AML/KYC POLICY

WELLCash Anti-Money Laundering and Know Your Client Policy
Last updated: July 10th 2019

1. Introduction

The Company implements the principles for assessing the risks associated with the provision of payment services, categorizing clients according to their degree of risk to the Company. This categorization includes the risk definition of individual products and services provided, the riskiness of individual groups of clients with respect to risk factors.

The policy of the Company is to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements under the Money Laundering and Terrorism (Prevention) Act, Money Laundering and Terrorism (Prevention) Act Guidelines, Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Guidelines , FATF recommendations and its implementing regulations.

2. AML Compliance Person

The Company has designated its Compliance Officer (CO) as its Anti-Money Laundering Program Compliance Person (AML Compliance Person), with full responsibility for the firm's AML program. CO has a working knowledge of compliance requirements and its implementing regulations and is qualified by experience, knowledge and training. The duties of the AML Compliance Person will include monitoring the firm's compliance with AML obligations, overseeing communication and training for employees. The AML Compliance Person will also ensure that the firm keeps and maintains all of the required AML records and will ensure that Suspicious transaction reports (STR) are filed with the Financial Intelligence Unit (FIU) when appropriate. The AML Compliance Person is vested with full responsibility and authority to enforce the firm's AML program.

3. Customer Identification

One of the international standards for preventing illegal activity is customer due diligence ("CDD"). According to CDD, the Company establishes its own verification procedures within the standards of anti-money laundering and "Know Your Customer" frameworks.

The Company have adopted a risk-based approach during the customer due diligence procedures in line with the current EU AML/KYC regulations. This section regulates how we process the registration of customers accounts, what information is collected and how it is verified.

The Company identifies the customer by obtaining a range of information about him/her. The verification of the identity consists of verifying some of this information against documents or information obtained from a reliable source which is independent of the customer. At least the following information must be received for identification purposes: name and surname; personal identity number (if such exists); date of birth; photograph on an official document which confirms his/her identity; residential address; the number of the personal identification document; the expiry date of the identification document.

Once a customer is identified and his/her identity is verified, the Company must conduct a certain level of due diligence based on a risk-based approach. For some business relationships, determined by the firm to present a low degree of risk of ML/TF, simplified due diligence (SDD) may be applied; in the case of higher risk situations, and specifically in relation to PEPs, enhanced due diligence (EDD) measures must be applied on a risk-sensitive basis.

4. Risk Assessment

The Company, in line with the international requirements, has adopted a risk-based approach to combating money laundering and terrorist financing. By adopting a risk-based approach, the Company is able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the identified risks. This will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention.

5. Transaction Monitoring

The Company has an ongoing live transaction monitoring process for the purpose of detecting suspicious activity. As advised by the regulator, the Company does not rely solely on a set of prescriptive rules and thresholds; instead, it uses a risk-based approach, both in alert generation and prioritization. The solution utilizes statistical and analytical techniques to identify patterns of unusual and suspicious behaviors by building profiles on each individual customer and comparing their financial activity against expected and/or peer group norms. This is accomplished by using several powerful data analytics tools for flagging anything that falls outside of "normal."

The Company reserve the right to refuse to process a transaction at any stage. Especially, when the Company believe that a transaction is connected in any way to money laundering or any other type of criminal activity. In accordance with the EU law, the Company are not obliged to inform the customer that it was reported to the corresponding bodies of the customer's suspicious activity.

6. Reporting

The Company has established a way in which its staff consults with their line managers to provide evaluation for the rationale of the further disclosure; by no means, this prevents contacting the nominated officer directly. All internal reports are registered in an appropriate way; the nominated officer maintains a secure suspicious report register. The framework is created in such a way, where a reasonable and faithful evaluation is provided to each report that is received. The nominated officer assesses the risk that is posed by a transaction or activity. In cases where there are associated accounts, an examination of such relationships is to be carried out. If an internal review has indicated enough grounds to know or suspect that any benefit has been acquired and if a criminal property exists, an external SAR report is submitted to NCA in a timely manner.

7. Record Keeping

Records must be kept of all customers' identity, the supporting evidence of verification of identity (in each case including the original and any updated records), the Companys' business relationship with them and details of any occasional transactions. As per regulatory requirements, we keep records for at least five years from the date a business relationship ends or from the date of the last transaction.

8. Sanctions

The Company have integrated with a leading electronic data provider to fulfil the regulatory obligations in line with the EU's financial sanctions regime. Information is aggregated from the most important sanction lists (OFAC, EU, UN, BOE, FBI, Bureau of Industry and Security etc.) worldwide and is grouped into one category.

9. Training

The Company will develop ongoing employee training under the leadership of the AML Compliance Person and senior management. Our training will occur on at least an annual basis. It will be based on our firm's size, its customer base, and its resources and be updated as necessary to reflect any new developments in the law.

The Company will develop training, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures and explanatory memos. The Company will maintain records to show the persons trained, the dates of training and the subject matter of their training.

The Company will review our operations to see if certain employees, such as those in compliance, margin and corporate security, require specialized additional training. Our written procedures will be updated to reflect any such changes.

Additional training should be provided regularly to all employees based on, but not limited to, changes in government regulations, Cryptopay AML Compliance Program requirements, related procedures, and policies, or in the event of a performance issue related to an AML incident.