AML/KYC Policy

OneSecPay Anti-Money Laundering and Know Your Customer Policy (hereinafter – the “AML/KYC Policy”) is designated to prevent and mitigate possible risks of OneSecPay being involved in any kind of illegal activity.

Both international and local regulations require OneSecPay to implement effective internal procedures and mechanisms to prevent money laundering, terrorist financing, drug and human trafficking, proliferation of weapons of mass destruction, corruption and bribery and to take action in case of any form of suspicious activity from its Users.

AML/KYC Policy covers the following matters:

•Verification procedures.

•Compliance Officer.

•Monitoring Transactions.

•Risk Assessment.

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

1.1. Identity verification

OneSecPay’s identity verification procedure requires the User to provide OneSecPay with reliable, independent source documents, data or information (e.g., national ID, international passport, bank statement, utility bill). For such purposes OneSecPay reserves the right to collect User’s identification information for the AML/KYC Policy purposes.

OneSecPay will take steps to confirm the authenticity of documents and information provided by the Users. All legal methods for double-checking identification information will be used and OneSecPay reserves the right to investigate certain Users who have been determined to be risky or suspicious.

OneSecPay reserves the right to verify User’s identity in an on-going basis, especially when their identification information has been changed or their activity seemed to be suspicious (unusual for the particular User). In addition, OneSecPay reserves the right to request up-to-date documents from the Users, even though they have passed identity verification in the past.

User’s identification information will be collected, stored, shared and protected strictly in accordance with the OneSecPay’s Privacy Policy and related regulations.

Once the User’s identity has been verified, OneSecPay is able to remove itself from potential legal liability in a situation where its Services are used to conduct illegal activity.

1.2. Card verification

The Users who are intended to use payment cards in connection with the OneSecPay’s Services have to pass card verification in accordance with instructions available on the OneSecPay’s Site.

Compliance Officer

The Compliance Officer is the person, duly authorized by OneSecPay, whose duty is to ensure the effective implementation and enforcement of the AML/KYC Policy. It is the Compliance Officer’s responsibility to supervise all aspects of OneSecPay’s anti-money laundering and counter-terrorist financing, including but not limited to:

Collecting Users’ identification information. b. Establishing and updating internal policies and procedures for the completion, review, submission and retention of all reports and records required under the applicable laws and regulations. c. Monitoring transactions and investigating any significant deviations from normal activity. d. Implementing a records management system for appropriate storage and retrieval of documents, files, forms and logs. e. Updating risk assessment regularly. f. Providing law enforcement with information as required under the applicable laws and regulations.

The Compliance Officer is entitled to interact with law enforcement, which are involved in prevention of money laundering, terrorist financing and other illegal activity.

Monitoring Transactions

The Users are known not only by verifying their identity (who they are) but, more importantly, by analysing their transactional patterns (what they do). Therefore, OneSecPay relies on data analysis as a risk-assessment and suspicion detection tool. OneSecPay performs a variety of compliance-related tasks, including capturing data, filtering, record-keeping, investigation management, and reporting. System functionalities include:

1) Daily check of Users against recognized “black lists” (e.g. OFAC), aggregating transfers by multiple data points, placing Users on watch and service denial lists, opening cases for investigation where needed, sending internal communications and filling out statutory reports, if applicable;

2) Case and document management.

With regard to the AML/KYC Policy, OneSecPay will monitor all transactions and it reserves the right to:

ensure that transactions of suspicious nature are reported to the proper law enforcement through the Compliance Officer;
request the User to provide any additional information and documents in case of suspicious transactions;
suspend or terminate User’s Account when OneSecPay has reasonably suspicion that such User engaged in illegal activity.

The above list is not exhaustive and the Compliance Officer will monitor Users’ transactions on a day-to-day basis in order to define whether such transactions are to be reported and treated as suspicious or are to be treated as bona fide.

Risk Assessment

OneSecPay, 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, OneSecPay 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.

Enhanced Due Diligence Procedures for High-Risk Customers

Enhanced Due diligence is a KYC process that provides a greater level of scrutiny of potential business partnerships and highlights risk that cannot be detected by Customer Due Diligence. Risk management procedures often differentiate based on a customer’s risk profile. It starts by taking steps to ensure you know who you are dealing with, understanding their activities and assessing their risk of money laundering. Determining if a potential account requires enhanced due diligence (EDD) includes:

•Location of the business

•Occupation or nature of business

•Purpose of the business transactions

•Expected pattern of activity in terms of transaction types, dollar volume, and frequency

•Expected origination of payments and method of payment

•Articles of incorporation, partnership agreements and business certificates

•Understanding of the customer’s customers

•Identification of beneficial owners of an account or customer

•Details of other personal and business relationships the customer maintains

•Approximate salary or annual sales

•AML policies and procedures in place

•Third-party documentation

•Local market reputation through review of media sources

Some EDD practical steps include:

•Obtaining additional identifying information from a wider variety or more robust sources and using the information to inform the individual customer risk assessment.

•Carrying out additional searches (e.g., verifiable adverse media searches) to inform the individual customer risk assessment.

•Commissioning an intelligence report on the customer or beneficial owner to understand better the risk that the customer or beneficial owner may be involved in criminal activity.

•Verifying the source of funds or wealth involved in the business relationship to be satisfied that they do not constitute the proceeds from crime.

•Seeking additional information from the customer about the purpose and intended nature of the business relationship.