange complies with regulatory requirements, including Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and sanctions enforcement. The primary goal of CDD is to identify and verify the identity of customers, assess the potential risks they may pose, and prevent the exchange from being used for illicit activities such as money laundering, terrorist financing, and sanctions evasion.

As part of our commitment to compliance, all customers are required to undergo a robust Know Your Customer (KYC) process:

Customers must provide accurate personal information such as full name, date of birth, residential address, and government-issued identification (e.g., passport, national ID). This information is cross-checked with independent, reliable sources to verify the individual's identity.

For high-risk clients or transactions, additional verification may be required, including biometric verification, proof of address, and other documents that confirm the legitimacy of the individual's identity and financial activities.

As part of the CDD process, the Company conducts a comprehensive risk assessment to evaluate the potential risks that clients may pose regarding sanctions and other regulatory frameworks.

Customers are assessed based on factors such as their country of origin, political exposure (e.g., Politically Exposed Persons or PEPs), transaction history, and overall behavior on the platform. Higher-risk clients or accounts will be subjected to more stringent Enhanced Due Diligence (EDD).

A key component of the risk assessment is checking customer details against global sanctions lists (e.g., OFAC SDN List, UN Sanctions List, EU Sanctions List). This ensures that customers are not engaged in activities prohibited by international sanctions.

Customers from sanctioned or high-risk jurisdictions, such as North Korea, Iran, and others, will undergo heightened scrutiny, including geo-blocking and transaction monitoring.

To ensure ongoing compliance with sanctions regulations, the Company conducts continuous monitoring of all customer transactions:

All transactions are reviewed for suspicious activity, including those linked to known illicit addresses or high-risk countries. Blockchain analytics tools are used to track and flag transactions involving wallets associated with sanctioned individuals or entities.

If any activity suggests that a customer may be violating sanctions laws, the transaction will be flagged for further investigation. Suspicious transactions may include, but are not limited to, large and irregular transfers, rapid withdrawals, or connections to sanctioned entities.

If a customer is found to be involved in illegal activities or sanctions violations, the exchange is obligated to file a Suspicious Activity Report (SAR) with the appropriate regulatory authorities.

As part of the Sanction Screening Policy, all customers and their transactions are continuously screened against updated sanctions lists:

Customer data is cross-referenced with lists from global authorities, such as the OFAC SDN List, UN Sanctions, and EU Sanctions List, at onboarding and during ongoing monitoring.

Any individual or entity identified as being on a sanctions list will have their account blocked, and all transactions will be immediately halted. No further transactions will be processed for accounts involved with sanctioned individuals or organizations.

In addition to user profiles, cryptocurrency wallet addresses are also screened against known blacklists and flagged if they are linked to sanctioned addresses.

As part of the CDD process, Politically Exposed Persons (PEPs) are carefully identified and monitored to mitigate the risk of corruption and bribery. PEPs are individuals who hold, or have held, prominent public positions, such as heads of state, senior politicians, or high-ranking government officials.

Customers who are classified as PEPs or who have close ties to them (e.g., family members or close associates) are subject to enhanced scrutiny.

For PEPs, the exchange applies Enhanced Due Diligence (EDD) procedures, which include more thorough background checks and a deeper review of their financial activities. These individuals are monitored more closely for signs of illicit activity or violations of sanctions.

The Company maintains comprehensive records of all CDD activities to ensure compliance with sanctions laws and regulatory obligations:

All CDD documentation, including customer verification details, transaction histories, and risk assessments, is retained for the duration required by law (5 years).

Regular internal audits and external compliance reviews are conducted to ensure that the CDD process is being adhered to, and to identify any potential gaps or weaknesses in the sanction screening procedures.

By incorporating Customer Due Diligence (CDD) into the Sanction Screening Policy, the Company ensures that all clients are thoroughly vetted, and transactions are constantly monitored to comply with global sanctions regulations. This comprehensive approach to compliance helps mitigate the risk of financial crime, ensures the platform remains secure, and aligns with international standards for Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Sanctions Enforcement.

Automated Tools

To enhance the efficiency, accuracy, and compliance of sanction screening and Customer Due Diligence (CDD) processes, the Company utilizes automated tools to monitor customer activity, detect suspicious transactions, and ensure adherence to global regulatory requirements. These tools play a crucial role in mitigating risks related to money laundering, terrorist financing, and sanctions violations.

To streamline the Know Your Customer (KYC) process, the Company employs automated tools that:

Cross-check customer details (name, date of birth, address, and ID documents) against government databases and third-party verification services.

Facial recognition and liveness detection are used to ensure that documents belong to the actual individual.

AI-driven tools analyze uploaded identity documents for signs of manipulation or fraud.

Customers are classified based on risk level, with higher-risk profiles subjected to enhanced due diligence (EDD).

To prevent dealings with sanctioned individuals, entities, or jurisdictions, the Company integrates automated sanction screening tools that:

Continuously check customer names, addresses, and transaction details against real-time databases, such as:

- OFAC SDN List (U.S. Office of Foreign Assets Control)
- UN Sanctions List
- EU and UK Sanctions Lists
- Financial Action Task Force (FATF) Blacklists

Monitor cryptocurrency transactions for links to blacklisted blockchain addresses associated with illicit activities.

If a customer or transaction is flagged, the system generates alerts for compliance teams to review and act upon immediately.

Automated transaction monitoring systems help detect anomalous trading patterns and potentially suspicious activities by analyzing real-time and historical data. These tools:

Use AI and Machine Learning to track deviations from normal customer behavior.

Identify High-Risk Transactions, including:

- Large and rapid transactions across multiple accounts.
- Transfers to/from high-risk jurisdictions.
- Use of privacy coins or mixers/tumblers to obfuscate transaction history.

Generate Suspicious Activity Reports (SARs) for further investigation.

To mitigate the risks associated with Politically Exposed Persons (PEPs) and individuals with adverse media exposure, the Company uses:

- Real-time screening against global databases of public officials, their family members, and close associates.
- AI-driven tools scan news sources, regulatory reports, and dark web activity for mentions of individuals/entities linked to fraud, corruption, or financial crimes.

To streamline compliance operations, risk scoring models are used to:

Customers are scored based on multiple risk factors (location, transaction behavior, PEP status, etc.).

Higher-risk clients are subject to Enhanced Due Diligence (EDD) and manual review by compliance officers.

AI-driven tools categorize and escalate flagged cases, reducing false positives and improving response times.

Regulatory compliance requires strict record-keeping of all customer interactions, transactions, and risk assessments. Automated tools:

- Ensure Secure Storage of KYC and AML Data for regulatory audits.
- Logs all compliance actions taken in response to flagged activities.
- Automates regulatory reporting for authorities such as FinCEN, FATF, and the EU AML Authority.

Automated tools significantly enhance the efficiency, accuracy, and compliance of the Company's Sanction Screening and Customer Due Diligence (CDD) policies. By leveraging AI-driven verification, real-time monitoring, blockchain analytics, and risk-scoring systems, the Company ensures full compliance with international regulations while reducing operational burdens.

Ongoing Monitoring

Ongoing monitoring ensures continuous compliance with AML, CTF, and sanctions regulations by detecting suspicious activities, updating risk assessments, and preventing violations.

Customers are regularly rescreened against updated sanctions lists (OFAC, UN, EU, FATF).

High-risk individuals (e.g., PEPs) undergo frequent reviews.

Real-time detection of high-risk transactions, such as large transfers, cross-border payments, and privacy tool usage.

Blockchain analytics identify sanctioned wallet addresses and illicit fund movements.

Trigger-based EDD reviews for suspicious activities.

Additional identity verification and source of funds checks for high-risk users.

AI-powered tools flag unusual activity for compliance review.

Suspicious transactions generate real-time alerts and potential account restrictions.

Suspicious Activity Reports (SARs) filed with authorities.

Monitoring records are retained for 5–10 years for audits.

The platform adapts to new regulations in real-time.

Accounts violating sanctions are restricted, funds frozen, and reported.

Ongoing monitoring enhances regulatory compliance, mitigates risks, and prevents financial crime through automated screening, AI-driven monitoring, and continuous oversight.

RISK-BASED APPROACH

A risk-based approach ensures that compliance efforts are proportional to the level of risk posed by customers, transactions, and jurisdictions. By prioritizing high-risk entities, resources are allocated efficiently to mitigate sanctions violations and financial crime.

Customers are categorized as low, medium, or high risk based on factors like:

- Geographic location (sanctioned or high-risk jurisdictions).
- Transaction patterns (large or irregular transfers).
- Business type (e.g., crypto mixing services, privacy coins).

High-risk customers undergo Enhanced Due Diligence (EDD), including source of funds verification.

Stricter screening for high-risk users and transactions.

Real-time alerts for suspicious activity.

Transaction limits or restrictions applied based on risk level.

Each customer is assessed using automated tools to determine their sanctions risk exposure.

Factors include PEP status, adverse media, past violations, and transaction behaviors.

High-value, rapid, or cross-border transactions are flagged for review.

Transactions involving privacy-enhancing tools (mixers, tumblers) receive heightened scrutiny.

Countries on sanctions lists or FATF blacklists are subject to enhanced screening and restrictions.

Payments linked to high-risk regions may be blocked or require additional verification.

Machine learning assigns risk scores to customers and transactions.

Higher risk = more frequent monitoring and manual reviews.

High-risk cases are investigated manually and may lead to:

Account restrictions or enhanced scrutiny.

Suspicious Activity Reports (SARs) filed with regulators.

A risk-based approach ensures efficient compliance by focusing on high-risk activities, enabling proactive detection, and minimizing regulatory risks. Automated risk assessments help maintain security and compliance in real time.

RED FLAGS AND ESCALATION

To detect, investigate, and escalate suspicious transactions that may indicate sanctions violations, money laundering, or illicit activities. A structured escalation process ensures timely intervention and compliance with regulatory obligations.

Reluctance to Provide KYC Information or submission of forged documents.

Frequent changes in personal or business details without a valid reason.

Unusual Account Activity (e.g., multiple new accounts with minimal interaction).

Transactions involving sanctioned individuals, entities, or jurisdictions.

Large, rapid, or irregular transactions that are inconsistent with a customer's profile.

Frequent cross-border transfers to high-risk or sanctioned countries.

Use of crypto mixers, tumblers, or privacy coins to obscure fund origins.

Structuring or Smurfing—Breaking large transactions into smaller amounts to evade detection.

Transactions that lack a clear economic or business purpose.

Blockchain-Specific Red Flags

Transactions linked to blacklisted wallet addresses identified in sanctions lists.

Rapid movement of funds between multiple wallets (chain-hopping) to obscure sources.

High-volume transactions involving decentralized exchanges (DEXs) with little to no KYC.

Use of peer-to-peer (P2P) transactions to bypass compliance checks.

AI-powered monitoring tools flag potential red flags in real-time.

Compliance team conducts an initial review to assess risk.

High-risk transactions undergo EDD, including:

- Additional identity verification.
- Source of funds and wealth documentation requests.
- Deeper analysis of transaction purpose and counterparty details.

If suspicion remains, the account may be temporarily restricted (withdrawals blocked).

Transactions involving sanctioned parties are immediately halted.

If a transaction is deemed suspicious, a SAR is filed with financial regulators (e.g., FinCEN, FATF, local authorities).

Regulatory authorities are notified as required.

If confirmed as a sanctions violation, the account is permanently restricted or closed.

Funds may be frozen and reported to law enforcement for further investigation.

By using automated tools, real-time monitoring, and a structured escalation process, the Company ensures early detection and swift action against suspicious transactions and sanctions violations. This proactive approach enhances regulatory compliance, prevents financial crime, and protects the platform from illicit activity.

TRAINING AND AWARENESS

To ensure employees are well-equipped to identify, prevent, and respond to sanctions violations and suspicious transactions through regular t

New hires receive comprehensive sanctions compliance training as part of onboarding.

Annual refresher courses keep staff updated on regulatory changes, sanctions lists, and emerging risks.

Compliance and risk management staff undergo advanced training on:

- AML/CFT regulations & sanctions screening tools.
- Identifying red flags in transactions and customer behavior.
- Escalation procedures and Suspicious Activity Reporting (SARs).

Employees are trained using real-world case studies of sanctions breaches.

Simulated exercises help staff recognize and respond to potential violations.

Employees receive regular updates on sanctions list changes (OFAC, UN, EU, FATF).

Internal newsletters and alerts inform staff about new typologies of financial crime.

Periodic compliance quizzes and certification programs ensure knowledge retention.

Employees must pass annual compliance assessments to maintain access to high-risk operations.

Staff are encouraged to report potential compliance breaches through a confidential reporting system.

A zero-tolerance policy protects whistleblowers from retaliation.

Ongoing training and awareness initiatives ensure that employees understand their compliance responsibilities, remain vigilant against sanctions violations, and contribute to a robust risk management framework.

RECORDKEEPING

To ensure all sanctions screening activities, investigations, and compliance measures are properly documented, retained, and accessible for audits, regulatory reviews, and investigations.

KYC documentation, including identity verification and risk assessments.

Enhanced Due Diligence (EDD) records for high-risk customers.

Customer and transaction screening results (pass, fail, false positives).

Details of sanctions hits, reviews, and resolution actions.

Documentation of flagged transactions, investigations, and regulatory filings.

Logs of flagged high-risk transactions, including blockchain analytics.

Escalation records and compliance team actions.

Records of employee training, awareness sessions, and assessment results.

Internal compliance policies and regulatory updates.

Minimum 5 years.

Records must be securely stored and readily available for regulatory audits.

Sensitive compliance records are encrypted and access-restricted.

All compliance actions are logged with timestamps and user activity tracking.

Proper recordkeeping and documentation ensure transparency, regulatory compliance, and a strong defense against financial crime risks.

REPORTING AND COMPLIANCE

To ensure timely and accurate reporting of sanctions-related activities, suspicious transactions, and regulatory compliance measures in accordance with legal requirements.

Suspicious Activity Reports (SARs) & Suspicious Transaction Reports (STRs)

- Filed with financial regulators (e.g., FinCEN, FATF, EU authorities) when suspicious transactions are detected.

- Must include customer details, transaction history, risk assessments, and justification for suspicion.

Any confirmed transaction or account linked to a sanctioned entity is immediately reported to regulatory authorities.

Funds may be frozen pending further investigation.

Regular reports submitted to regulatory bodies to demonstrate ongoing compliance

May include audit results, risk assessments, and policy updates.

Compliance Team Responsibilities

- Monitors all transactions and ensures adherence to AML/CFT and sanctions regulations.
- Conducts internal investigations on flagged transactions.

Annual third-party audits assess the effectiveness of the sanctions compliance program.

Regulatory agencies may conduct compliance inspections to verify adherence.

Compliance officers provide regular reports to senior management on sanctions screening performance.

High-risk cases and regulatory actions are escalated to the board.

All regulatory filings and compliance reports are encrypted and stored securely.

Employees can report violations through confidential internal channels.

Effective regulatory reporting and compliance oversight strengthen risk management, ensure legal adherence, and maintain transparency in sanction screening efforts.

CONSEQUENCES FOR NON-COMPLIANCE

To enforce compliance with sanctions screening policies by outlining the consequences for violations, ensuring accountability, and mitigating regulatory risks.

Severe financial penalties for failing to comply with sanctions laws (e.g., OFAC, FATF, EU).

Potential license suspension or revocation for repeated violations.

Criminal prosecution for knowingly facilitating transactions with sanctioned entities.

Seizure of assets if funds are linked to sanctioned individuals.

Loss of customer trust and business partnerships due to compliance failures.

Increased regulatory scrutiny and restrictions on operations.

Employee Consequences

- Warnings & Re-training for minor compliance breaches.
- Suspension or termination for intentional non-compliance.
- Legal action if an employee is found complicit in sanctions violations.

Account restrictions or termination for users violating sanctions policies.

Frozen funds if linked to sanctioned individuals or illicit activities.

Reporting to authorities for suspicious transactions.

Termination of partnerships with vendors or service providers who fail to comply.

Contractual penalties for non-compliance with sanctions screening obligations.

Preventative Measures

- Regular compliance training to prevent accidental violations.
- Automated risk-based monitoring to detect and flag high-risk transactions.
- Internal audits & external reviews to ensure policy adherence.

Strict enforcement of compliance policies ensures regulatory adherence, financial security, and operational integrity. Violations result in serious legal, financial, and reputational consequences for individuals and the organization.