Codego SRL (“Codego”)

ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING POLICIES AND PROCEDURES

Confidentiality

All information contained in this document shall be kept in confidence. No part of this document is to be altered or copied without the written agreement of the CEO of Codego.

None of this information shall be divulged to persons other than to authorised employees of Codego, and shall be on a need to know basis. Release of this document to other parties shall be to individuals of organisations authorised by the CEO of Codego and in accordance with existing policy regarding release of company information and shall only be made available when an acceptable NDA has been signed with that party.

Summary of Changes

This paragraph records the history of significant changes to this document. Only the most significant changes are described here.

Version	Issue Date	Approved by	Description of changes
1.0	28 March 2024	CEO	Initial Document (Procedure)

Table of Contents

TERMS AND ABBREVIATIONS	
AML	Anti-Money Laundering
AFU	Asset Freezing Unit which is a department within HM Treasury responsible for the freezing of assets belonging to sanctioned individuals
Beneficial Owner	An individual who owns or controls more than 25% of the shares or voting rights in a body (e.g. Company/ business) and hence, carries an element of control over the management of the Organization
CDD (Customer Due Diligence)	Identifying and verifying the identity of the customer and any beneficial owner of the customer, and obtaining information on the purpose of intended nature of the business relationship
Merchant	Merchant is online e-shop or web service that is offering its goods or services online via Internet
Cardholder	Cardholder is the client of merchant willing to make a payment for goods or services offered at the website
Codego	Codego SRL (Codego)
Criminal Conduct	Conduct which constitutes an offence in any part of the United Kingdom, or would constitute an offence in any part of the United Kingdom if it occurred there
Criminal Property	Any money or other assets which constitutes a person's benefit from crime
KYB	Know Your Business
EEA	European Economic Area
Enhanced Due Diligence (EDD)	Additional customer due diligence measure that must be applied: 1. Where the customer has not been physically present for identification purposes 2. Where the customer is a PEP or In any other situation which by its nature can present a higher risk of money laundering or terrorist financing
KYC	Know Your Customer/Client
MLR	Money Laundering Regulations

PEP (Politically exposed persons)	A natural person who is or who has been entrusted with prominent public functions and includes the following: heads of State, heads of government, ministers and deputy or assistant ministers; members of parliament or of similar legislative bodies; members of the governing bodies of political parties; members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances; members of courts of auditors or of the boards of central banks; ambassadors, chargés d'affaires and high-ranking officers in the armed forces; members of the administrative, management or supervisory bodies of State-owned enterprises; directors, deputy directors and members of the board or equivalent function of an international organization
PEP close relatives (family members)	The spouse, or a person considered to be equivalent to a spouse, of a PEP; the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person; the parents of a PEP
PEP close associates	Natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a PEP; natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit
Nominated Officer/ MLRO	A Nominated Officer (also known as the MLRO officer) is the focal point within the company for the oversight of all activity related to anti-financial crime issues
Supporting Officer (s)	A person or persons nominated to act on behalf of the Nominated Officer
POCA	Proceeds of Crime Act 2002
Simplified due diligence (SDD)	An exception to the obligation to apply the customer due diligence measures for specific customers, e.g. financial institutions subject to the Money Laundering Directive or equivalent legislation and supervision. It is also available for some categories of products and transactions which may be provided by financial institutions
Transaction	The provision of any advice by a business or individual to a client by way of business, or the handling of the client's finances by way of business. A transaction could be simply operating across a client's account
SAR	Suspicious activity report
NCA	National Crime Agency
AEMI	Authorised Electronic Money Institution

1 INTRODUCTION

This document has been created for the employees of Codego, a company with headquarters in Milano, to use as guidelines for the AML responsibilities of both the company and the staff. Basically, the guidelines contain the information which all members of staff need to be aware of in order to prevent the business from being used to launder the proceeds of crime or terrorist financing. The AML Procedures Guidelines will provide the basis for all employees to comply with all applicable requirements in this area and will contribute to employees in preserving the good name and reputation of our company. The guidelines also have the procedures at place that deeply describe the rules that all staff member is obliged to comply and to use on a daily basis , fulfilling their responsibilities.

1.1 GUIDANCE

- outlines the legislation on anti-money laundering (AML) and combating terrorist financing measures;
- explains the requirements of the Money Laundering Regulations how these should be applied in practice.

Codego will always seek to disrupt this activity by cooperating fully with the authorities and reporting all suspicious activity to the National Crime Agency (NCA)

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.

The main goal of Codego's AML procedures is to reduce all possible risks in order 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 Bank Secrecy Act (BSA)/Anti-Money Laundering (USA), Directive (EU) of the European Parliament and of the Council and Visa and MasterCard regulation regarding Money laundering prevention.

Codego's policy has a strong risk-mitigation approach (fraud prevention tools and customised risk rules) , which helps guarantee compliance with all existing AML stipulations.

It is also the policy of Codego that staff must receive AML training on the commencement of their duties. Staff will be given a copy of this procedure with guidelines and education materials and will be tested on its contents before starting any client- facing duties.

Codego AML policies, 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 the business.

2 MONEY LAUNDERING

Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments. Such monetary instruments could be: money orders or traveller's checks, deposited into accounts at financial institutions, dividing the cash into smaller amounts and make various deposits into one or more accounts at one or more banks; customer opens several accounts in different names at different institutions; employ or persuade others to deposit funds for them; purchasing goods such as jewellery, art and other assets with a view to reselling them at a later date; making deposits with the help of employees of the relevant financial institution.

A) Placement

Cash generated from crime is placed in the financial system. This is the point when proceeds of crime are most apparent and at risk of detection.

Placement Red flags for Codego:

1. Transactions from multiple accounts for the same receiver;
2. Transactions from one account to multiple receivers;
3. Transactions coming from accounts created by auction houses, betting sites or e-wallets providers mainly used by gambling and betting sites;
4. Transactions from pre-paid credit cards.

At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. As example: Selling assets or switching to other forms of investment; transferring money to accounts at other financial institutions; wiring transfers abroad (often using shell companies); depositing cash in overseas banking systems.

B) Layering

Once proceeds of crime are in the financial system, layering obscures their origins by passing the money through complex transactions. These often involve different entities like companies and trusts and can take place in multiple jurisdictions.

C) Integration

Once the origin of the funds has been obscured, the criminal is able to make the funds reappear as legitimate funds or assets.

Integration Red flags for Codego:

1. Outgoing transactions to countries known as "offshore" banking countries;
2. Customers are using funds of a sales of assets like as house or jewellery;
3. Customers are using the funds for purchases of real estate, buying stakes in companies, or other large assets;
4. Incoming/outgoing transactions from private people to a company;
5. Prepaid credit card transferred funds to bank accounts (unusual that the receiver is more financially inclusion than the remitter).

At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses, for example - an inheritance, loan payments, asset sales abroad.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations.

In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

All members of staff are at risk of committing a criminal offence if they assist in a criminal transaction by missing the warning signs.

3 REGULATORY FRAMEWORK

The legislation in EU/UK governing money laundering and Terrorist Financing and the fight against it is contained in the following:

1. Proceeds of Crime Act 2002 (as amended);
2. Terrorism Act 2000 (as amended by the Anti-terrorism, Crime and Security Act 2001);
3. Money Laundering Regulations 2017;
4. UK Bribery Act 2010;
5. Payment Services Regulations 2009;
6. E-Money Services Regulations 2011;
7. Counter-Terrorism Act 2008, HM Treasury Sanction Notices;
8. FCA Handbook;

In addition, but not limited, references, guidance and instruction are given in HM Treasury Sanctions notices and news releases and the Financial Services Authority. It is important to note that EEA/UK legislation in respect of money laundering is “all crimes legislation”.

4. MLRO'S ROLES AND RESPONSIBILITIES

All staff must take steps to ensure compliance with this policy and ensure that they fully understand the material contained in this manual.

Responsible for the overall compliance policy of Codego and ensuring adequate resources are provided for the proper training of staff and the implementation of risk systems. This includes computer software to assist in oversight.

The MLRO (Money Laundering Reporting Officer) holds copies of all training materials. Updated AML training is given annually. Records of all training, including dates delivered and by whom, are kept both centrally and on staff personnel files.

Senior management will be sent monthly updates by the MLRO on compliance. They will also receive and consider the annual MLRO report and implement any recommendations made within it. Assistance may be given to the MLRO in the preparation of the AML manual.

All issues related to any noticed suspicious activity must be referred to MLRO in the first instance. The duties of the Money Laundering Reporting Officer include:

1. Monitoring the firm's compliance with AML obligations;
2. Being designated for, and accessible to, receiving and reviewing reports of suspicious activity from employees;
3. Considering of such reports and determining whether any suspicious activity as reported gives rise to a knowledge or suspicion that a customer is or could be engaged in money laundering or terrorist financing;
4. Overseeing communication and training for employees;
5. Ensures that the firm keeps and maintains all of the required AML records and will ensure that Suspicious Activity Reports are filed. The Money Laundering Reporting Officer is vested with full responsibility and authority to enforce the firm's AML program;
6. To receive disclosures from employees (also known as Suspicious Activity Report-SARs);
7. To decide if disclosures should be passed on to the National Crime Agency (NCA)
8. To review all new laws and deciding how they impact on the operational process of the company;
9. To prepare a written procedures manual and make it available to all staff and other stakeholders;
10. To make sure appropriate due diligence is carried out on customers and business partners;
11. To receive internal Suspicious Activity Reports (SARs) from staff;
12. To keep and review records of all decisions relating to SARs appropriately;
13. To ensure that staff receive appropriate training when they join and that the receive regular refresher training on an annual basis or if necessary;
14. To monitor business relationships and record reviews and decisions taken;
15. To make a decision on continuing or terminating trading activity with particular customer;
16. To make sure that all business records are kept for at least five years from the date of the last customer transaction.

Provision of Exemptions:

MLRO may only grant an exemption where he is clearly required or where practical experience reveals that it is necessary to do so. All exemptions will be considered on a case-by-case basis. Codego has adopted a risk-based approach to achieving its regulatory objectives and exemptions should not be considered as a way to avoid meeting our regulatory obligations. Careful consideration will be given to issues of transparency, equity and competitive neutrality in issuing exemptions. MLRO will assess the potential implications of applying an exemption and aims to adopt a consistent approach, taking account of the facts and circumstances particular to each case. Request for Exemptions from standard Customer Identification Process requirements may be received from AML and the Risk department in circumstances where, taking account of the CDD which has been obtained, MLRO is satisfied that the ML/TF risk has been adequately addressed. AML and the Risk department must use the "E-mail Exemption Request" when requesting an exemption from the Customer Identification Process. The completed e-mail must be sent to MLRO and must be approved by return of email by MLRO before any exemption can be provided.

5. RISK- BASED APPROACH

As per the Money Laundering Regulations, each regulated firm must exercise a 'risk- based approach' to its customers, products and business practices.

Codego operates a regimented system based upon processes. Our 5-step approach is:

- Identify the money laundering risks that are relevant to our business;
- Carry out periodic risk assessments on various parts of our business, focusing on customer behavior, delivery channels, patterns, and irregularities;
- MLRO to design and put in place effective controls to manage and reduce the impact of the risks;
- MLRO/Compliance to monitor the controls and improve efficiency;
- Maintain records of processes/systems that were checked and why we checked them.

The results of Codego annual risk assessment will be presented and approved by the Board of directors.

As a small sized entity, we review ourselves internally and base our assessment on our chosen business models, our products and services.

International AML legislation demands risk-based approach to be implemented for every financial institution. The Risk based approach helps to drive the institution's compliance resource allocation, internal controls strategy, system structures, and enables an organization to focus on higher risk areas. Codego considers the risk-based approach as two-tiered concept. First of all, every financial institution should estimate all possible money laundering and terrorist financing risks. Secondly, every financial institution should implement its own, most appropriate for its type of business prevention concept.

Our policies are formed by using the FATF guidance on the Risk-Based Approach, that a regulated firm should adhere to, in order to effectively combat Money Laundering and Terrorist Financing. The FATF guidance supports Codego in the development of:

- A common understanding of what the risk-based approach involves;
- Outlining the high-level principles involved in applying a risk-based approach;
- Promoting Codego in the eyes of its partners, as our risk-based approach indicates a good public and private sector practice.

It is recognized that a higher level of due diligence and monitoring would be specified for business areas prone to higher AML risks. Accordingly, entities, their owners, directors whose identities can be easily identified and transactions implemented by them and large conform to the known profile, may be categorized as low risk.

Further, customers that are liked to pose a higher than average risk to Codego may be categorized as medium or high risk depending on factors such as Merchant's backgrounds nature and location of activity etc.

All in all, the risk assessment's scope includes, but not limited to: the type, scale and complexity of the business, the products and services sold, target markets, high risk customers, jurisdiction exposure, distribution channels, transaction size and volumes as compared to historic trends, systems, major organizational changes, and compliance testing, audit and regulatory findings.

The risk assessment should include as much information as is obtainable to provide a clear and accurate assessment.

6. IBAN ACCOUNT CUSTOMERS' MITIGATION PROCEDURE

The identification process for e-wallets is the most difficult one from different points of view. Based on each country's legislation , there are a lot of restrictions, and also card schemes have their own regulations on this question.

One of the ways how Codego can go with IBAN account is to build the concept of motivation, remuneration and strict control.

The motivation to use the wallet should be:

- Stability;
- Safety of funds;
- Easy and understandable registration process;
- Availability on mobile devices;
- Worldwide accessibility;
- Opportunity to pay on different websites;
- Immediate payments;
- Multi-currency accounts
- 24/7 customers support.

Registration is the initial step and probably the most important step in process of attracting a new Client to a product. To make registration as painless and simple as possible, Codego attempts to capitalize on the on the waiver provided by the European regulatory regime.

Legal Background

European legislation has been adopted to protect the financial system and other vulnerable professions and activities from being misused for money laundering and financing of terrorism purposes. The primary European Union act that applies to the financial sector is the 3rd anti-Money Laundering Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. The Directive has been transposed to all EEA and UK legislation in form of Law on the Prevention of Laundering the Proceeds from Criminal Activity (Money Laundering) and of Terrorist Financing. The law specifies cases where simplified due diligence may be applied.

Simplified due diligence

Simplified due diligence may be applied to non-reloadable purses, accounts, and otherwise payment instruments in physical and digital form. Where electronic money purses cannot be recharged and the total purse limit does not exceed 500 EUR (verification of identity does not need to be undertaken. This takes into account the ability of individuals to purchase multiple purses and to, therefore accumulate a higher overall total of purchased value.

Those issuers that provide electronic money purses that can be recharged, whether card or purely server-based, are required to undertake verification of identity procedures only when the annual turnover limit of 2,500 EUR is exceeded or if the customer seeks to redeem (withdraw in cash) more than the 1,000 EUR annual allowance.

Where purses can both send and receive payments, such as, for example, in online account-based products that enable person -to- person payments, the 2,500 EUR turnover limit is applied separately to sending and receiving transactions. In other words, the turnover limit is calculated separately for credit and debit transactions, and the verification requirement is applied when either of the two is exceeded.

In respect of products benefitting from simplified due diligence, identity must be verified before cumulative turnover limits are exceeded. Systems must , therefore be in place to anticipate the approach of limits and to seek identification evidence in good time, before the annual turnover limits are reached. The customer's account must be frozen if the limits are reached before verification of identity has been completed.

Gradation of User levels and access:

Registered user (1st lane of KYC/AML)	
Registration process:	
• Enter name and surname (middle name if applicable); • Phone number; • Email address; • Approve that agree with Terms & Conditions and Privacy Policy; • Get verification code and verify email or phone number;	
Allowed activities:	
• Log in; • Fill the profile; • Add banking details; • Top-up the account; • Verify banking account; • Add payment card (3DS); • Verify payment card.	
Codego Risk department responsibilities:	
• Track merchant registration; • Send proposal to upgrade the account showing the added value that comes with it; • Send offer with wallet top-up opportunities; • Assign the status of registered client and set automatically the limits.	
Allowed top-up amount per month:	100 GBP / USD / EUR
Allowed settlement amount per month:	0 GBP / USD / EUR
Annual turnover restrictions:	1000 GBP / EUR / USD
Payments:	Not-allowed

Pre-verified user (2nd lane of KYC/AML):	
Pre-verification process:	
When the 1st stage is completed user must pre-verify his account to start using the IBAN wallet account with cut functionality but already operated. • Complete the user profile with all required information; • Verify two communication channels (email & phone); • Phone verification – call or SMS; • Email verification – URL or code. • Add banking details for settlements; • Verify banking details by sending 1 EUR/ USD transaction; • Add payment card for wallet top-up or other available method; • Verify payment card by 4-digit security code and 3DS if card supports it: • In some cases, send the front side of the payment card (photo or scan). • Send corporate or personal documents: • Personal: ID Card / utility bills for the last 3 months / Tax number; • Corporate: incorporation documents and UBOs data.	
Allowed activities:	
Make a payment to merchant or other users (B2P / P2P / B2B);	
Allowed top-up amount per month:	500 GBP / USD / EUR
Allowed settlement amount per month:	1000 GBP / USD / EUR
Annual turnover restrictions:	2500 GBP / USD / EUR
Payments:	Allowed with limits

Verified user:

Verified user account allows users had passed full AML/KYC procedures and we fully know our customer and his personality.

Verification process:

- Pass screening procedures in World Check and other services;
- Pass documents due-diligence procedure;
- Verify bank account with 1 EUR (USD) transaction;
- Pass address verification by receiving an envelope with secure 4 digits and 2 letters code
- Pass video biometric verification with device and mobile application becoming unique token authorization for users

Unlimited user:

Unlimited user refers to client rage who has active wallet during the last 6 months from the registration period. These users are not simply verified account holders but also clients that are active and we see their financial flows and understand income sources.

Unlimited user account status:

- Pass all verification procedures;
- Active account for the last 6 months;
- Added +1 family member of colleague with verified account;
- Active usage of IBAN account top-up and settlement method;
- For the users who operate with more than.

CUSTOMER PROFILE FIELDS
Basic:
• *Name and surname (middle name);* • *DoB;* • *Gender;* • *Registered address;* • *Living address:* • *Street number;* • *City;* • *Country;* • *Postal code.* • *Contact information:* • *Phone number;* • *Email address;* • *Correspondence address.*
Advanced:
• *Passport number;* • *Issuing date;* • *Issued authority;* • *TAX number.*

•

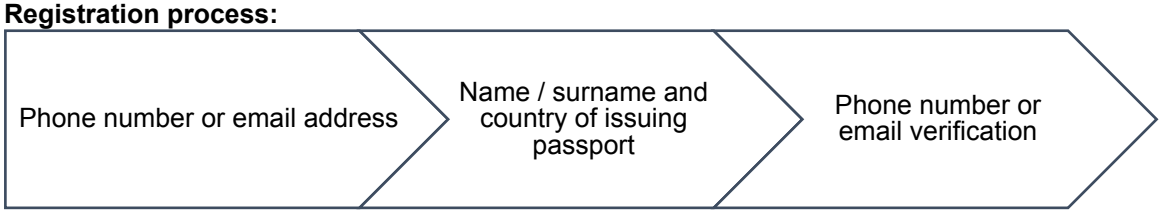
Customer KYC/AML profile:

This profile is used be the monitoring and risk department to have full access to customers' profiles and data with the opportunity to open any day log file and investigate his activity or unusual behavior.

Personal account:

PROFILE RISK RULES
• Name – Internal profile identification; • Countries – choose where this profile can be used; • Allowed accounts – list of currencies in which a member assigned to current profile can create an account.

Registration process:



After the first stage Codego should:

- Create a user profile;
- Tick the verified email or phone number;
- Check person in screening services for alerts;
- Activate the profile.

The second stage include additional verification to grant user right to operate with account:

- Add ID data;
- Add physical and declared address;
- Upload ID scan;
- Upload utility bill.

Completing this stage, Codego risk department should check the provided documents, run Checks and assign the first level of Codego e-wallet user account grade. User s based on this verification can:

- Transfer money;
- Pay for goods and services;
- Receive money;
- Withdraw money to his bank account.

There should also be assigned the appropriate monthly and annual limits.

7. MERCHANTS RISK MITIGATION PROCEDURE

Codego understands that the Risk Assessment starts during the Underwriting Stage. That is why merchant screenings are implemented in order to spot any potential threat to our business operations and to our reputation. Codego partners with world first class risk prevention and mitigation services and others to enhance the merchant checks by doing the following:

- Merchant screening before boarding: a comprehensive background report is provided, which allows us to know who we're dealing with before signing the contract. It also reduces the time needed to conduct due diligence of merchants;
- Simple and regular Merchant monitoring: it provides automatic follow ups on our current merchants' online activities;
- Constant long-term protection: the software protects our reputation by reducing the risk of falling victim of fraudulent merchants.

Also during the underwriting stage, the merchant is provided with general and specific processing rules which serve as guidelines for the future partnership with Codego. Among other things, such rules aim to anticipate and reduce the threats associated to each type of merchant.

8. CARDHOLDERS RISK MITIGATION PROCEDURE

Codego identifies the money laundering and terrorist risks presented by:

- Geographic area of operation;
- Product;
- Customer;
- Delivery channel.

Cardholders are classified according to their risk level:

- Low Risk;
- Medium Risk;
- High Risk.

In determining a risk assessment for a cardholder, the presence of one factor that might indicate higher risk does not automatically establish that a customer is higher risk. Equally, the presence of one lower-risk factor should not automatically lead to a determination that a customer is lower risk.

9. POLITICALLY EXPOSED PERSONS (PEPS)

PEPs are defined as individuals who have been entrusted with a prominent public function outside of the EEA/UK. Codego will also extend the definition of a PEP to any immediate family member and/or close associate of the person mentioned above in order to comply with regulations, Codego ensure that all accounts relating to PEP's must:

- Be approved by the MLRO;
- Be subject to enhanced due diligence;
- Codego consider s all transactions and any association with a PEP as high risk. Any transactions or requests from a PEP (or someone who you think is a PEP) must be signed by MLRO. Any PEP wishing to become Codego's customer shall be asked to verify the source of their funds.

The definition of a PEP is set out below:

- Is or has, at any time in the preceding year, been entrusted with prominent public functions;
- Is an immediate family member of such a person;
- Is a known associate of such a person;
- Is or has, at any time in the preceding year, been entrusted with a prominent public function by:
    - A state other than the European Community;
    - The United Kingdom or
    - An international body; or
- Is an immediate family member or a known close associate of a person referred to in the paragraph immediately above.

It is a matter of company policy that all customers will be required to indicate whether they or any member of their family has previously worked in a non-EU country at any time in the preceding 12 months. In case the answer is yes, the cashier must make enquiries to establish whether the customer may meet the criteria for being 'politically exposed'.

In cases where a PEP is identified:

- Senior management approval should always be sought before establishing a business relationship with a PEP;
- The source of funds should be established;
- The business relationship should be subject to enhanced monitoring.

10. SANCTIONS SCREENING

Sanctions are normally used by the international community for one or more of the following reasons:

- to encourage a change in the behaviour of a target country or regime;
- to apply pressure on a target country to comply with set objectives;
- as an enforcement tool when international peace and security has been threatened and diplomatic efforts have failed;
- to prevent and suppress the financing of terrorists and terrorist acts.

Financial sanctions are normally one element of a package of measures used to achieve one or more of the above. Financial sanctions measures can vary from comprehensive – prohibiting the transfer of funds to a sanctioned country and freezing the assets of a government, corporate entities and residents of the target country – to targeted asset freezes on individuals/entities.

Taking into consideration both EU and US regulations, Codego uses additional tools to check potential or actual Merchants against OFAC and non-OFAC sanction lists. It is essentially important for Codego not to establish any business activity with the companies (individuals) which are included in these lists.

Before opening an account, and on an ongoing basis, Codego will check to ensure that a customer does not appear on the sanction list or is not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by EU, US and United Nations.

Codego checks every Merchant and their cardholder who implements transactions for large amounts against three existed Sanctions Lists: OFAC list, European Union Sanction List, United Nations 1267 List.

If Codego determines that a customer is on the one of sanctions list or is engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by regulations, the company will reject the transaction and/or block the customer's assets and file a blocked asset and/or rejected transaction.

Taking into account the cross-border business of Codego, it is very carefully processing its customers CDD, EDD, ongoing transaction monitoring and other activities to prevent possible violation of the ML/TF and other limitations/restrictions.

As Codego will use automated screening program with ‘fuzzy matching’ logic and which is calibrated in accordance to Codego risk level, once the integrated screening lists (including OFAC SDN list) will be updated within the program, the screening process will be performed using the most recent lists immediately, but in any case, not later than within 1 week after the screening lists updated.

Customers with whom a business relationship is established would be screened against relevant notices published by:

- European Union sanctions (EU);
- Her Majesty’s Treasury Department – UK (HMT);
- OFAC.

If a positive match is discovered, the responsible employee must inform MLRO immediately. MLRO must investigate received information and if positive match, inform the responsible employee which must block the customer in operational system until consent is given to proceed or refuse. MLRO makes a disclosure to the relevant.

11 CUSTOMER DUE DILIGENCE

Codego applies Due diligence at the start of customer engagement by identifying and verifying the customer identity on the basis of documents, data or information obtained from a reliable and independent source.

Codego conducts CDD both for natural customers, business customers, merchants and cardholder, as detailed below.

Codego identifies the Beneficial Owner of the Customer (in case of both, legal entities and individuals) and takes adequate measures, on a risk sensitive basis to verify his identity (including in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure).

Codego creates policies and procedures that relate to customer due diligence, ongoing Monitoring, suspicious reporting and record keeping.

If any suspicions are identified, then these should be raised to the MLRO for further investigation by completing the relevant internal Suspicious Activity Report (SAR) form.

The purpose of the Customer Due Diligence (CDD) process is to collect, process, verify and keep the information about Codego customers, due to minimize the possible and potential ML/TF risks. There are circumstances in which enhanced due diligence should be applied and others in which simplified due diligence may be appropriate:

- It should be recognized that certain situations present a greater risk of money laundering or terrorist financing. Although the identity and business profile of all customers should be established, there are cases in which particularly rigorous customer identification and verification procedures are required;
- Relationships with individuals who hold or who have held important public functions, within the Union or internationally, and particularly individuals from countries where corruption is widespread.

Customer identification:

For the purposes of further, Codego must identify its Customer unless the identity of that Customer is already known to, and has been verified by, the relevant person. After the Customer has been identified, Codego must verify the Customer's identity unless the Customer's identity has already been verified by the relevant person. Amount of information to be received from a Customer depends on whether the Customer is a legal entity or an individual (natural person), namely:

- If a customer is a legal entity, at least the following information must be received for identification purposes: company name; registration number; address of the registered office (and, if different, its principal place of business); the law to which the legal person is subject; its constitution (whether set out in its articles of association or other governing documents); full names of the board of directors (or if there is no board, the members of the equivalent management body) and the senior persons responsible for the operations of the legal entity.

- If a customer is an individual (natural person), then 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; number and date of issue of the personal identification document, state and authority which has issued the document; period of validity of identification document.

Customers Who Refuse to Provide Information:

A risk-based approach lies in a very foundation of Codego AML program. The rule that Codego considers as one of the most important is Know your Customer in order to minimise all possible risks connected both with unknown identity of Natural Customers, Business Customers, Merchants as well as Cardholders, which can be caused by Lack of Verification and unusual merchants or Cardholders behaviour which could be detected during ongoing transactions monitoring.

In a case when a potential Merchant refuses to provide the required information, Codego doesn't establish any business relationship with such kind of merchant and doesn't take it on board. If Codego reveals the fact that a Cardholder who implements large amount transaction doesn't want to provide the information needed for establishing his/her identity Codego doesn't approve this transaction and further transactions made by this Cardholder unless he provides all required documents.

Customers – Insufficient or Suspicious Information:

- Provides unusual or suspicious identification documents that cannot be readily verified;
- Reluctant to provide complete information about nature and purpose of business;
- Background is questionable or differs from expectations based on business activities;
- Customer with no discernible reason for using the firm's service.

Codego scrutinizes transaction flow throughout the course of any business relationship to ensure consistency with the knowledge of customers, their business and risk profile. The MLRO conducts ongoing monitoring of all high-risk activity, including customers who regularly implement transactions for large amounts.

List of Acceptable Identification:

- Current passport.
- Current National Identity Card.
- Current EU/UK Residence Permit (Issued by the Home Office).
- Current full EU/UK photocard driving licence (provisional licences are acceptable for U18s only).
- Current full EU/UK driving licence (old style paper version).

List of Acceptable Address Verification:

- Utility bill (dated within last 3 months).
- Bank, Building Society, Credit Union statement – showing current activity (dated within last 6 months). Certain conditions may apply for overseas financial providers.

Non-EU/UK Residents:

Due to new legislation, Non EU/UK residents must always present their Passport or National Identity card when applying for an account.

11.1 SIMPLIFIED DUE DILIGENCE (SDD)

Simplified due diligence means – not having to identify the customer, or to verify the customer's identity, or, where relevant, that of a beneficial owner, nor having to obtain information on the purpose or intended nature of the business relationship.

It is, however, still necessary to conduct on-going monitoring of the business relationship. Codego must have reasonable grounds for believing that the customer, transaction or product relating to such transaction falls within one of the categories set out and may have to demonstrate this to their supervisory authority.

Clearly, for operating purposes, Codego will nevertheless need to maintain a base of information about the customer. Codego may apply a 'lighter touch' in terms of the extent of CDD undertaken.

Also, mandatory would be applied under SDD, sanctions and PEP's screening procedure to ensure that companies' customers are not listed before getting into relationships.

Customers without full KYC documentation on file are limited to:

- no more than 250.00 EUR for a single transaction;
- no more than 1,000.00 EUR in a 12-month period;
- no more than 2 approved transactions in 6 months.

The limits above apply to the Customer, regardless of number of cards used.

Customers with full KYC documentation on file and approved by Codego Risk and Compliance Department:

- Transaction amounts less than an agreed- upon threshold will be Captured Automatically;
- Transaction amounts in excess of an agreed- upon threshold will be placed in a queue for approval by the Codego Risk and Compliance Department.

Codego only accepts transactions for Countries that are not considered high- risk jurisdictions by FATF and OFAC.

11.2 ENCHANCED DUE DILIGENCE (EDD)

Codego's Enhanced Due Diligence (EDD) policy is designed to obtain as much information as possible in order to ensure the validity of the transaction and that Codego complies with ML Regulation (2007), POCA (2002), Terrorism Act (2000) and the EU Money Laundering Directives. In practical terms, EDD will include:

- taking reasonable measures to establish a customer's source of wealth – source of wealth is distinct from source of funds, and describes the activities that have generated the total net worth of a person, i.e. those activities that have generated a customer's income and property;
- considering whether it is appropriate to take measures to verify source of funds and wealth from either the customer or independent sources (such as the Internet, public or commercially available databases);
- obtaining further CDD information (identification information and relationship information);
- taking additional steps to verify the CDD information obtained;
- commissioning due diligence reports from independent experts to confirm the veracity of CDD information held;
- requiring more frequent reviews of business relationships (twice per year);
- carrying out stricter monitoring of transactions and setting lower transaction thresholds for transactions connected with the business relationship, and;
- setting alert thresholds for automated monitoring at a lower threshold for PEPs.

Customers subject to EDD are required to provide a written confirmation regarding the legal origin of funds. Failure to provide such may result in a transaction being held.

The degree of EDD must be determined by MLRO on a case-by-case basis.

11.3 BUSINESS CUSTOMERS/MERCHANTS FULL DUE DILIGENCE (FDD)

It is important for Codego's AML program to obtain sufficient information about each Business Customer/Merchant that allows the evaluate the risk presented by that customer and to detect suspicious activity.

Business Customer/Merchant Due Diligence of a risk- sensitive bas is depending on the type of client, business relationship, or services to be provided is the foundation of Codego Data AML compliance program. Merchant Due Diligence provides the firm with a baseline for evaluating customer transactions to determine whether the transactions are suspicious and need to be reported.

The main goals of MDD for Codego are:

- Be satisfied that Business Customer/Merchants are who they say they are;
- Understand whether its customers are acting on behalf of others and the identity of any beneficial owner(s);
- Understand its customers' circumstances to guard against their being used for fraud, money laundering or other criminal activity.

Steps of Business Customer/Merchant Due Diligence:

- Obtaining information to identify the Business Customer/Merchant(s);
- Verifying the Business Customer/Merchant and/or beneficial owner(s) identification information;
- Collecting KYC optional documents;
- Conducting Business Customer/Merchants screening.

Obtaining information to identify the Business Customer/Merchant(s):

Codego follows procedures to identify all Business Customers /Merchants that the company has relationships with. During underwriting stage, Codego requires all the documents needed for the Business Customer/Merchant identification. Business Customer/Merchant boarding and application process starts with completing merchant's KYC. Our document requirements comply and often surpass the standard requirements:

- Codego forms;
- Corporate documents:
    - Certificate of incorporation;
    - Incorporation documents showing directors and shareholders (not only company representatives, we perform full UBO identification, in case of more complex structures, we collect information about all owning companies).
- Passport/national ID(s) of directors and shareholders owning more than 2% company shares (we do accept companies created with hosts);
- Bank statements as a proof of accomplished bank's verification procedures (recent 3-6 months);
- Processing statements (recent 3-6 months);
- Company utility bills;
- Re-presentment files;
- Domain ownership.

Forms:

- Pre-application form – containing basic information, useful while presenting a merchant;
- Preliminary scan form - a substitution (along with forecast) for the pre-application. Contains basic company data required to start automated reputational checks;

Verifying the Business Customer/Merchant and/or beneficial owner(s) identification information:

- In some cases, the Business Customer/Merchant's information is obtained directly from the customer. In other situations, the information is obtained from other sources. Irrespective of how or where the identification information is obtained, a determination must be made whether the information also needs to be verified.

Irregularities in the above documentations may be indicators for suspicion, leading Underwriters and Risk staffs to do additional research.

Before onboarding process, Codego estimate all risks connected with:

- Business Customer/Merchant's actual or anticipated business activity;
- Business Customer/Merchant's ownership structure;
- Anticipated or actual volume and types of transactions;
- Transactions involving high-risk jurisdictions.

KYB Optional Documents

For some specific merchant applications (related to higher risk or for merchants providing services that may be regulated by some authorities) we might request some more specific documents:

- Resume or CV(s) of directors and owners and detailed business plans with 6-month prognosis (if processing history not available);
- Annual tax documents (for company and director or shareholder);
- Business / operating licenses and permits;
- Legal opinions - in case of any doubts about the Merchant's business if it is legal in the incorporation country;
- Certificate of Good Standing issued by competent authorities (issued for example by states secretaries);
- List of businesses that Company principals and/or beneficial owners own(ed)/operated) or have been involved in the past 5 years (statement).

Apart from additional documents in some cases collaterals could be implemented and have to be properly calculated (for example in case of long breaks between payment and fulfilment, i.e. Travel agencies).

Conducting Business Customer/Merchants screening

- Codego understands that the Risk Assessment starts during the Underwriting Stage. That is why merchant screenings are implemented in order to spot any potential threat to our business operations and to our reputation;
- Reputation should be handled in two ways - manual and automatic/semi-automatic. For manual checks the key tool is the web search engine (i.e. Google, Bing, Yahoo) along with some more specific tools like who.is (for domain information), robtex.com (for domain and IP related checks) and alexa.com (to estimate the website traffic);
- During manual check some key data like Business Customer/Merchant name, directors' names, URL address and related phones, emails and addresses should be checked along with phrases that may occur in regard to the business model (i.e. crime, scam, review) to narrow search results to the results really interesting in terms of international investigation (i.e. if merchant's director is a felon or a convict or known fraudster);
- Generally, in case of suspicious Business Customer/merchants usually director's full name or merchant's company name should return some results that will give the initial information to follow up or reject application at the early stage, however that is not a rule and sometimes the important results are found in most unexpected places.

Website Compliance Check

- Codego implements checks of Business Customer/Merchant websites that must comply to the following requirements. Every website that is about to be used for ecommerce processing must comply to the specific requirements regulated by card schemes (Visa/MC):
- Clear posting of the Refund and Return Policy;
- Clear Privacy Policy;
- Clear statement on website regarding security controls used to protect customers;
- Clear posting of the Terms and Conditions;
- Clear posting of the customer service telephone number and email address;
- Clear posting of delivery methods and delivery times (if applicable);
- Clear posting of the company legal name and corporate address;
- Clear posting of the billing descriptor on the payment page;
- Card Schemes logos visible on the payment page.

Contact information and customer support are always verified by performing test calls/emails.

Automated Checks

Parallel to manual screening we are also executing external tools provided by 3rd party companies, i.e.

To run that automated screening Codego requires completed preliminary scan form, that contains following data:

- Company name, registration number and address;
- Director’s name, passport number and email address;
- UBO’s (Ultimate Beneficial Owner) name, passport number and email address;
- Merchants bank details;
- Website address.

11.4 REGULAR CUSTOMERS/CARDHOLDERS FULL DUE DILIGENCE

Codego follows reasonable procedures to verify and identify customers/cardholders who makes transactions for large amounts (customers/cardholder due diligence). Such procedure of identification and verification of customers/cardholders based on information the firm collects from the customers/ cardholder and then this information is verified.

Codego risk department, first of all, collects certain customer identification information from each customer who implements transaction for large amount, secondly, utilizes risk-based measures to verify the identity of every customers/cardholders who implements transaction for large amount, thirdly, records customer identification information and the verification methods and results, finally, using gathered information about the cardholder, risk department makes cardholder screening against OFAC and other sanction lists.

CDD process steps:
For all customers CDD must be completed prior enter into the relationship and it is necessary to complete the steps as follows:

- Perform identification and verification – identify and where required verify the identity of the prospective customer and related parties;
- Screen all customers and related parties against the EU list, HM Treasury sanctions list, and OFAC SDN list, UN list;
- Screen all customers and related parties to determine if there are any PEPs associated with the customer, by using public, trustable and opened information source;
- Determine customer risk rating;
- Complete EDD as required by the risk rating,

Minimum information to create customer's file

Natural persons:

- Name, surname;
- Original and current identification evidencing nationality or residence and bearing a photograph or similar safeguard, such a passport, national identification card or alien identification card with date of birth and place of birth;
- Living address and postal code;
- Officially certified copies of the above documents;
- Disclaimer/questionnaire for the origin of funds not being derived from the proceeds of crime.

Legal entities:

- Company' name;
- Beneficial owner name;
- Ownership memorandum, article of association etc.;
- Legal and physical address;
- Other relevant documentation such as company's activity details, expected turnover or expected etc.;
- Officially certified copies of the above documents;
- Expected type and volume of transaction;
- Main counterparties and countries;
- Disclaimer/questionnaire for the origin of funds not being derived from the proceeds of crime.

Codego requirements for the customers/cardholders who exceed certain thresholds include following documents:

- A signed Authorization Form (form must be as provided by Codego or approved by the Risk and Compliance Department if furnished by the Merchant);
- A copy of a valid government issued ID with photo;
- A copy of a recent utility bill or a bank statement displaying the home address as stated in the Authorization Form.

In verifying the information, we will consider whether the identifying information that we receive, such as the customer's name, street address, zip code, telephone number (if provided), date of birth allows us to determine that we have a reasonable belief that we know the true identity of the customer (e.g., whether the information is logical or contains inconsistencies).

Appropriate documents for verifying the identity of customers include the following:

- For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and
- For a person other than an individual, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or a trust instrument.

12 ONGOING TRANSACTIONS MONITORING REVIEW

Codego pays special attention to ongoing monitoring of transactions, customers behaviours in order to prevent all the possibilities of fraud and money laundering appearance. The company monitors client's' instructions and transactions to ensure that they are consistent with those anticipated, that possible grounds to suspect money laundering will be noticed and scrutinized, and that changes requiring a re-assessment of money laundering risk will be acted upon.

Possible risks associated with customer behaviour:
Codego considers following possible risks associated with customer behaviour which could be divided in 3 areas:

- Risks posed by regular customer;
- Risks posed by business customer or merchant;
- Geography risks.

Following possible risks can be connected with Customer who uses payment cards:

- Cardholder uses a stolen card or account number to fraudulently purchase goods/services online;
- Uncharacteristic transactions which are not in keeping with the customer's known activities;
- Family member uses payment card to order goods/services online, but has not been authorized to do so;
- Cardholder falsely claims that he or she did not receive a shipment.

Risks posed by business customers or merchant:

- Unscrupulous merchant employee steals cardholder data and fraudulently uses or sells it for unauthorized use or identity theft purposes;
- Selling illegal or defective products (brand piracy, child pornography, prescription narcotics);
- Circumventing blacklisting by the Merchant Category Code. Especially in the credit card industry this is referred to as “miscoding”.

Geography Risks:

- High-Risk IP addresses;
- Peaks of activity at particular locations;
- Multiple cards used from a single IP (Internet Protocol) address;
- Multiple payments done from one location.

13 FRAUD MITIGATION MEASURES

Codego implements fraud-screening tools to identify high-risk transactions. Codego makes check of high-risk Customers and Business Customers addresses. It helps the company to reduce fraud by comparing the addresses given by the Customers or Business Customers to high-risk addresses in Codego own negative files. Codego pays special attention to high-risk locations such as mail drops, prisons, hospitals, and addresses with known fraudulent activity.

Codego establishes velocity limits and controls. Every Business Customers has its own limits per every payment (as max permitted transactions per day, week and month along with permitted transactions amount).

14 STAFF TRAINING AND AWARENESS

The Regulations requires all financial institution ensure that all employees are aware of the policies and procedures that have been put in place to prevent the company from being sued for money laundering or terrorist financing purposes. Each company must also take steps to ensure that all employees are aware of the requirements and their own obligations.

The AML Guidelines will be given to all employees to meet the foregoing requirement. The AML Guidelines with its more detailed provisions will be given to employees having dealings with or other contact with Merchants and Cardholders to further support this obligation.

Non-compliance with the AML Guidelines may result in disciplinary actions. Before a decision with regard to disciplinary action is taken, the seriousness and merits of each case shall be appraised by the Management.

Codego will develop ongoing employee training under the leadership of the Money Laundering Reporting Officer, Head of Risk and Compliance department and senior management. The training will occur on at least an annual basis. It is important, as part of ongoing staff training, to make staff aware of changing behaviour and practices amongst money launderers and those financing terrorisms.

Staff training on anti-money laundering and counter terrorist financial will be carried out annually for all staff members, and details will be recorded and stored in the company achieve.

One of Codego's key controls in mitigating the threat of being used for money laundering is having staff that is aware of and alert to the threat. All staff, whether on a full-time, part-time or contract basis, are made aware of our anti-money laundering policy, manual and the obligations arising from them for both themselves and Codego provides training on anti-money laundering.

These training comprising two key elements:

- Induction Training - The MLRO is responsible for identifying relevant new staff that are required to undertake induction training within 45 days after requirement. The training is provided by the MLRO or the MLRO will engage external AML Advisors and is face to face training. The content of the training includes awareness training, covering Money Laundering and Terrorist Financing. Understanding of the subject matter is assessed throughout the training through case studies. Until a new member of staff has been signed off as competent no direct customer contact is allowed;

- Refresher Training - all relevant staff must undertake face to face refresher training on annual basis. The training is provided by the MLRO or the MLRO will engage AML Advisors and assessment of staff understanding is carried out throughout the training.

Codego will obtain acknowledgement from staff that they have received the necessary training by requesting staff to sign their attendance at training sessions. Overall monitoring of attendance is recorded manually and stored on the AML file. Certificate will be provided to each participant on successful completion.

15 PROHIBITIONS ON CUSTOMER RELATIONSHIPS

Codego, in considering money laundering risks, regulations and guidance, decided that certain types of relationships are unacceptable:

- shell banks;
- individuals or entities that are on relevant sanctions lists issued by countries in compliance with UN resolutions or to which countries have applied sanctions unilaterally (EU, UK, US and others);
- individuals or entity whose identity cannot be verified or
- who refuses to provide the information required to verify identity or required for account opening purposes; or;
- who has provided information that contains inconsistencies that cannot be resolved after further investigation;
- Where there is suspicion or evidence of found, money laundering or other criminal activity or involvement;
- If falsified documentation or information is detected during the account opening/relationship establishment process;
- Individuals, entities and organisations sanctioned by UN, EU, HM Treasury list or OFAC;
- An account using a pseudonym or number rather than the actual name of the customer;
- Anonymous ownership entity accounts, where the ownership of the entity cannot be determined because the entity has a form or structure that prevents an account accurate identification of the Beneficial Owners;
- Unlicensed financial institutions, including unlicensed currency exchange houses and money transmitters, and
- Persons involved in unlawful internet gaming business;
- Customers - merchants whose business Merchant Category Code (MCC) is included into the International Card Organisations prohibition list.

16 SUSPICIOUS ACTIVITY REPORTING

The Proceeds of Crime Act 2002 (POCA) requires (amongst other things) that when in the course of business, a member of staff of Codego comes across what is described as Suspicious Activity it should be reported in the first instance to the MLRO.

There is no definitive list of what constitutes suspicious activity, however, if the principles of KYC are rigorously applied, then in the course of conducting business with the client, sufficient information should be available, to make a judgment about what constitutes suspicious activity in each case.

When suspicious activity is suspected, the following procedures will be followed:

- The person suspecting should immediately make a written report or e-mail to the MLRO If urgent, telephone first, then follow up with a written report;
- No discussion with other members of staff should take place. A record of the date and time of the report should be recorded;
- Acknowledgement of the receipt of the report should be obtained from the MLRO. This can be done via a receipt email from the MLRO;
- New suspicion of the same client means a new report must be made;
- Failure to report knowledge or suspicions of laundering of the proceeds of crime is a Maximum Five years imprisonment and/or an unlimited fine.

Tipping off

It is an offence to make a disclosure which is likely to prejudice any investigation which might be conducted following the making of a Suspicious Activity Report Maximum 2 years imprisonment/or an unlimited fine.

Money Laundering

It is an offence to conceal, disguise, convert, transfer or remove criminal property from the Europe and United Kingdom. Maximum Fourteen years imprisonment and/or an unlimited fine:

- It is an offence to enter into or become concerned in an arrangement which he knows or suspects facilitates the acquisition retention use or control of criminal property by or on behalf of another;
- Maximum Fourteen years imprisonment and/or an unlimited fine;
- It is an offence to acquire use or have possession of criminal property;
- Maximum Fourteen years imprisonment and/or an unlimited fine.

If in doubt report your suspicion to MLRO, you have then complied with your obligation.

All contact with Law Enforcement Agencies will be handled by the MLRO.

The MLRO is responsible for providing information and updates to the legislation as and when they occur.

Codego consider s any failure to comply with any of the relevant legal or regulatory requirements by any member of staff to be gross misconduct and will lead to immediate dismissal of that member of staff.

- High Risk Customers: twice a year;
- Medium - and low-risk customers: Once a year.

Codego employees could face prosecution if it is proven that nobody did make a report to our own MLRO, even though one had reasonable grounds for suspicion. Codego has made a SAR template (see Annex 1) available to staff, all reports must be made using this template to ensure consistency.

From the moment, a suspicion of money laundering arises no further work will be carried out on the matter that gave rise to the suspicion. Neither commercial considerations nor the difficulty in responding to the client's enquiries on the matter shall be permitted to take precedence over Codego ' s legal obligations in this regard.

In such circumstances, the MLRO shall act with all possible speed to enable work to continue, and assist staff in any communications with the client affected.

As soon as a member of staff forms or becomes aware of a suspicion of money laundering, no further work is to be done on the matter giving rise to suspicion. If there is any likelihood of the client becoming aware that work has stopped, for example because an anticipated transaction has not gone through, the member of staff concerned must contact the MLRO for instructions on how to handle the matter with the client.

On receipt of a suspicion report, the MLRO shall:

- instruct the originator of the report and any other staff involved to cease work on the matter , giving rise to suspicion;
- decide in the shortest possible time whether all work for the client concerned should be stopped or whether other work that is not the cause of suspicion may continue, and advise relevant staff accordingly;
- assist all affected staff in handling the matter with the client so that no tipping- off offence is committed;
- When work for a client has been stopped, the MLRO shall carry out the evaluation of the suspicion report as quickly as possible to decide whether a disclosure must be made to the authorities;
- If the MLRO decides that there are no reasonable grounds to suspect money laundering, he will give consent for work to continue on his own authority.
- If the MLRO decides that a disclosure must be made, he will request consent to continue from NCA as quickly as possible.
- On giving consent to continue, either on his own authority or on receipt of notice of consent or implied consent from NCA, the MLRO will confirm this in writing to the affected staff.
- If consent is refused by NCA, the MLRO will take advice from NCA.

It is important that all employees and management are properly trained and remain vigilant of potential money laundering. The report should be made as soon as reasonably possible – this should normally be within the first 24 hours after discovery.

17 RECORD KEEPING

Entities have to retain the following documents and information in accordance with national law for the purpose of preventing, detecting and investigating, by competent authorities, possible money laundering or terrorist financing:

- In the case of customer due diligence, a copy of the documents and information which are necessary to comply with the customer due diligence requirements for a period of five years after the end of the business relationship with their customer or after the date of an occasional transaction;
- The supporting evidence and records of transactions, consisting of the original documents or copies admissible in judicial proceedings under the applicable national law, are necessary to identify transactions for a period of five years after the end of a business relationship with their customer or after the date of an occasional transaction.

CDD and transaction records
We will store records of all transactions for 5 years from the conclusion of the transaction on behalf of our customers or the end of the relationship. The records we must keep are:

- Copies of or references to the evidence of the customer's ID obtained under our CDD requirements; and
- The supporting evidence and records in respect of the business relationships and occasional transactions, which are subject of CDD or ongoing monitoring.

All records of CDD documentation are scanned and upload into our operational system linked in the customer's unique reference number.

Internal and External SAR records
As previously indicated, all internal reports will be kept on the SAR file as opposed to the customer file. The report will be kept for 5 (five) years. In addition to this, all SAR submitted, including correspondence with FCA or HMRC, will be kept for unlimited period of time.

Training records
The company maintains records of all AML training undertaken by staff, the date it was provided and the results of any tests if applicable. These records will be kept for 5 (five) years following the end of employment with the company.

Internal procedures, training and feedback
Entities have to implement group-wide policies and procedures, including data protection policies and policies and procedures for sharing information within the group for AML/CFT purposes. Those policies and procedures shall be implemented effectively at the level of branches and majority-owned subsidiaries in Member States and third countries.

Member States shall require that obliged entities that operate establishments in another Member State ensure that those establishments respect the national provisions of that other Member State transposing this Directive.

Audit results
All audit results must be kept for 5 (five) years following the date of the Board of Directors approval of them.

AML program audit and testing

To provide reasonable assurance that Codego AML program is functioning effectively, Codego conducts an audit of its AML program. an audit is conducting the on regular bases, at least every 12-18 months, if ML Risk assessment results will be rated as moderate, high or severe and every 18-24 months is the results will be rated as law and intermediate.

The main actions of the audit will cover:

- Examination of AML processes compliance with applicable Laws and regulation;
- Customer files review;
- Incoming/outgoing transactions review;
- Examination of representative documents to determine whether customer identification and verification procedures are being followed;
- Whether CDD and EDD are being properly applied;
- Whether the suspicious activity is being properly alerted investigated, escalated and reported;
- Whether severance of a customer relationship;
- Merchants including process into International Card Organizations blacklists (VMAS/MATCH) and scoring systems;
- Reporting process to International Card Organizations;
- Whether complaints process was initiated by the customer etc.

The audit results must be reported and an appropriate action plan must be established and presented directly to the Board of Directors.