This Anti-Money Laundering (AML) and Know Your Customer (KYC) Policy for Wave Wallet. was approved by the Board of Directors and is effective immediately. This policy replaces and supersedes any previous AML and KYC policies or procedures implemented by the Company. It shall be reviewed and updated periodically to ensure compliance with applicable laws, regulations, and industry best practices.

# ANTI MONEY LAUNDERING ("AML")

# AND

# KNOW YOUR CLIENT (KYC) POLICY

Wave Wallet is committed to the highest standards of the Anti-Money Laundering (AML) compliance and Anti-Terrorist Financing and requires the management, and employees to follow the named standards.

## INTRODUCTION

Definitions

**AML:** Anti Money Laundering.

**CDD:** Client Due Diligence.

**Client:** A verified user.

**ECDD:** Enhanced Client Due Diligence.

**PEP:** Politically Exposed Person. A PEP is a natural person who is or has been entrusted with prominent public functions as well as their family members or close associates of such persons. Prominent public functions mean the following functions in any governmental and/or state institutions:

- heads of State, heads of government, ministers, vice-ministers or deputy ministers, secretaries of State and chancellors of parliament, government or ministry;
- members of parliament;
- members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal;
- mayors of municipalities, directors of municipal administrations;
- members of the management bodies of national supreme audit and control institutions or chairs of the boards of central banks, deputy chairs or board members;
- ambassadors, commanders of military forces and units, high-ranking officers in the armed forces of foreign states;
- members of the management or supervisory bodies of state enterprises, public limited liability companies and private limited liability companies whose shares or a part of shares carrying more than 1⁄2 of all the votes at the general meeting of shareholders of these companies are held by the right of ownership by the State;

- members of the management or supervisory bodies of municipal enterprises, public limited liability companies and private limited liability companies whose shares or a part of shares carrying more than 1⁄2 of all the votes at the general meeting of shareholders of these companies are held by the right of ownership by municipalities and which are considered to be large undertakings under the Laws on Financial Reporting;
- heads and deputy heads of international intergovernmental organizations and members of their management or supervisory bodies;
- heads and deputy heads of political parties and members of their management bodies.

**Public key:** a code of letters, numbers and/or symbols designed to identify the client and generate the client's virtual currency address.

**SCDD:** Simplified Client Due Diligence

**Threshold:** Trading limit (total volume) in USD per client.

**UBO:** Ultimate Beneficial Owner. The natural person(s) who ultimately owns or controls a legal entity and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

**User:** Any user on the Wave Wallet platform with a registered user account. Not necessarily a client.

**VASP:** Virtual Asset Service Providers.

**Virtual currency**: a digital representation of value that does not possess a legal status of currency or money, that is not issued or guaranteed by a central bank or any other public authority, is not necessarily attached to a currency, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.

**Virtual currency address**: an address/account generated from letters, numbers and/or symbols in the blockchain, by which the blockchain allocates the virtual currency to the owner or recipient.

## SCOPE

This Policy outlines the general unified procedures, guidelines and standards of internal AML control which would be adhered to by the company in order to mitigate the legal, regulatory, reputational, operational, and as a consequence financial risk.

For the avoidance of doubt, the Company conducts AML/KYC procedures through third party service providers, so the following provisions are general terms used by all the professionals in the field, but it also reserves the right to directly conduct AML/KYC verifications, on a case-by-case basis, in which case the following rules apply.

## COMPLIANCE CULTURE

Wave Wallet is committed to fostering a strong compliance culture that promotes adherence to all applicable laws, regulations, and internal policies related to anti-money laundering and counter-terrorist financing. The company's compliance culture is built on the following principles:

Top-Level Commitment: The Board of Directors and senior management demonstrate a strong commitment to AML/CFT compliance. They provide clear leadership and allocate sufficient resources to establish, implement, and maintain an effective AML/CFT program.

Tone from the Top: Senior management sets the tone from the top by communicating the importance of AML/CFT compliance to all employees and reinforcing the company's zero-tolerance policy towards money laundering, terrorist financing, and other illicit activities.

Policies and Procedures: Comprehensive AML/CFT policies and procedures are established, regularly reviewed, and updated to reflect changes in regulations, business practices, and emerging risks. These policies and procedures are effectively communicated to all relevant employees.

Employee Training and Awareness: All employees receive appropriate training on AML/CFT requirements, red flags, and reporting procedures. Training programs are tailored to the specific roles and responsibilities of employees and are conducted on an ongoing basis.

Reporting Mechanisms: Established mechanisms allow employees to report suspected AML/CFT violations or compliance issues confidentially and without fear of retaliation. Reported incidents are promptly investigated, and appropriate corrective actions are taken.

Monitoring and Oversight: The Compliance Officer, with the support of senior management, continuously monitors and oversees the implementation and effectiveness of the AML/CFT program. Regular risk assessments and audits are conducted to identify and address any deficiencies or areas for improvement.

Disciplinary Actions: Failure to comply with AML/CFT policies and procedures may result in disciplinary actions, up to and including termination of employment, in accordance with the company's disciplinary procedures.

By fostering a strong compliance culture, Wave Wallet aims to create an environment where all employees understand their roles and responsibilities in preventing and detecting money laundering and terrorist financing activities.

## COMPANY POLICY

It is the policy of Wave Wallet to fully comply with all applicable anti-money laundering and counter-terrorist financing laws and regulations in all jurisdictions where we operate. This includes, but is not limited to, adhering to the travel rule and implementing risk-based customer due diligence procedures in alignment with standards set by intergovernmental bodies like the Financial Action Task Force (FATF).

As the cryptocurrency industry continues to evolve globally, we actively monitor regulatory developments in major markets like the European Union (EU), the United States, Canada, Japan, Singapore, and Hong Kong. This allows us to proactively update our internal controls as appropriate prior to the enactment of new laws. A recent example is the EU's Markets in Crypto-Assets (MiCA) regulation, which standardizes governance for cryptocurrency service providers across Member States and emphasizes anti-money laundering obligations when it takes effect in 2024.

Wave Wallet is committed to advancing ethical practices and mitigating illicit finance risks in the cryptocurrency ecosystem. We will leverage innovative solutions like blockchain analytics where helpful to further strengthen our compliance program over time. By taking a collaborative and globally-conscious approach, we aim to facilitate sustainable cryptocurrency adoption and ensure bad actors cannot take advantage of this technology for harm.

Our AML policies, procedures and internal controls are designed to ensure compliance with all applicable regulations and rules and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

**Objectives**

The objective of the guidelines is to prevent the company from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. The Policy also enables the company to know / understand status of its Investors / users and their financial dealings better, to manage risks including reputation.

**Overview**

Wave Wallet, like most companies providing services in the crypto market, adheres to the principles of Anti-Money Laundering and actively prevents any actions that aim or facilitate the process of legalizing of illegally gained funds. AML policy means preventing the use of the company's services by criminals, with the aim of money laundering, terrorist financing or other criminal activity.

For this purpose, third-party service providers using strict policies on the detection, prevention and warning of the corresponding bodies of any suspicious activities have been contracted by the company. Hence, Wave Wallet has the right to report users and the law enforcement bodies may be informed on their activity, on a case-by-case basis. Complex electronic systems for identifying every company's user and conducting a detailed history of all operations was introduced as well by our service providers.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Terrorist financing is an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes.

The process of money laundering can be divided into three sequential stages:

Placement. At this stage funds may be converted into financial instruments, such as checks, bank accounts, and money transfers, or can be used for purchasing high-value goods that can be resold. They can also be physically deposited into banks and non-bank institutions (e.g., currency exchangers). To avoid suspicion by the company, the launderer may as well make several deposits instead of depositing the whole sum at once, this form of placement is called smurfing.

Layering. Funds are transferred or moved to other accounts and other financial instruments. It is performed to disguise the origin and disrupt the indication of the entity that made the multiple financial transactions. Moving funds around and changing in their form makes it complicated to trace the money being laundered.

Integration. Funds get back into circulation as legitimate to purchase goods and services.

In response to the scale and effect of money laundering, the United States of America and the European Union has passed Laws and Directives designed to combat money laundering and terrorism. These Acts, together with other regulations, rules and industry guidance, form the cornerstone of our AML/KYC obligations and outline the offenses and penalties for failing to comply.

Whilst Wave Wallet's business domain is currently relatively unregulated and does not fall within the scope of the AML/KYC obligations, our management has decided to avail third party services that implement systems and procedures which meet the standards set forth by the USA, European Union and other Asian jurisdictions. This decision reflects the management's desire to prevent money laundering and not be used by criminals to launder proceeds of crime.

**ANTI-MONEY LAUNDERING POLICY**

Currently, Wave Wallet is directly implementing and applying the KYC procedures and the risk-based anti-money laundering program, but will reserve the right to avail third party KYC and KYT services from third parties, in the future, in which case it will inform the community. Such measures comprise of:

- Written Anti-Money Laundering Policies
- Customer Identification Procedures
- Anti-Fraud Procedures
- Record-Keeping Requirements
- Customer Risk Assessment Procedures
- Sanction Lists Procedures
- Wave Wallet Employees Training Procedures
- On-going Customers' activity procedures

The Wave Wallet AML Policy is designed to inform the users about our commitment to preventing money laundering by meeting the worldwide standards on combating money laundering and terrorism financing, including the need to have adequate systems and controls in place to mitigate the risk of the firm being used to facilitate financial crime. This AML Policy sets out the minimum standards which must be complied with and includes:

- Establishing and maintaining a Risk-Based Approach (RBA) to the assessment and management of money laundering and terrorist financing risks faced by the firm;
- Establishing and maintaining risk-based Customer Due Diligence (CDD), identification, verification and Know Your Customer procedures, including enhanced due diligence for customers presenting a higher risk, such as Politically Exposed Persons (PEPs);
- Establishing and maintaining risk-based systems and procedures for the monitoring of on-going customer activity;
- Establishing procedures for reporting suspicious activity internally and to the relevant law enforcement authorities as appropriate;
- Maintaining appropriate records for the minimum prescribed periods;
- Providing training for and raising awareness among all relevant employees.

Before Wave Wallet starts a specific relationship with the user, the company ensures that satisfactory evidence is produced or such other measures that will produce clear evidence of the identity of any customer or counterparty are taken. The company, either directly, or through third party service providers, may apply heightened scrutiny to users who are residents of other countries, that may represent a high risk for crime and corruption and to beneficial owners who resides in and whose funds are sourced from named countries.

**APPOINTMENT OF AML/KYC OFFICER. ROLES AND RESPONSIBILITIES**

In accordance with the Anti-Money Laundering Regulations, 2008 (as amended) of the British Virgin Islands, Wave Wallet hereby appoints Mrs Lee Han as the Money Laundering Reporting Officer (MLRO) and Compliance Officer, responsible for overseeing the company's compliance with all applicable AML/CFT laws and regulations.

The AML/KYC Officer shall have the following roles and responsibilities in relation to the company's engagement:

- Act as the primary point of contact between Wave Wallet and the relevant authorities for all matters related to AML/KYC compliance.
- Ensure that the AML/KYC processes and procedures align with the company's internal policies and the applicable AML/CFT laws and regulations.
- Review and approve the risk assessment methodology and customer due diligence processes implemented by Wave Wallet.
- Oversee the integration eventually new AML/KYC solutions into the company's operations and ensure seamless collaboration between the two entities.
- Regularly review and evaluate the effectiveness of the AML/KYC services, including the accuracy and completeness of customer due diligence reports, transaction monitoring alerts, and other outputs.

- Escalate any concerns or issues related to the performance or compliance with AML/KYC requirements to the appropriate authorities within the company and, if necessary, to relevant regulatory bodies.
- Ensure that Wave Wallet provides appropriate training and guidance to the company's employees on the use of their AML/KYC solutions and the interpretation of their outputs.
- Maintain oversight and control over the company's AML/KYC compliance program.

The AML/KYC Officer shall retain overall responsibility for ensuring the company's compliance with AML/CFT laws and regulations. All employees of Wave Wallet are required to cooperate fully with the AML/KYC Officer and provide any information or documentation requested in relation to the company's AML/KYC compliance program.

**RISK ASSESSMENT**

Key facts

If there are concerns about the validity of previous verification data, it is necessary to obtain approval from the AML Officer before establishing or continuing business relationships with these clients. Trading permission should be disabled and mandatory re-verification initiated. The AML Officer decides whether to report to the competent authorities.

In the event of suspected money laundering or terrorist financing, the AML Officer must be notified immediately, and trading permission should be disabled. Client re-verification is required, and the AML Officer decides whether to report to the competent authorities.

Risks that lead to the refusal of the business relationship

The following risks automatically lead to the refusal of the business dealings, operations or transactions:

- The client is residing in a high-risk third country as defined by the FATF (high-risk and other monitored jurisdictions) and EU Regulation 2016/1675.
- The client is a PEP
- The client is a US-Person
- The UBO does not match with the (potential) client.

Risks that can lead to a higher risk level and the termination of the business relationship

The following risks lead to ECDD and can lead to the termination of the business dealings, operations or transactions and/or reporting to the competent authorities.

| **Client risks** | **Operational risks Country-based risks** | |
|---|---|---|
| • The business relationship of the client is conducted in unusual | • Payments are received from unknown or | • Payments are received from a |

| | | |
|---|---|---|
| circumstances without any apparent economic or visible lawful purpose;<br>• The client avoids submitting the information required<br>• The client avoids answering questions from Compliance Team / delays answers / does not cooperate with Compliance Team<br>• User asks for special services (non standard) | unassociated third parties;<br>• Complex transactions;<br>• Unusually large transactions;<br>• Transactions conducted in an unusual pattern;<br>• Transactions that do not have an apparent economic or lawful purpose;<br>• Transactions conducted in an unusual pattern;<br>• Transactions that do not have an apparent economic or lawful purpose; | bank account in a non SEPA country |

Operational measures when a high-risk client is detected:

1. Set high-risk level in the system if not automatically done by the system
2. Document the reason for setting the high-risk level
3. Disable trading permission of that client.
4. ECDD process

**Individual users**

Whenever necessary for the provision of any of the company's permanent or temporary services, during any required process of registration, each user may have to provide any or all of the following personal information: full name; email address; complete address, including phone number and city code; date of birth; origin. For the avoidance of doubt: Wave Wallet does not require any or all of the documents hereinafter detailed for the provision of all the services,

instead such requirements will be issued on a case-by-case basis, specifically whenever the law or the regulation applicable to any specifically provided service may require us to do so.

A user may have to send the following documents (in case the documents are written in non-Latin characters: to avoid any delays in the verification process, it is necessary to provide a notarized translation of the document in English) because of the requirements of KYC and to confirm the indicated information:

- a high-resolution copy of the first page of local or international ID or passport, where the photo and the signature are clearly seen, or a copy of driver's license with the same requirements. The indicated documents must be valid at least 6 months from the filing date.
- a high-resolution copy of a receipt of utility services payment or bank statement, containing the full user's name and the actual place of residence. These documents should not be older than 3 months from the date of filing.

**Client Due Diligence (CDD)**

If the user wants to raise his threshold and become a client, the user needs to proceed with the CDD process, which consists of the Identity Verification, Residency Verification and Financial Background Check. The CDD process must be completed successfully to raise the threshold. All automatic and manual checks by our compliance team must be successful in order to reach the client status “verified” and complete the CDD process successfully.

**Simplified Client Due Diligence (SCDD)**

Required Information

Upon registration, users go through an automated verification process where they submit:

- Full name;
- Email address.

All submitted user information is manually reviewed. For users who cannot be verified through automated means (geolocation, algorithmic face detection, sanctions list check), enhanced due diligence is requested as described below.

**Second Level Client Due Diligence**

*Government-issued ID*

Verification of identity is required by obtaining a high-resolution, non-expired copy of the user’s government-issued ID (passport, national identity card, or a driver’s license). The submitted imaged requirements include:

• Full color image. Black and white, watermarked, etc. are not accepted;

• Legible. All information on the ID must be completely clear and readable. Wave Wallet does not accept IDs that are torn or worn out; and

• Background. The edges of the ID document must be clearly visible on a contrasting background.

*Proof of residence*

Verification of residence is required by obtaining a copy of an acceptable address proof document issued in the 3 months prior to establishing an account. The document must carry the user's name and address.

A valid proof of residence document can be:

- bank statement;
- debit or credit card statement;
- utility bill (water, electricity, gas, internet, phone);
- payroll statement or official salary document from employer;
- insurance statement;
- tax document; or
- residence certificate.

Proof of residence documents must contain the user's name, address, and be dated less than 3 months ago.

*Unique photo of user*

Further verification is requested from users by submitting a unique photo of themselves holding their government-issued ID as well as a unique handwritten note. In the photo, the user must be visibly smiling. This allows Wave Wallet to easily prove that the user's picture was not stolen or photoshopped, and is being used exclusively for Wave Wallet.

The ID the user holds in their hand:

- must be the same government-issued ID the user submitted previously; and
- must be fully clear and readable.

The note the user holds in their hand:

- must be handwritten (not typed);
- must be in English;
- must contain today's date;
- must contain the user's signature.

***Verification***

Based on the risk, and to the extent reasonable and practicable, we ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures

to verify and document the accuracy of the information we get about users. Our AML Compliance Officer analyzes the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the customer.

We may decide to use the following non-documentary methods of verifying identity:

- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database or other source;
- Checking references with other financial institutions;
- Analyzing whether there is logical consistency between the identifying information provided, such as the users' name, street address, postal code, and date of birth;
- Utilizing complex device identification (such as "digital fingerprints" or IP geolocation checks); and
- Obtaining a notarized or certified true copy of an individual's birth certificate or government-issued ID for valid identification.

**Corporate users**

In case the applicant company is listed on a recognized or approved stock exchange or when there is independent evidence to show that the applicant is a wholly owned subsidiary or a subsidiary under the control of such a company, no further steps to verify identity will normally be required. In case the company is unquoted and none of the principal directors or shareholders already has an account with Wave Wallet, the official provides the following documents:

- a high-resolution copy of the certificate of incorporation/certificate;
- an extract from the Commercial Register, or equivalent document, evidencing the registration of corporate acts and amendments;
- names and addresses of all officers, directors and beneficial owners of the corporate entity;
- a high-resolution copy of Memorandum and Articles of Association or equivalent documents duly recorded with the competent registry;
- evidence of the company's registered address and the list of shareholders and directors;
- description and nature of business (including the date of commencement of the business, products or services provided; and the location of principal business).

This procedure is performed to establish the identity of the user and to help Wave Wallet know / understand the users and their financial dealings to be able to provide the best services of online trading.

**Enhanced Client Due Diligence (ECDD)**

The ECDD process is initiated if there is a suspicion of money laundering or terrorist financing or when there are doubts about the veracity or authenticity of obtained identification data of the client (which must always be the same as the UBO). Every start of a ECDD process is also called an internal investigation.

In the ECDD process, more data or information must be obtained from a reliable and independent source and requested from the client. The client has to indicate public sources which could validate the information about him, about the confirmation that he is also the beneficial owner, about his identity or other information. Additional information and clear proof from reliable and independent sources must also be obtained about the nature of the business relationship and the reasons for the intended or performed transactions, as well as about the financial background (source of funds, source of wealth).

If the user is able to resolve the uncertainties during the ECDD process, obtain approval from the AML Officer for establishing business relationships with such clients or continuing business relationships with these clients. Possible outcome:

a) If the client is not able to resolve the uncertainties, terminate the business relationship. Inform the AML Officer, who will decide on reporting to the competent authorities.

b) If the client is able to clarify the doubts and/or open issues from the Compliance Team, the trading permission must be enabled. This step must be decided together with the AML Officer.

## RISK-BASED APPROACH

Wave Wallet adopts and maintains a Risk-Based Approach ("RBA") towards assessing and containing the money laundering and terrorist financing risks arising from any transactions it has with users. The guidelines are as follows:

- Before entering into any transaction or proposed transaction, necessary checks shall be conducted in line with the RBA so as to ensure that the identity of the users does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations;
- For the purpose of risk categorization of the users, the relevant information shall be obtained from the users at or before the time of entering into a transaction;
- The risk categorization process for different types of users may take into account the background of the users, country of origin, sources of funds, volume of turnover or deposits, as well as social and financial background;
- The outcome of the risk categorization process shall be decided based on the relevant information provided by the users at the time of commencement of business relationship;
- Enhanced due diligence would be required for higher-risk users, especially those for whom the sources of funds are not clear, or for transactions of higher value and frequency, which shall be determined by Wave Wallet at its sole and absolute discretion; and
- Wave Wallet must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the Wave Wallet in compliance with the relevant legislations in place.

## MONITORING OF CLIENT ACTIVITY

In addition to gathering information from the users, Wave Wallet may have to continue to monitor the activity of every user to identify and prevent any suspicious transactions. A

suspicious transaction is known as a transaction that is inconsistent with the user's legitimate business or the usual user's transaction history known from user activity monitoring. Wave Wallet has implemented the system of monitoring the named transactions (both automatic and, if needed, manual) to prevent using the company's services by criminals.

The company reserves the right to suspend any user's operation, which can be regarded as illegal or, may be related to money laundering in the opinion of the staff.

## INTERNAL CONTROLS

Wave Wallet implements and maintains internal controls for the purpose of ensuring that all of its operations comply with AML legal requirements and that all required reports are made on a timely basis.

## MONITORING AND REPORTING

Wave Wallet may have to diligently monitor transactions for suspicious activity. Transactions that are unusual are carefully reviewed to determine if it appears that they make no apparent sense or appear to be for an unlawful purpose. When such suspicious activity is detected, the Compliance Officer will determine whether a filing with any law enforcement authority is necessary.

Suspicious activity can include more than just suspected money laundering attempts. Activity may be suspicious, and Wave Wallet may wish to make a filing with a law enforcement authority, even if no money is lost as a result of the transaction.

We will initially make the decision of whether a transaction is potentially suspicious. Once we have finished his review of the transaction details, we make the decision as to whether the transaction meets the definition of suspicious transaction or activity and whether any filings with law enforcement authorities should be made.

For the purpose of the Policies, a “Suspicious Transaction” means a transaction or attempted transaction, which to a person acting in good faith,

- gives rise to a reasonable ground of suspicion that it may involve proceeds of criminal or other illicit activity, regardless of the value involved;
- appears to be made in circumstances of unusual or unjustified complexity;
- appears to have no economic rationale or bona fide purpose; and
- gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

<u>Automatic monitoring</u>

The following rules are automatically checked by the system for every new incoming/outgoing transaction:

- Total volume of a single user is > USD 500’000.
- Monthly volume of a user is > USD 250’000.

- Full name and birth date do not appear on a Sanction + PEP list
- Transactional Irregularities:
    - A transaction over USD 20'000 after at least 3 transactions below USD 1'000.
    - 12 months no transactions, then more than 5 transactions within 30 days

A positive result on any of these automatic rule checks does not automatically lead to the disabling of the trading permission and/or termination of the business relationship. The Compliance Team and AML Officer are informed on any positive result of these checks. The AML officer decides on further actions in these cases. It can trigger ECDD measures.

All PEP Lists, Sanction Lists and Cryptocurrency Address Blacklists are downloaded once per day, all existing users are checked against all lists on a daily basis automatically. If there is any match, the specific user is automatically blocked from doing any transactions and the Compliance Team automatically receives an email with a warning. The Compliance Team then tries to clarify the situation by asking the user for proof that it is not a correct match with the Sanction List, PEP List or Cryptocurrency Address Blacklist. If the user is unable to prove it, the user remains blocked from doing any transactions. If the user made transactions before, the AML Officer has to be notified by the Compliance Team. The AML Officer decides if the reporting of the user is necessary.

Manual monitoring

*Monitoring of high-risk users:* For users that are already marked as high-risk, enhanced monitoring of the business relationships with such clients is performed by the Compliance Team. All transactions of such clients are being monitored closely and checked once per month. If there are any irregularities, the Compliance Team can contact the AML Officer, who decides on potential further action.

*Asking the user for updated identification document:* As we save the expiry date of the identity document for all clients, we ask the client to send as the updated identity document at least 30 days before the document is expired. If the user cannot provide a new document until the expiry date of the identity document, the business relationship is automatically terminated by the system.

*Monthly random basis checks:* Users and their transactions are subjected to a manual monthly plausibility check on a random basis. The data and documents submitted and the transaction history are checked. Client dossiers and the associated transactions are checked. The AML Officer must be notified of any anomalies.

The client risk profile serves as a baseline for assessing potentially suspicious activity. The AML Officer is responsible for this monitoring, reviews any activity that our monitoring system detects, determines whether any additional steps are required, documents the resulting actions in the client dossier, and reports suspicious activities to the competent authorities.

Rules

Rules which are checked in the manual checks which can – if violated – signal possible money laundering or terrorist financing include, but are not limited to:

- The client provides Wave Wallet with unusual or suspicious identification documents that cannot be readily verified or are inconsistent with other statements or documents that the client has provided. Or, the client provides information that is inconsistent with other available information about the client. This indicator may apply to account openings and to interaction subsequent to account opening.
- The client is reluctant or refuses to provide Wave Wallet with SCDD, CDD, ECDD information as required by Wave Wallet's procedures, which may include information regarding the nature and purpose of the client's business, prior financial relationships, anticipated account activity, business location and, if applicable, the entity's officers and directors.
- The client refuses to identify a legitimate source of funds or information is false, misleading or substantially incorrect.
- The client has difficulty describing the purpose of his transactions.
- The client has been rejected or has had its relationship terminated as a client by other financial services firms.
- The client's background is questionable or differs from expectations based on business activities.
- The client maintains multiple accounts, or maintains accounts in the names of family members.
- The client attempts or makes frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from Wave Wallet's policies and procedures
- The client seemingly breaks funds transfers into smaller transfers to avoid raising attention to a larger funds transfer. The smaller funds transfers do not appear to be based on payroll cycles, retirement needs, or other legitimate regular deposit and withdrawal strategies.
- The client makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
- Wire transfers are made in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Upon request, a client is unable or unwilling to produce appropriate documentation (e.g., invoices) to support a transaction, or documentation appears doctored or fake (e.g., documents contain significant discrepancies between the descriptions on the transport document or bill of lading, the invoice, or other documents such as the certificate of origin or packing list).
- A dormant account suddenly becomes active without a plausible explanation.
- Many small, incoming wire transfers or deposits are made using checks and money orders that are almost immediately withdrawn or wired out in a manner inconsistent with the client's history.

• The client exhibits unusual concern with Wave Wallet's compliance with reporting requirements and Wave Wallet's AML policies.

• The client tries to persuade an employee not to file required reports or not to maintain the required records.

• The client makes high-value transactions not commensurate with the client's known income or financial resources.

• The professional background or transactions of the client are not commensurate with the type or level of activity of the client.

• The client engages in transactions that show the client is acting on behalf of third parties with no apparent business or lawful purpose.

• The client engages in transactions that show a sudden change inconsistent with normal activities of the client.

When an employee of Wave Wallet detects any red flag, or other activity that may be suspicious, he or she will notify the AML Compliance Manager. Under the direction of the AML Officer, Wave Wallet will determine whether or not and how to further investigate the matter. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account and/or reporting to the competent authorities.

Evidence

In case of doubt, the Compliance Team will make additional inquiries to verify the accuracy of the information. The evidence listed below can be requested for this purpose.

- Annual net income
- Liquid net assets
- Net assets
- Name and address of employer
- Employment references

**PROHIBITED CUSTOMER TYPES**

Wave Wallet will not establish or maintain business relationships with certain categories of customers and entities that are associated with heightened risks of money laundering, terrorist financing, or other illicit activities. The following types of customers are prohibited from using the company's services:

- Shell Banks: Banks that do not have a physical presence in any country and are not affiliated with a regulated financial services group.
- Entities involved in illegal activities: Companies or individuals known to be involved in illegal activities such as drug trafficking, human trafficking, terrorist activities, or other criminal enterprises.
- Individuals or entities subject to sanctions: Customers listed on sanctions lists issued by the United Nations, European Union, United States (OFAC), or other relevant authorities.

- Politically Exposed Persons (PEPs): Individuals who are or have been entrusted with prominent public functions, as well as their family members and close associates, unless appropriate enhanced due diligence measures can be applied to mitigate the risks.
- Anonymous entities: Companies or legal entities that do not provide adequate information about their ownership and control structure or ultimate beneficial owners.
- Unlicensed money services businesses: Businesses engaged in money transfer services, currency exchange, or other financial services without the required licenses or registrations.
- High-risk/prohibited jurisdictions: Customers residing or companies established in jurisdictions identified as high-risk or prohibited by the Financial Action Task Force (FATF) or other relevant authorities, subject to applicable laws and regulations.

The Compliance Officer, in consultation with senior management, may add or modify the categories of prohibited customers based on changes in regulatory requirements, risk assessments, or other relevant factors. If an existing customer is subsequently identified as falling under a prohibited category, appropriate actions, including termination of the business relationship, shall be taken in accordance with the AML/KYC Policy and procedures.

**RECORD-KEEPING**

We make sure that AML records are maintained properly.

We document our verification, including all identifying information provided by a user, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We keep records containing a description of any document that we relied on to verify a user's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we retain documents that describe the methods and the results of any measures we took to verify the identity of a user.

We also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. We retain records of all identification information for seven years after the account has been closed, or as long as reasonably necessary to comply with applicable regulations; we retain records made about verification of the customer's identity for seven years after the record is made, or as long as reasonably necessary to comply with applicable regulations.

**TRAINING**

New employees may receive anti-money laundering training as part of the new-hire training program. All applicable employees are also required to complete AML training annually. Participation in additional targeted training programs is required for all employees with day-to-day AML and KYC responsibilities.

Our training will include, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties; (2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red

flags (3) what employees' roles are in Wave Wallet's compliance efforts and how to perform them; (4) Wave Wallet's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance.

Our operations are regularly reviewed to check whether certain employees require specialized additional training. Written procedures are updated to reflect any such changes.

**AML/KYC PROCEDURES**

Customer Identification and Verification:

- Identity verification through government-issued ID document checks. Wave Wallet can verify a wide range of documents from over 220 countries and territories. This includes passports, residence permits, driver's licenses, and ID cards.
- Facial biometrics and liveness detection. Wave Wallet can use facial recognition to verify a user's identity.
- Proof of address verification. Wave Wallet can verify a user's address using a variety of methods, including document verification and geolocation checks.
- Sanctions and watchlist screening.

Customer Due Diligence (CDD):

- Risk scoring and risk-based CDD procedures
- Enhanced Due Diligence (EDD) for high-risk customers
- Ongoing monitoring and periodic review of customer information

Transaction Monitoring:

- Monitoring of transactions for suspicious activity patterns
- Screening of virtual currency addresses against watchlists
- Generation of alerts and case management for further investigation

Compliance Management:

- Centralized platform for AML/KYC compliance processes
- Audit trails and record-keeping for regulatory compliance
- Reporting capabilities for suspicious activity and regulatory filings

Ongoing Support and Updates:

- Regular updates to comply with changing regulations and sanctions lists
- Technical support and integration assistance

The Wave Wallet's integrated software platform provides the following ongoing services:

- KYC/AML: Verify user IDs, addresses, and age worldwide. Perform liveness checks, video verification and ongoing AML monitoring using global watchlists, sanctions, PEPs and adverse media.

- Age verification: Protect the business and the users by verifying age. Keep minors away from prohibited content, products or services to meet regulatory requirements.
- Business verification (KYB): Get full KYB done in just 3 hours. Run automated AML and registry screening or delegate deeper ownership and control structure analysis to certified compliance experts.
- Transaction monitoring: Automatically monitor, detect and report suspicious activities in real time. Wave Wallet considers multiple factors, such as identity profile, onboarding data, transactions and account activity.
- Workflow Builder: Transform the AML policy into user-friendly verifications with a flexible Workflow Builder. Combine triggers and actions to build custom user flows that balance compliance and pass rates.
- Case management: Collaborate effectively in one dashboard. Review cases that need your attention, analyze indicators with handy visual tools, investigate suspicious activities and create reports—all in one place.

**SANCTIONS POLICY**

Wave Wallet is prohibited from transacting with individuals, companies and countries that are on prescribed sanctions lists. Wave Wallet will therefore screen against Canada, United Nations, European Union, UK Treasury and US Office of Foreign Assets Control (OFAC) sanctions lists in all jurisdictions in which will operate.