SecPaid Limited

AML

Anti-Money Laundering Program

Compliance Supervisory Procedures

SecPaid Limited
KANDOY HOUSE
2 FAIRVIEW STRAND,
CLONTARF WEST
DUBLIN 3,
D03 R8P3,
Ireland

Table of Content

1. Company policy....4

2. Appointment and duties of the AML Compliance Officer....4

3. Sharing AML-Information with federal authorities and financial institutions....5

3.1 National requests from counter-intelligence services....6

3.2 Summons from federal authorities, other investigative authorities....6

3.3 Voluntary exchange of information with financial institutions and payment service providers....6

3.4 Joint submission by our affiliated financial institutions of reports of suspicious transactions, companies or persons to competent authorities....7

3.5 Transmission of minutes from a subsidiary to the parent company or transmission of minutes from a parent company to the subsidiary....7

4. Comparison with the EU sanctions list or the US sanctions list....7

5. Customer identification program....8

5.1 Required customer information....8

5.2 Customers or companies that do not provide information....9

5.3 Verifying information....9

5.4 Lack of verification....10

5.5 Documentation....11

5.6 Comparison with government-provided terrorist lists....11

5.7 Reliance on another financial institution for identity verification....11

6. Duty of care towards the customer....12

6.1 Identification and verification of beneficial owners....12

6.2 Understanding the nature and purpose of customer relationships....13

6.3 Conducting continuous monitoring to identify and report suspicious transactions....13

7. Correspondent accounts for foreign Bank-Coat companies (Offshore Bank)....13

8. Due diligence obligations and extended due diligence obligations for correspondent accounts of foreign financial institutions....14

9. Due diligence and increased due diligence obligations for private bank accounts and high-ranking foreign politicians....14

10. Compliance with special measures adopted against foreign jurisdictions, financial institutions or international transactions where there is a significant risk of money laundering....14

11. Monitoring transactions for suspicious activity....14

11.1 Emergency notification to law enforcement authorities by telephone....15

11.2 Warning signs.....15
11.3 Responding to warning signals or suspicious activities.....17
12. Suspicious transactions.....17
13. AML-Recording.....18
13.1 Responsibility for required AML records and protocol or form submissions 18
14. AML training program.....19
15. Independent tests for the AML compliance program.....19
15.1 Evaluation and Reporting.....20
16. Monitoring the behavior and any user accounts of freelancers.....20
17. Confidential reporting of anti-money laundering violations.....20
18. Other risk areas.....20
19. Approval by the Senior Manager, Managing Director.....21

1. Company policy

The company's policy is to prohibit and actively prevent money laundering and all activities that facilitate money laundering or the financing of terrorist or criminal activities by complying with all applicable requirements of the EU as well as the US regulations and its implementing provisions are complied with.

Money laundering generally refers to activities aimed at concealing the true origin of criminal proceeds so that they appear to come from legitimate sources or represent legitimate assets. Money laundering generally occurs in three stages. Cash first enters the financial system in the «placement stage», where the money generated from criminal activity is converted into payment instruments such as money orders or traveller’s checks, or deposited into accounts at financial institutions. In the «layering stage», the funds are transferred or moved to other accounts or to other financial institutions to further separate the money from its criminal origins. In the «integration stage», the funds are reintroduced into the economy and used to purchase legitimate assets or to finance other criminal activities or legitimate businesses.

Although cash is rarely deposited into securities accounts, the securities industry is unique in that it can be used to launder funds acquired elsewhere and to generate illicit funds through fraudulent activities within the industry itself. Examples of types of fraudulent activities include insider trading, market manipulation, cybercrime, and other fraudulent activities related to investments.

Terrorist financing does not necessarily involve proceeds from criminal activity, but rather an attempt to conceal either the origin of the funds or their intended use, which could serve criminal purposes. Legitimate sources of funds are a key difference between terrorist financing and traditional criminal organisations. In addition to charitable donations, legitimate sources include foreign government sponsors, corporate ownership, and personal employment. Although the motivations of traditional money launderers and terrorist financiers differ, the actual methods used to finance terrorist operations may be the same or similar to the methods used by other criminals to launder money. Financing terrorist attacks does not always require large sums of money, and the transactions involved do not have to be complex.

Our AML policies, procedures and internal controls are designed to ensure compliance with all applicable EU regulations, EU laws and EBA rules. They are regularly reviewed and updated to ensure that appropriate policies, procedures and internal controls are in place to reflect both changes in regulations and changes in our business.

2. Appointment and duties of the AML Compliance Officer

The company has appointed Mr. Broennum as AML Compliance Officer, who has full responsibility for the company's AML program. Mr. Broennum has practical knowledge of anti-money laundering and its implementing regulations and is qualified by experience, knowledge and training. The duties of the AML Compliance Officer include monitoring the company's compliance with its AML obligations, monitoring communication and training of freelancer. The AML Compliance Officer also ensures that the company keeps and maintains

all required AML records and ensures that reports of suspicious activities are made when required submitted to the relevant authorities. The AML Compliance Officer has full responsibility and authority to enforce the company's AML program.

The company provides the authorities, if necessary, basically the following contact information for disposal, including:

(1) Name;
(2) Title;
(3) Mailing Address;
(4) E-Mail Address;
(5) Telephone Number und
(6) Fax, if available.

The company will correct any changes in the AML and will review and update this information as necessary within 17 business days after the end of each calendar year. The annual review will be conducted by Mr. Mücke and completed with any required updates no later than 17 business days after the end of each calendar year. In addition, Mr. Mücke will update the information promptly if changes are made, but in any event no later than 30 days after the change.

3. Sharing AML-Information with federal authorities and financial institutions

We will respond to authorities requests regarding user accounts and transactions by promptly searching our records to determine whether we maintain or have maintained a user account for, or have conducted transactions with, any named individual, entity, or organisation. We expect to have 14 days from the date the request is submitted to respond to a request, unless we are instructed to do so within a different time frame. If we find a match, we will notify the authorities that made the request and provide the required documentation. If we have searched our database and cannot find a matching account or transaction, we will notify the authority. If some parameters from the request match the data in our system, we will coordinate with the authority on how to proceed. We will keep documentation that we have conducted the required search in the form of a log that records which authority, including the appropriate authority contact person, the date of the request, the number of accounts searched, the name of the person who conducted the search, and a note of whether or not a match was found and any further action taken. We will not disclose the fact that an authority has requested or received information from us in response to a request, except to the extent necessary to fulfil the request for information. Documents related to the request will be protected and secured with the same level of care as other data held by our company, unless otherwise required by the authority making the request.

We will forward any questions we have regarding the request to the requesting authority named in the request.

Unless otherwise stated in the request, we are not obliged to treat the information request as ongoing. If periodic requests from an authority are to be made to us, then we work out a procedure with the authority that wants to make periodic requests.

3.1 National requests from counter-intelligence services

We are aware that maintaining an investigation request, an intelligence services strictly confidential. We are aware that none of our freelancers or agent may directly or indirectly communicate to any person that an intelligence service or another federal authority has requested or received access to our records. To protect the confidentiality of all requests we receive, we process and maintain no more than four (4) people processing the request. If, after receiving an investigative request, we need to involve more than four (4) people in searching our systems, the correspondence or communication will not contain any indication of the receipt or existence of such national security request. Only detailed information on the facts and circumstances of the suspicious activity detected will be corresponded and communicated. Nor will any indication or existence of such a request be noted in a protocol created for this purpose.

3.2 Summons from federal authorities, other investigative authorities

We understand that receipt of a subpoena from a federal authority or other investigative authority concerning a customer does not automatically require us to file a suspicious activity report. When we receive a subpoena, we conduct a risk assessment of the customer who is the subject of the subpoena and review the activity of the customer. If we discover suspicious activity during our risk assessment and review, we will increase the risk score of that customer, inform the EBA and the authority that need to be informed on this matter. We are aware that none of our senior Consultant, freelancer, founder of the company or Representative of the person who is the subject of the subpoena may directly or indirectly disclose its existence, its contents, or the information we used to respond to the subpoena. To maintain the confidentiality of any subpoena we receive, we process and maintain the subpoena with special care and treat them as requests under 3.1. If other people than the four (4) people who would respond to this summons need to inform other freelancers of the company about their absence from the company during the appointment or need to involve people in order to be able to have information available for the appointment, no correspondence or communication will be entered into regarding the receipt or existence of the summons. Information from the person summoned only contains detailed information about the facts and circumstances of the suspicious activity identified.

3.3 Voluntary exchange of information with financial institutions and payment service providers

We will share information about individuals, companies, organisations and countries with other financial institutions to identify and, where appropriate, report activities that we suspect may involve terrorist activities or money laundering. In order to cooperate with financial institutions, the relevant data that is important for our transaction business as a technical service provider must of course be passed on to the financial institution with which we cooperate, so that the financial institution can respond to requests from authorities if we are not asked, which depends on the country in which the financial institution is based. We will ensure that our company will prepare a protocol before transferring and the financial institution that receives the data would be, point out the special duty of care and have the AML of the receiving financial institution presented to us before passing on the data. This

process is recorded in the protocol that we produce. We understand that this requirement also applies to financial institutions with which we are affiliated and that we will obtain the necessary notifications from affiliates to ensure that our business follows all required procedures.

We will use strict procedures to ensure that only relevant information is shared and to protect the security and confidentiality of that information, for example by separating it from other company documents and records.

We will also put in place procedures to ensure that information received from another financial institution is used only for the following purposes:

- Identifying and, where appropriate, reporting money laundering or terrorist activities;
- Decision to carry out a transaction; or
- Assisting the financial institution in carrying out such activities.

3.4 Joint submission by our affiliated financial institutions of reports of suspicious transactions, companies or persons to competent authorities

In cases of suspicious activity, we will establish joint protocols with our affiliated financial institutions and payment service providers and submit a joint log of the activities to the authorities accordingly. We will also share information about a specific suspicious transaction with any financial institution or payment service provider involved in that particular transaction, as appropriate, to determine whether we should jointly maintain a log of the information that our company, financial institutions and payment service providers documented, prepared and submitted jointly.

If we decide that the joint filing of a protocol appropriate, we are aware that we require the submission of a protocol no other financial institution and payment service providers than the financial institution and payment service providers, which makes the joint submission.

3.5 Transmission of minutes from a subsidiary to the parent company or transmission of minutes from a parent company to the subsidiary

A protocol or report about potentially suspicious transactions may be passed on from a subsidiary to a parent company or from a parent company to the subsidiary for further investigation in order to confirm or refute an initial suspicion. Before we pass a protocol or report, we will enter into written confidentiality agreements or written regulations. The confidentiality agreement states that the receiving foreign parent company or the receiving foreign daughter society no protocol, no report or the fact that such as protocol or report submitted. The agreement allows the foreign parent company or the foreign subsidiary to obtain underlying information, i.e. information on the reported disclose without authorization any customers and transactions that form the basis of a record or report and that do not expressly disclose that a record or report has been filed and that are not otherwise subject to disclosure restrictions.

4. Comparison with the EU sanctions list or the US sanctions list

Before concluding a contract and on an ongoing basis, we check whether a customer is not on the sanctions list or carries out transactions that are prohibited by the economic sanctions and embargoes administered and enforced by the EU and OFAC. Since the sanction list and listings of economic sanctions and embargoes are updated frequently, we will, when updates are available, our existing ones will be replaced by the current ones. The respective list, is available to us in PDF format to ensure speed and accuracy when searching this list. If we discover that a customer is on the sanctions list or is conducting transactions prohibited by the economic sanctions and embargoes administered and enforced by the EU or OFAC, we will reject the transaction and immediately notify the authorities and companies affiliated with us.

Our review covers existing customers, new customers, customers with whom we are in contractual transactions, transactions with customers and the companies with which the customer is associated or with which the customer makes transactions for, for example, goods, services, donations or as an investment transaction.

5. Customer identification program

In addition to the information, we are required to collect under national and European laws and regulations, we have put in place a written customer identification program. We will take steps to verify the identity of each customer who wishes to enter into or has entered into a contract; we will record customer identification information and the verification methods and results; we will reasonably inform customers that we will ask for identification information to verify their identity; and we will compare customer identification information with government-provided lists of suspected terrorists once such lists are issued or updated by the government. We collect information to determine whether an entity that signs a contract with us on behalf of a company or its own company also works for the company, discloses the company's information to us so that we can audit the company and the entity is also audited by us.

For the purposes of the customer definition, the following entities are also excluded from the definition of «customer»:

- A financial institution that by a federal regulatory authority regulated or a bank regulated by a state banking regulatory authority;
- A department or agency of the EU, the United States, a state or a political subdivision of a state;
- Any corporation organised under the laws of the EU, the United States, any state, province, or political subdivision thereof that exercises governmental power on behalf of the United States, any state, province, or political subdivision thereof;

5.1 Required customer information

Before concluding a contract, where applicable, we collect the following information for each person, entity or organisation that wishes to enter into a contract with us and whose name appears on the contract:

(1) The name;

(2) Date of birth (in the case of a natural person);
(3) An address, which may be a residential or business address or a principal place of business, local office or other physical location (for a person who is not an individual); and
(4) An identification number.

This is a tax identification number for US citizens or one or more of the following numbers: a tax identification number, a passport number and the country of issue, a foreigner's identity card number or the number and country of issue of another government-issued document proving citizenship or residence that contains a photograph or similar protection.

If you wish to enter into a contract for a foreign company or organisation that does not have an identification number, we will request an alternative government-issued document confirming the existence of the company or organisation.

5.2 Customers or companies that do not provide information

If a prospective or existing client refuses to provide the information described above when requested, or if it appears that they have intentionally provided misleading information, our company will not enter into a new contract or terminate an existing contract and, after weighing the risks involved, will consider terminating all existing contracts and business relationships and their associated entities. In both cases, our AML Compliance Officer will be notified so that we can determine whether to communicate the situation in a protocol to the authority.

5.3 Verifying information

Based on the risk and where reasonable and practicable, we ensure that we have reason to believe that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we receive about our customers. Mr. Zimmermann analyses the information we receive to determine whether the information is sufficient to have reason to believe we know the customer's true identity, for example, whether the information is logical or contains inconsistencies.

We verify the customer's identity using documentary, non-documentary, or both means. We use documents to verify the customer's identity when appropriate documentation is available. Given the increasing cases of identity fraud, we supplement the use of documentary evidence with the non-documentary means described below when necessary. We may also use non-documentary means if we remain unsure whether we know the customer's true identity.

When verifying the information, we consider whether the identifying information received, such as the customer's name, address, postal code, telephone number, if provided, date of birth, allows us to establish that we have reasonable grounds to believe that we know the customer's true identity, for example, whether the information is logical or contains inconsistencies.

Suitable documents for verifying the identity of customers include:

- For an individual, an unexpired government-issued identification card that proves citizenship or residency and contains a photograph or similar security feature, such as a driver's license or passport; and
- For persons who are not private individuals, these are documents that prove the existence of the legal entity, such as a certified statute, a government-issued business license, a partnership agreement or a trust deed.

We understand that we are not obligated to take steps to determine whether the document presented to us by the customer for identity verification was validly issued and that we may rely on a government-issued ID to verify a customer's identity. However, if we determine that the document contains an obvious form of fraud, we must consider this factor in determining whether we can reasonably believe that we know the customer's true identity.

We use the following non-documentary methods to verify identity:

Checking references with other financial institutions; Obtaining a financial report; Obtaining an operating license; registration or official documents relating to a company.

We use non-documentary verification methods when:

(1) The customer is unable to present a valid government-issued photo ID or an equivalent ID card with proof of identity;
(2) The company is not familiar with the documents submitted by the customer for identity verification;
(3) There is no personal contact between customer and company; and
(4) There are other circumstances that increase the risk that the company will not be able to verify the customer's true identity using documents.

We will provide the information within a reasonable time before or after conclusion of the contract depending on the type of contract and the requested transactions, we may refuse to carry out a transaction before we have verified the information, or in some cases, if we need more time, we may not be able to carry out the type of transactions until verification, limit the transactions. If we find suspicious information indicating possible money laundering, terrorist financing or other suspicious activities, we will file a report in accordance with applicable laws and regulations after internal consultation with the company's AML Compliance Officer.

We are aware that the risk of not knowing the true identity of a customer may be significant in certain transaction species can be increased, for example in transactions opened in the name of a corporation, partnership or trust that is incorporated in or carries on substantial business in a jurisdiction, from the EU or the United States has been identified as a priority money laundering area, a terrorist risk area, or a non-cooperative country or territory. We will identify customers who are at increased risk of not being properly identified. We will also take additional measures that may be used to obtain information about the identity of persons connected with the customer. If the identity cannot be clearly established despite appropriate efforts, we will coordinate the further procedure with our AML Compliance Officers, whether the business relationship should be terminated and a report submitted to the authority or whether we submit a report to the authority.

5.4 Lack of verification

If we cannot reasonably be expected to know the true identity of a customer, we will do the following:

(1) Wed do not enter into a business relationship;
(2) We establish conditions under which a customer may conduct transactions while we attempt to verify the customer's identity;
(3) Immediately break off all business relations if attempts to verify a customer's identity have failed; and
(4) We check whether it is necessary to prepare a protocol that we submit to the competent authority, in accordance with applicable laws and regulations.

5.5 Documentation

We document our verification, including any identification information provided by a customer, the methods used and results of the verification, and the resolution of any discrepancies identified in the verification process. We maintain records describing all documents we relied on to verify a customer's identity, noting the type of document, the identification number contained in the document, the place of issue, and, if applicable, the date of issue and expiration date. With respect to non-documentary verification, we maintain documents describing the methods and results of any actions we took to verify a customer's identity. We also maintain records describing the resolution of any material discrepancies identified in verifying the identification information received. We maintain records of all identification information for five years after the termination of a business relationship; we maintain records of customer identity verification for five years after the record was created.

5.6 Comparison with government-provided terrorist lists

Once we receive notification that a federal authority has issued a list of known or suspected terrorists and that list to identify provides and we will, within a reasonable period of time after conclusion of a contract with a customer or sooner if required by another federal law or regulation or a federal directive issued in connection with an applicable list, determine whether a customer is on any such list of known or suspected terrorists or terrorist organizations issued by a federal agency and designated as such by the Secretary of the Treasury in consultation with federal regulators. We will comply with any federal directives issued in connection with such lists.

We will continue to separately sanction rules and laws of the EU and the United States that prohibit transactions with certain foreign countries or their nationals.

To assist the government in combating terrorist financing and money laundering, federal law requires all financial institutions, monetary institutions, payment service providers, technical service providers to collect, verify, and record identifying information for each person who opens an account or enters into a contract with a business to receive transactions.

5.7 Reliance on another financial institution for identity verification

We may rely on another financial institution, including an affiliate, to complete some or all of our customer identification program in respect of any customer who has opened an account

or established an account or similar business relationship with a financial institution to provide or conduct services, business or other financial transactions in the following circumstances:

- If such reliance is reasonable in the circumstances;
- If the other financial institution is subject to a regulation implementing the requirements of the anti-money laundering compliance program and is supervised by a federal regulatory authority; and
- If the other financial institution has entered into a contract with our company that requires it to certify to us annually that it has implemented its anti-money laundering program and that it or its agent will comply with certain requirements of the customer identification program.

6. Duty of care towards the customer

In order for our company to exercise appropriate due diligence towards its customers, we list the four components of customer due diligence here:

(1) Customer identification and verification;
(2) Identification and verification of the beneficial owner;
(3) Understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and
(4) Conducting ongoing monitoring to identify and report suspicious transactions and maintaining and updating customer information on a risk basis. Since the first component is already a requirement of the AML program, pursuant to our Customer Identification Program, customer due diligence focuses on the other three components.

According to our rules, section six (6), member companies must obtain from the natural person who concludes contracts with our company on behalf of the legal client the identity of the beneficial owners of the company. In addition, this person must confirm to the best of his knowledge and belief that the information is correct.

In addition to the steps required under the written customer identification program, we have established procedures that are reasonably designed to identify and verify beneficial owners of legal entities as customers. We will implement certain minimum. We will collect information from beneficial owners of legal entities as customers. We will understand the nature and purpose of customer relationships to develop a customer risk profile. We will conduct continuous monitoring to identify and report suspicious transactions and maintain and update customer information on a risk basis.

6.1 Identification and verification of beneficial owners

At the latest after the conclusion of the contract, or should we decide to do it earlier on an individual basis, Mr. Zimmermann identifies all persons who are beneficial owners of the legal customer by identifying all persons who directly or indirectly own 25% or more of the legal customer's equity shares, as well as all persons who have significant responsibility for

the control, administration or management of a legal customer. The following information is recorded for each beneficial owner:

(1) The name;
(2) Date of birth (in the case of a natural person);
(3) An address that is a residential or business address for an individual.
(4) An identification number. This may be a Social Security number for US citizens, one or more of the following: a passport number and country of issue, or a similar identification number, such as a foreigner's identification card number or the number and country of issue of another government-issued document evidencing citizenship or residency that contains a photograph or similar security feature for non-US citizens.

If we receive copies of an ID card or other documents that must be used for identification and are submitted to us, we will store these with the customer data and take measures to prevent third-party access. We will also describe all non-documentary methods and the results of any measures taken.

6.2 Understanding the nature and purpose of customer relationships

We will understand the nature and purpose of customer relationships to develop a customer risk profile.

Depending on the facts and circumstances, a customer risk profile may contain the following information:

- The type of customer;
- The goods or services offered by the customer;
- The service offered from us to the customer;
- The transaction volume of the customer;
- The number of transactions of the customer;
- The residential or business customer's place of business;
- The main occupation or business of the customer; and
- For existing customers, the customer’s activity history.

6.3 Conducting continuous monitoring to identify and report suspicious transactions

We conduct continuous monitoring to identify and report suspicious transactions. In order to detect suspicious transactions, we use the customer risk profile as the basis against which customer activity is assessed for reporting suspicious transactions. Our procedures for monitoring suspicious activity are described in detail in Section 11, Monitoring Accounts for Suspicious Activity.

However, we are not expected to update customer information, including beneficial owner information, on an ongoing or continuous basis

7. Correspondent accounts for foreign Bank-Coat companies (Offshore Bank)

As a technical service provider, our company does not offer accounts in the usual sense that are comparable to accounts of a money, credit, bank or financial institution. Nor will our company maintain business relationships or conclude contracts with any credit institution that holds a banking licence in its country of domicile but does not operate there and does not belong to a financial services group that is subject to effective banking supervision. If we only identify such shell banks after a contract has been concluded, we immediately terminate the contracts, prepare a report and inform the authorities.

We only offer technical services, transactions via API interfaces for companies. The user account associated with this service, which we set up for our customers, is only to be able to clearly assign the transactions to the customer and by whom and for what a transaction was made in favour of our customer.

No correspondent accounts are managed or offered by our company.

If a shell bank or an employee of such a bank uses our technical service despite all precautions to combat money laundering, we will immediately inform a federal authority and terminate all business relations with the person or such a company.

8. Due diligence obligations and extended due diligence obligations for correspondent accounts of foreign financial institutions

As described under section seven (7), our company is a technical service provider.

As a technical service provider, a banking license is not required and we have no plans to operate as a bank at the moment. Should this happen in the future due to legal developments, we will apply for a banking licence and then bring the AML into line with the law.

Our company does not maintain correspondent accounts.

We do not have any correspondent accounts and do not intend to open or maintain any and are not permitted to do so by law.

9. Due diligence and increased due diligence obligations for private bank accounts and high-ranking foreign politicians

As under section seven (7) and section eight (8) as described, our company is a technical service provider.

We do not open or maintain private bank accounts, as we are not permitted to open or maintain accounts in the sense of bank accounts, including correspondent accounts, without a banking licence.

10. Compliance with special measures adopted against foreign jurisdictions, financial institutions or international transactions where there is a significant risk of money laundering

As under section seven (7), section eight (8) and section nine (9) described, our company is a technical service provider.

We do not open or maintain private bank accounts, business accounts, as we are not permitted to open or maintain accounts in the sense of bank accounts, including correspondent accounts, without a banking licence.

If a final regulation is issued with respect to transactions conducted by technical service providers, we will read it and comply with all rules and prohibitions contained therein.

11. Monitoring transactions for suspicious activity

We monitor the transaction for unusual size, volume, pattern or type of transactions, taking into account risk factors and warning signals relevant to our business. For this purpose, an automatically created document is generated by our system for each of our customers' user accounts for incoming transactions for a customer, which is then examined by the AML Compliance Officer or their representative. The document contains all transactions that have been verified for the respective customer by a payer, their selected payment service provider and by stripe.com, which is a payment service provider, in accordance with the requirements of the United States of America.

In addition, automatic fraud prevention is provided by our partner stripe.com.

The AML Compliance Officer or their representative, shall conduct an appropriate investigation and review relevant information from internal or external sources before a report is issued and submitted to the competent authority.

Internal sources here are the documents that our system creates and external sources are the anti-fraud radar of stripe.com.

Monitoring takes place at least once a day.

11.1 Emergency notification to law enforcement authorities by telephone

In situations where violations occur that require immediate attention, such as terrorist financing or ongoing money laundering schemes, we will immediately refer the matter to an appropriate law enforcement agency.

If a customer or company appears on the most current sanctions list available to us, we will immediately contact the relevant authority. We will always keep a record of our actions.

We are aware that, even if we reported it by telephone, we must report it in writing to the competent authority with all the necessary records.

11.2 Warning signs

Warning signs that indicate possible money laundering or terrorist financing include:

- The customer provides the company with unusual or suspicious identification documents that cannot be readily verified or that conflict with other statements or documents provided by the customer. Or the customer provides information that conflicts with other available information about the customer.
- The customer is unwilling or refuses to provide the company with full customer due diligence information as required by the company’s procedures. This may include

information about the nature and purpose of the customer's business, previous financial relationships, anticipated activities, place of business and, where applicable, the officers and directors of the company.

- The customer refuses to provide legitimate bank details or the information is false, misleading or materially inaccurate.
- The customer is resident in a jurisdiction that is considered a banking secrecy haven, a tax haven, a high-risk geographical location, e.g. a known drug producing state, a known anti-money laundering or anti-terrorist financing system, or a conflict area, including those with a proven terrorist threat, or conducts business there or regularly conducts transactions with counter parties.
- The customer has difficulty describing the nature of his business or lacks general knowledge of his industry.
- There is no discernible reason for the customer to use the company's services or location, for example because the customer is not rooted in the local community or has made a special effort to use the company
- The customer appears to be acting as a representative of an unnamed client, but is unwilling to disclose any information.
- The client is a trust, shell company or private investment company that does not wish to disclose information about controlling interests and underlying beneficiaries.
- It is publicly known or the company is aware that the customer is the subject of criminal, civil or regulatory proceedings for crime, corruption or misuse of public funds, or that the customer is associated with such persons. Sources for this information may include news, the internet or commercial database research.
- The customer's background is questionable or deviates from expectations based on the business activity.
- The customer maintains several user accounts or leads user accounts on behalf of family members or companies without any apparent commercial or other purpose.
- A contract is run by a non-profit organisation with us that provides services in geographic areas known to have a higher risk of an active terrorist threat.
- A contract is made on behalf of a legal entity concluded with us, who is involved in the activities of an association, organisation or foundation whose objectives are related to the claims or demands of a known terrorist organisation.
- Transactions are apparently made in small amounts in order to circumvent identification and reporting requirements.
- Transactions are made from or to financial havens, tax havens, high-risk geographical locations or conflict areas, including those with a proven terrorist presence.
- The parties involved in the transaction, e.g. the principal or beneficiary, come from countries known to support terrorist activities and organisations.
- Transactions are made to a beneficiary which do not reveal the name or account number of the payer.
- There are unexplained, recurring or unusually high transactions that exhibit unusual patterns or have no discernible commercial purpose.
- A customer is unable or unwilling to provide appropriate documentation to support a transaction when requested, or the documentation appears to be forged.

- Nonprofit or charitable organisations engage in transactions for which there is no apparent logical commercial purpose or where there appears to be no connection between the organisation's stated activities and the other parties involved in the transaction.
- When looking at transactions over a certain period of time, suspicious or unusual patterns can be recognised, for example circular payments, repetitive transactions or cumbersome money movements.
- The customer is unwilling to provide the information necessary to submit reports and complete the transaction.
- The customer expresses unusual concern regarding the company's compliance with regulatory reporting requirements and anti-money laundering policies.
- The customer attempts to persuade a freelancer not to submit required reports or keep required records.
- Law enforcement authorities have issued subpoenas or suspension orders regarding a customer.
- The customer makes high-value transactions that are disproportionate to his known income or financial means.
- The customer wants to conduct transactions that have no business sense or are contrary to the customer's stated business.
- The customer carries out transactions which indicate that he is acting on behalf of third parties without any apparent commercial or legitimate purpose.
- The customer conducts transactions that involve a sudden change that is inconsistent with the customer's normal activities.

11.3 Responding to warning signals or suspicious activities

If a company freelancer detects a red flag or other suspicious activity, he or she will notify the AML Compliance Officer. Under the direction of the AML Compliance Officer, the company will decide whether and how to investigate the matter further. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the user's account, and/or submitting a report to the appropriate authority.

12. Suspicious transactions

Our company's procedures for identifying suspicious transactions and determining whether further investigation is necessary or whether it is necessary to notify a competent authority through a report prepared by us.

Our company will need to exercise due diligence in monitoring suspicious activity, as regulations require companies to file a report with the relevant authority if they «know, suspect or have reason to believe» that transactions involve certain suspicious activity.

We will prepare and file records of all transactions conducted or attempted to be conducted through our company involving transactions of EUR 5,000 or more, either individually or in the aggregate, where we know, suspect or have reason to believe:

(1) the transaction involves funds derived from an illegal activity, or is intended or conducted for the purpose of concealing or disguising funds or assets derived from

an illegal activity as part of a plan to violate or circumvent any Federal law or regulation, or to evade any transaction reporting requirement under any Federal law or regulation;

(2) the transaction is designed to meet, through structuring or otherwise, the requirements of laws and to circumvent regulations;

(3) the transaction does not pursue a commercial or obviously legitimate purpose or is not of the type that the customer would normally carry out and we do not see a reasonable explanation for the transaction after examining the background of the possible purpose of the transaction and other facts; or

(4) the transaction involves the use of the company to facilitate criminal activities.

We will also file a report and inform the relevant law enforcement agency in cases involving violations that require immediate attention, such as terrorist financing or ongoing, if identifiable to us, money laundering schemes.

We may file a voluntary report for any suspicious transaction that we believe is relevant to a possible violation of a law or regulation, but that we are not required to report under the laws and regulations.

It is our policy to report all minutes prepared on a regular basis to the Board of Directors and the relevant senior management, with a clear indication that the confidentiality of the minutes must be maintained.

We report suspicious transactions by preparing a report or completing a form with the appropriate authority and we collect and retain supporting documentation as required by regulations. We will submit a report or completed form no later than 30 calendar days after the date of first discovery of the facts that provide a basis for filing a report or completing a form. If no suspect is identified on the date of first discovery, we may delay filing a report or completing a form with the appropriate authority for an additional 30 calendar days until a suspect is identified; however, in no event shall reporting be delayed more than 60 calendar days after the date of initial discovery. The «initial discovery» stamp or notation does not indicate the moment a transaction is highlighted for review. The 30-day or 60-day period begins when an appropriate review is conducted and the transaction under review is determined to be «suspicious» within the meaning of the legal requirements. A review must be initiated promptly upon identification of unusual activity that warrants an investigation.

We will retain copies of all submitted records and the original or business record equivalent of all supporting documents for five years from the date the record is submitted. We will identify and retain supporting documents and make this information available upon request from, for example, the FIU, other appropriate federal or state law enforcement agencies. We will not inform any person involved in the transaction that the transaction has been reported, unless permitted by laws and regulations.

13. AML-Recording

Our company has procedures in place to securely store all relevant records and reviews of the AML program.

13.1 Responsibility for required AML records and protocol or form submissions

Our AML Compliance Officer and those appointed by them are responsible for ensuring that AML records are properly maintained and protocols or forms are submitted as required.

In addition, as part of our AML program, our company creates and maintains all logs, forms, relevant documentation relating to customer identity and verification (see section 5 above) and transactions. We retain logs and related documentation for at least five years. We retain other documents in accordance with existing regulations, laws and other retention obligations, unless we are required to maintain a different retention obligation. We keep logs and all supporting documentation confidential. We do not inform anyone outside of the relevant Financial Intelligence Units or any other relevant law enforcement or regulatory authority about a log. We do not provide any information that would reveal that a log has been created or filed and we promptly notify FIU of any such requests we receive. We separate log, form and suspicion filings and copies of supporting documentation from other company records to avoid disclosure of filings. Our AML Compliance Officer will process any subpoenas or other requests for filings we have made. We may share information about suspicious transactions with another financial institution to determine whether we should act in accordance with the provisions in section 3.4 jointly file a record. In cases where we file a joint record for a transaction processed by both us and another financial institution, both financial institutions will maintain a copy of the filed record.

14. AML training program

We will develop ongoing training for our freelancers under the direction of the AML Compliance Officer and senior management. Our training will take place at least once a year. It will be based on the size of our business, its client base and its resources and will be updated as necessary to take into account any new developments in legislation.

Our training courses include at least:

(1) How to recognize warning signs and signs of money laundering that occur in the course of the work of freelancers;
(2) What to do when the risk is identified, including how, when and to whom to report unusual customer activity or other warning signals for analysis and, if necessary, submission of protocols should be forwarded;
(3) What responsibilities freelancers have in the company's compliance efforts and how to fulfill them;
(4) the company's data retention policy; and
(5) The disciplinary consequences, including civil and criminal sanctions, for non-compliance.

Training may include training brochures, videos, intranet systems, face-to-face lectures and explanatory memos. We maintain records showing the people trained, the dates of the training and the training content.

We will review our operations to determine whether certain freelancers require specific additional training, for example in the areas of compliance and corporate security.

15. Independent tests for the AML compliance program

Independent testing of the AML compliance program of our company should generally include at least the following steps:

(1) Assessing the overall integrity and effectiveness of your company's AML compliance program;
(2) Assessment of your company's reporting, protocol- and record-keeping obligations;
(3) Assessment of the implementation and maintenance of the customer identification program of your company;
(4) Assessing your company's due diligence obligations towards customers;
(5) Assessing your company's transactions with a focus on high-risk areas;
(6) Assessment of the adequacy of the training program for the freelancers of your company;
(7) Assessing your company's systems for detecting suspicious activity, whether automated or manual;
(8) Assessing your company's system for reporting suspicious activity;
(9) Assessing your company's policy for reviewing accounts that generate multiple logs, reports and submissions, both internally and to government agencies;
(10) Assessing your company's response to previously identified deficiencies.

The audit of our AML program is conducted at least annually in a calendar year by Mr. Mücke of our company, who is neither the AML Compliance Officer, nor performs the AML functions being tested, nor reports to such persons. We separate the AML program audit from our AML procedures and normal business operations to ensure uninterrupted business operations during the audit. Independent testing will be conducted more frequently as circumstances warrant.

15.1 Evaluation and Reporting

Upon completion of the independent review, Mr. Mücke will report its results to senior management. We will promptly consider any resulting recommendations and maintain records of how each identified deficiency was remedied.

16. Monitoring the behavior and any user accounts of freelancers

We subject user accounts and freelancer transactions to the same AML procedures as client accounts under the supervision of the AML Compliance Officer. We also review the AML performance of line managers as part of their annual performance review. The AML Compliance Officer's accounts are reviewed by Mr. Burbach.

17. Confidential reporting of anti-money laundering violations

Freelancers must immediately report any potential breaches of the company's AML compliance program to the AML Compliance Officer, unless the breaches concern the AML Compliance Officer, in which case the freelancer report to the Managing Director or his representatives. Such reports are confidential and the freelancers do not have to provide any sanctions fear.

18. Other risk areas

The company has reviewed all areas of its business to identify potential money laundering risks that may not be covered by the procedures described above.

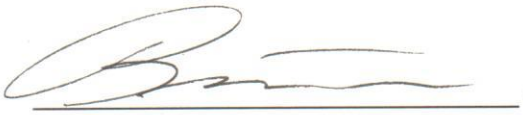
If a risk is identified that is not covered by our procedures, procedures will be developed immediately and all activities in the identified risk area may be suspended until a procedure has been developed. This new procedure will then be implemented immediately and incorporated into the AML program. The freelance employees will then be trained in the new procedure within fourteen (14) days.

19. Approval by the Senior Manager, Managing Director

Management has approved this AML compliance program in writing as it is appropriately designed to achieve and monitor our company's ongoing compliance with the requirements of the laws and regulations and their implementing rules. This approval is confirmed by the signatures below.

Signed by:

Claus-Allan Broennum



_____ (Signature)

Date: 06.07.2025