Approved
by Resolution of the Director
dated “30” May 2023

COLLECT & EXCHANGE

Anti-Money Laundering, Counter Terrorist Financing, and Sanctions Policy

“30” May 2023

INTRODUCTION

1. Policy, Controls, and Procedures

This Anti-Money Laundering, Counter Terrorist Financing, and Sanctions Policy (the 'AML Policy') of Collect & Exchange Ltd. (the 'C&E', 'Collect & Exchange', the 'Company') is developed in compliance with the Astana International Financial Centre's ('AIFC') Anti-Money Laundering, Counter-Terrorist Financing, and Sanctions Rules No FR0008 of 2017[1] (the 'AIFC AML Rules'), the Law of the Republic of Kazakhstan 'On counteracting legalization (laundering) of proceeds obtained through criminal means and financing of terrorism' No 191-IV dated 28 August 2009[2] (the 'AML/CFT Law'), other relevant legislation of the Republic of Kazakhstan, AIFC Guidelines for Anti-Money Laundering/Countering Terrorist Financing Policies and Procedures[3], international conventions, and treaties ratified by the Republic of Kazakhstan, as well as best international standards and practices, including those of the Financial Action Task Force (the 'FATF').

It is essential that the C&E is able to identify, report, and take precautions to guard against money laundering and ensure sanctions compliance. We are required to abide by anti-money laundering (the 'AML') legislation that applies to our activities as a private company incorporated under the Acting Law of the AIFC and holding a license for Providing Money Services in the AIFC.

This AML Policy is a binding document throughout the C&E and for the entire C&E personnel. This AML Policy shall be reviewed from time to time and amended, if necessary, considering any changes in the Acting Law of the AIFC, national legislation of Kazakhstan, and international best standards and practices. In particular, this shall be conducted, without limitation, at least each quarter and discussed at the relevant Committee meeting, and be taken further steps, if relevant.

2. What is Money Laundering?

Money Laundering is the process where criminals attempt to hide and change the true identity of the proceeds of their crimes so that they appear legitimate i.e. where funds derived from the proceeds of criminal activity are given the appearance of being legitimate by being exchanged for 'clean' money.

The various stages are termed placement, layering, and integration:

1) placement – 'dirty money is placed directly into the financial system;
2) layering – the proceeds are moved through a series of financial transactions, making it harder to establish their origin;
3) integration – the money launderer creates a legitimate explanation for the funds' source, allowing them to be retained, invested in the legitimate economy, or to acquire assets and they re-enter the financial system.

Being involved in any of these activities is potentially criminal activity.

3. What is Terrorist Financing?

Terrorist financing is the following process:

[1] https://afsa.orderly.kz/articles/antimioneylauderingcountterrfinsancrules

[2] https://adilet.zan.kz/rus/docs/Z090000191_

[3] https://aifc.kz/uploads/Guidelines%20for%20AML_CTF%20Policies%20and%20Procedures.pdf

1) wilfully providing or collecting funds or other assets by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they will be used,
   (a) to carry out a terrorist act;
   (b) by an individual terrorist, or
   (c) by a terrorist organization; and
2) financing travel of persons who travel to a country that is not their home country (residence or nationality) for the purpose of the penetration, planning or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training.

4. What is Sanction?

The Sanction means a restrictive measure against a government, an organisation, a state body, a legal person, or a natural person to force it to behave in a particular way or as a punishment for not doing so.

The Sanctions, so far, are imposed by (a) United Nations' official decisions (b) states or relevant state authorities, and (c) companies and individuals.

Classification of Sanctions (a):[4]

(a) Economic - embargo, boycott, economic blockade, freezing of financial resources, including funds received or withdrawn from property owned or under the direct or indirect control of the object of sanctions, prohibition of investments in the economy of the object of sanctions, as well as the provision of financial, material, technical etc. help;
(b) Diplomatic - restriction or cancellation of high-level government visits or expulsion of diplomatic missions and staff; and
(c) Military - UN peacekeeping system. The use of armed force in such a case is mandatory and sanctioned by the UN Security Council.

Classification of Sanctions (b):[5]

a) Comprehensive - completely blocking any kind of trade and financial transactions with entire countries;
b) Personal - against natural and legal persons that are included in the list of specially designated persons and blocked persons (SDN - Specially Designate Nationals and Blocked Persons);
c) Sectorial - Sectoral Sanctions Identifications (SSI) list, affecting individual sectors of the economy and groups of persons; and
d) Addressed - restricting such transactions with individuals and/or companies.

It is essential that C&E's employees are aware of any sanctions imposed on potential customers, partners, and suppliers, that may affect the company's reputation and business activity overall. In this regard, the C&E encourages its personnel to familiarise themselves with the Sanctions Guidance, policies, lists, and approaches of the relevant jurisdictions[6].

5. Penalties

[4] According to the UN Charter

[5] According to the US OFAC

[6] The links for the relevant materials are as follows:
- AIFC Authority: https://aifc.kz/sanctions-compliance/
- UN Security Council: United Nations Security Council Consolidated List | United Nations Security Council
- UK (OFSI HM Treasury): General_Guidance_-_UK_Financial_Sanctions__Aug_2022_.pdf (publishing.service.gov.uk)
- US (OFAC): Home | Office of Foreign Assets Control (treasury.gov); (Document (millerchevalier.com)

The C&E personnel shall be aware of that any breach or ignoring the provisions of AIFC AML Rules, AML/CFT Law, and any other applicable laws and regulations are punishable by a fine, or even more, criminal liability may take place.

The maximum AML/CFT civil penalty can vary significantly. Civil and criminal penalties may be imposed against a company or any of its officers, directors, and employees. Penalties pursuant to civil action vary significantly based on the type of violation and the enforcement authority, a criminal penalty may lead to fine and short-term imprisonment.

However, if the violation is part of a pattern of conduct, and/or involves the violation of another criminal law, the penalty increases and would lead to a longer sentence and higher fine.

6. The AML Policy's Aim

This AML Policy's aim is to undertake a company-wide risk assessment and ensure that evidence of identity is obtained and retained as applicable to each customer based on the risk assessment undertaken (such as Business Risk Assessment, Customer Due Diligence, Transaction Due Diligence, etc., that are further elaborated in greater detail).

Overall, the risk assessment will be done on each new customer, transaction, our business relationship, and even on our new staff members, which will be assigned a risk rating based on their particular money laundering risks (such as location, PEP and sanctions status, etc.). In addition, enhanced due diligence will be undertaken where customers have been assigned a high-risk rating as well as in relation to the relevant transactions.

7. Importance of the Policy and the procedures set

This AML Policy is adopted to help our Company to combat money laundering and terrorist financing (the 'ML/TF') by stopping criminals from engaging in transactions to disguise the origins of funds connected to illegal activities, as well as to set the tone for the Company and reinforce a culture of compliance. Given the volume of transactions within the Company, to put our AML Policy into action toward preventing, detecting, investigating, and reporting suspicious transactions.

The C&E carries out the following Risk-Based Approaches (AML procedures) in order to implement the above-mentioned aims of the AML Policy:

- Business Risk Assessment (the '**BRA**');
- Know Your Customer (the '**KYC**');
- Customer Due Diligence (the '**CDD**');
- Transaction Due Diligence (the '**TDD**');
- Know Your Supplier (the '**KYS**'); and
- Know Your Employee (the '**KYE**').

To ensure adherence to the pertinent AML rules and regulations, it is imperative that these procedures be completed before beginning any activity.

8. THE RISK MANAGEMENT

Risk Management is the process used to identify the potential threats to the Company and to define the policies and procedures to eliminate or minimize the threats, as well as develop a strategy or guideline to monitor and review those identified risks.

Risk management of the Company includes the following processes (without limitations):

(a) Risk Identification is the first step to managing risks.The main goal of this stage is the early detection of potential future events that could negatively influence a company and its ability to achieve its goals.

(b) Analyze the Risk - once a risk has been identified it needs to be analyzed.

Determine the risk's extent first. Understanding the relationship between risk and various organizational characteristics is also crucial. It is vital to look at how many business operations the risk affects in order to gauge the risk's degree and severity. There are dangers that, if they materialize, might put the entire firm at risk, while other hazards will, according to the research, merely cause small annoyances.

When analyzing risks, the Company will identify and eliminate risks as follows:

- the risks relating to the geographical locations they operate in;
- the risk relating to the it's business activities;
- the risks relating to the products & services;
- the types of customers that it deals with.

(c) Risk Assessment is a systematic process that involves identifying, analyzing and controlling hazards and risks. The significance of risks depends on two factors:

- Its probability - chance of the risk happening;
- Its severity - the amount of loss or damage if the risk happened.

C&E must thus assess all risks based on both factors to determine which risks need immediate action and which risks can just be monitored for now.

(d) Risk treatment is a goal to select one or more options for addressing the risk and then implementing the option(s).

- minimize and/or remove the risk source;
- change the likelihood of the event associated with the risk;
- change the consequences of the event associated with the risk;
- manage the risks;
- apply strategies, policies, and procedures;
- put in place systems and controls.

(e) Risk monitoring and review:

- develop and carry out monitoring process;
- keep necessary records;
- review risk plan and AML/CTF program;
- do internal audit or assessment.

8.1. The Risk Factors

Company must consider the risk posed by any element or any combination of the elements listed below:

(a) Customers - followings are some indicators to identify ML/TF risk arises from different customers of the C&E:

- a new customer;
- a new customer who wants to carry out a large transaction;
- a customer or a group of customers making lots of transactions to the same individual or group;
- a customer whose identification is difficult to check;
- customers conducting their business relationship or transactions in unusual circumstances, such as, significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, frequent and unexplained movement of funds between institutions in various geographic locations;
- a corporate customer whose ownership structure is unusual and excessively complex;
- customers that are PEPs or influential persons or head of international organizations and their family members and close associates;
- customers submit account documentation showing an unclear ownership structure.

(b) Products and services:

- anonymous transaction;
- non-face to face business relationship or transaction;
- payment received from unknown or unrelated third parties;
- any new product & service developed;
- service to walk-in customers.

(c) Business practice/delivery methods or channels:

- online/internet;
- phone;
- email;
- third-party (referrals).

(d) Country and/or jurisdiction:

- any country subject to economic or trade sanctions;
- any country known to be a tax haven and identified by credible sources as providing funding or support for terrorist activities or that has designated terrorist organizations operating within their country;
- any country identified by FATF as not having an adequate AML&CFT system;
- any country identified as a destination of illicit financial flow and having a significant level of corruption and criminal activity.

8.2. Risk Rating and Scoring Matrixes

The Company uses the ratings and scoring tools to identify the level and possible consequences that may cause the business relationship with the potential customer and/or a customer's transaction.

The Risk Rating

Probability scale refers to the potential of an ML/FT risk occurring in the business for the particular risk being assessed. Four levels of risk are shown in the table below.

The potential customer will be given a preliminary risk classification based on its evaluated risk level after being identified, having their information cross-referenced with the PEP database and sanctions list, and responding to any further questions.

When the Company assessing risks, the following criteria are considered (without limitation):

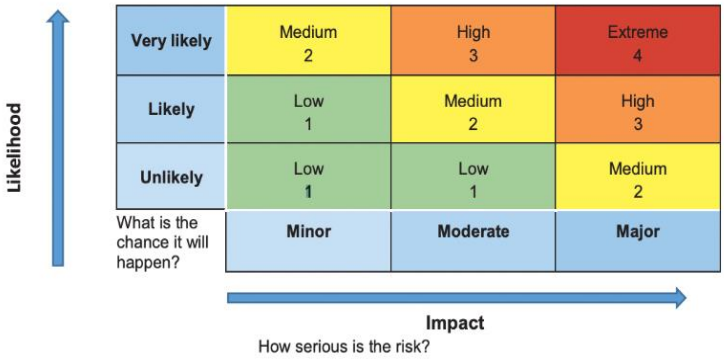
- how it may affect the business (if risks are not dealt with properly the C&E may suffer a financial loss from either a crime or through fines from a regulator);
- the risk that a particular transaction may result in the loss of life or property through a terrorist act;
- the risk that a particular transaction may result in funds being used for any of the predicate offenses such as corruption and bribery, counterfeiting currency, counterfeiting deeds and documents, human trafficking, banking offenses, narcotics offenses, psychotropic substance offenses, illegal arms trading, kidnapping, terrorism, theft, embezzlement, or fraud, forgery, extortion, smuggling of domestic and foreign currency and black marketing;
- the risk that a particular transaction may cause suffering due to the financing of illegal drugs;
- reputational risk, how it may affect the C&E if it is found to have (unknowingly) aided an illegal act, which may mean government sanctions and/or being shunned by the community of customers; and
- how it may affect the wider community of customers if it is found to have aided an illegal act; the community may get a bad reputation as well as the business.

The C&E establishes four customer risk levels to classify risks into those that are acceptable to the business and those that are considered unacceptable. The business avoids doing business with customers that pose an "unacceptable risk".

Three levels of impact are shown in the table below, but the C&E can have as many as they believe are necessary.

Consequence	Impact – of an ML/FT risk
Major	Huge consequences – major damage or effect. A serious terrorist act or large-scale money laundering
Moderate	Moderate level of money laundering or terrorism financing impact.
Minor	Minor or negligible consequences or effects.

How the Risk Rating is derived can be seen from the Risk Rating Matrix shown below.



Rating	Impact – of an ML/FT risk
4 Extreme	Risk almost sure to happen and/or to have very dire consequences. Response: Do not allow transactions to occur or reduce the risk to an acceptable level
3 High	Risk likely to happen and/or to have serious consequences. Response: Do not allow transaction until risk reduced
2 Medium	Possible this could happen and/or have moderate consequences. Response: May go ahead but preferably reduce risk.
1 Low	Unlikely to happen and/or have minor or negligible consequences. Response: Okay to go ahead.

8.3. Risk Scoring

The Risk Scoring Matrix for KYC consists of the following factors:

Factors	Scoring				
	Low (1)	Medium (10)	High (20-30)	Extreme/ Unacceptable (200)	

Country of incorporation	Low-level	1	-		High-level	20	-	
Legal Structure	Low-level	1	Medium level *(e.g. FZE; BVI; OU; etc.)*	10	High-level *(e.g. trusts; foundations; NV; etc.)*	20	-	
Business Activity	Low	1	Medium *(e.g. wholesale; pharmacy; IT; marketing; etc.)*	10	High *(e.g. online casinos; gambling; etc.)*	20	-	
Source of Wealth	Low	1	Medium l *(e.g. salary; business earnings; sale of property earnings; etc.)*	10	High *(e.g. family gift; no confirmation of source of wealth, etc.)*	20	-	

Relation of an authorised person/ Management/ UBO with PEP	No	-	-	-	Yes	30	-	
Affiliation with the Government	0 - 9%	1	10 % - 49%	10	50% - 100%	20	-	
Bank Statement presence	Yes	1	-	-	No	-	-	
Licence presence	Yes	1	Not applicable	-	No	-	-	
Sanctions relations	No	-	-	-	Yes	30	Yes (*imposition of a sanction, involvement in the financing of terrorism, corruption, etc.)*	200
Restrictions (penalties, prohibitions, etc.) of the relevant regulatory	No	-	-	-	Yes	30	Yes (*Financial crime, engaging in illegal activities, etc.)*	200
Whether the company is newly incorporated	More than 1 year	1	4 months - 1 year	10	Less than 3 months	20	-	
Whether the UBO, Director or Authorised signatory has some offences	No	-	-	-	Yes	30	-	

Key:

- ***Extreme:*** *more than 200*
- ***High Risk:*** *50-200*
- ***Medium Risk:*** *10-50*
- ***Low Risk:*** *0-10*

in case of suspicion of the applicant and / or detection of information of an inappropriate nature about the applicant (financial crime, imposition of a sanction, involvement in the financing of terrorism, corruption, engaging in illegal activities, etc.) and/or detection of an* ***explicit risk* *of non-compliance with AML CFT requirements and Company policies, regardless of the result of the risk scoring (but not limited to), AML Team decides to reject the applicant or the AML team member initiates a discussion at a meeting of the Compliance Committee.*

The outcome of the Compliance meeting is documented in the form of Minutes of the Compliance meeting, which are carefully prepared and signed by the Senior Executive Director.

In the event that the decision is made to reject the applicant's application, a member of the AML team promptly notifies the relevant regulatory authority, specifically the Financial Intelligence Unit (FIU), regarding the refusal to establish business relations with the applicant.

Example of a calculation according to the scoring system:

Factors	Customer	Scoring
Country of incorporation	High Risk (any high-risk country)	20
Legal Structure	Low	1
Business Activity	Low	1
Source of Wealth	Low	1
Relation of an authorised person/ Management/ UBO with PEP	Yes	30
Affiliation with the Government	10 % - 49%	10
Bank Statement presence	Yes	1
Licence presence	Yes	1
Sanctions relations	No	1
Restrictions (penalties, prohibitions, etc.) of the relevant regulatory	No	1
Whether the company is newly incorporated	More than 1 year	1
Whether the UBO, Director or Authorised signatory has some offences	No	1
Total:	**High Risk**	**79**

The Risk Scoring Matrix for KYT consists of the following factors:

Factors	Scoring			
	Low (1)	Medium (10)	High (20-30)	Extreme/Unacceptable (200)

Countries of the counterparty and the Customer's	Low	1	Medium	10	High	20		
Invoice presence	Yes	1	-		No			
Contract presence	Yes	1	-		No			
The subject of the contract	Low-level	1	Medium *(e.g. purchase and sale; engineering services; legal services etc.)*	10	High *(e.g. FX Options; wealth management; alternative investments etc.)*	20		
Risk level of the Customer	Low-level	1	Medium	10	High	30		
Whether the transaction is subject to reporting	No		-		Yes	30		
Counterparty status (PEP/SOE/not)	No		-		Yes	30		
Bank jurisdiction (counterparty)	Low-level	1	Medium	10	High	20		
Sanctions relations (counterparty)	No		-		Yes	30	(*imposition of a sanction, involvement in the financing of terrorism, corruption, etc.)*	200
Restrictions of the relevant authority (counterparty)	Yes	1	-		No		(*Financial crime, engaging in illegal activities, etc.)*	
the origin of the cryptocurrency	Yes	1	-		No			

Key:

- ***Extreme:*** *more than 200*
- ***High Risk:*** *50-200*
- ***Medium Risk:*** *10-50*
- ***Low Risk:*** *0-10*

Example of a calculation according to the scoring system:

Factors	Customer	Scoring

Countries of the counterparty and the Customer's	High	20
Invoice presence	Yes	1
Contract presence	Yes	1
The subject of the contract	Low	1

Risk level of the Customer	High	30
Whether the transaction is subject to reporting	No	1
Counterparty status (PEP/SOE/not)	No	1
Bank jurisdiction (counterparty)	Low	1
Sanctions relations (counterparty)	No	1
Restrictions of the relevant authority (counterparty)	Yes	1
the origin of the cryptocurrency	Yes	1
Total:	**High Risk**	**59**

The total score can be changed, if the AML team finds something suspicious in the case.

in case of suspicion of the Customer and / or detection of information of an inappropriate nature about the Customer (financial crime, imposition of a sanction, involvement in the financing of terrorism, corruption, engaging in illegal activities, etc.) and/or detection of an **explicit risk of non-compliance with AML CFT requirements and Company policies, regardless of the result of the risk scoring (but not limited to), AML Team decides to reject the transaction or the AML Team member initiates a discussion at a meeting of the Compliance Committee.*

The outcome of the Compliance meeting is documented in the form of Minutes of the Compliance meeting, which are carefully prepared and signed by the Senior Executive Director.

In the event that the decision is made to reject the transaction, a member of the AML team promptly notifies the relevant regulatory authority, specifically the Financial Intelligence Unit (FIU), regarding the suspicious transaction.

8.4. Risk Mitigation (systems and controls)

8.4.1. If the AML Team considers the Customer as High-Risk, all of the transactions that will be made by this Customer will be considered by EDD.
8.4.2. If the AML Team initiates the internal investigation on the transaction, and the results of such investigation will be negative, the Customer should be rejected from the C&E platform and reported to FIU;
8.4.3. If the AML Team finds the close relations of the applicant with PEP, the applicant should be discussed on the Compliance Committee;
8.4.4. C&E has the register of “Black listed” applicants, that were rejected from the C&E platform by the order of the Compliance Committee to ensure that C&E won’t consider such applicants in the future.

9. THE RISK-BASED APPROACH

The risk-based approach (the "RBA") to AML/CFT means that obliged entities should have an understanding of the ML/TF risks to which they are exposed and apply AML/CFT measures in a manner and to an extent which would ensure mitigation of these risks.

The risk assessment, therefore, serves as the foundation for the risk-sensitive application of AML/CFT measures. Obligated entities should study and endeavor to understand how the AML/CFT risks they find influence them. RBA is not a "zero failure" strategy because there may be instances in which an institution has taken all reasonable precautions to identify and reduce AML/CFT risks but is nevertheless exploited for money laundering or terrorist financing.

The RBA to customer due diligence is a requirement of the AML/CFT legislation, which means that the company must evaluate the money laundering risks posed by each customer entity and obtain customer due diligence in accordance.

9.1. Obligations of the Risk-Based Approach

General Duty
The C&E is required to take appropriate steps to identify and assess the risks of ML/FT to which our business may be exposed.

Nature and size of business
In deciding what steps are appropriate to identify and assess the risks of money laundering to which the business is exposed, C&E must consider the size (number of employees, revenue or market capitalisation) and nature of the business and the complexity of its activities.

To identify and assess the risks of money laundering and terrorist financing C&E undertake the following:

(a) a business risk assessment;
(b) a customer risk assessment.

New products and business practices
If applicable, the Company will identify and assess the ML/TF risks before the launch or use of any new products and new business practices, including new delivery mechanisms and the use of new or developing technologies for both new and pre-existing products.

10. BUSINESS RISK ASSESSMENT (THE ‘BRA’)

In order to detect, assess, monitor, and manage the risk of fraud, bribery and corruption, and money laundering, the company has been conducting a business-wide financial crime risk assessment that takes into consideration business products, services, channels, customs, and geographic regions.

The Director/CEO may review the risk assessment, systems, and controls at least once per year, in conjunction with any changes to the business or management.

In the proper way to comply with the Guidance (Requirements) applicable to the Rules of Internal Control for the purposes of combating the legislation (laundering of proceeds from crime and the financing of terrorism), the Company will establish clear plans to implement

any improvements necessary.

The financial crime risk assessment is both qualitative and quantitative and will address hazards at least at the company product, service, channel, customer, and geographic level.

10.1. Risk factors to be considered when undertaking a BRA

The C&E will carry out BRA and consider the following factors:

(a) the countries or geographic areas in which it operates;
(b) the customer's products or services;
(c) the customers' transactions;
(d) the customers' delivery mechanisms, channels, and partners;
(e) the development of new products and new business practices, including new delivery mechanisms, channels, and partners; and
(f) the use of new or developing technologies for both new and pre-existing products.

10.2. Use of the BRA

The C&E will use the information obtained from the BRA for the following:

(g) develop and maintain its AML Policy, procedures, systems and controls.
(h) ensure that the AML Policy, procedures, systems and controls adequately mitigate the risks identified;
(i) assess the effectiveness of the AML Policy, procedures, systems and controls;
(j) assist in the allocation and prioritisation of AML resources; and
(k) assist in the carrying out of customer risk assessments as set out below.

The business will put the BRA in place to have procedures in place for identifying and evaluating money laundering threats. Then, in proportion to the Company's exposure to certain money laundering concerns, it will monitor, manage, and reduce the risks.

10.3. Financial crime risks

A financial crime risk assessment is a systematic, step-by-step process of analyzing vulnerability to financial crime. To perform a financial risk assessment, C&E will identify its risks:

(a) Money Laundering;
(b) Terrorist Financing;
(c) Fraud;
(d) Bribery and corruption;
(e) Embezzlement;
(f) Personal purchases; and
(g) Theft;
(h) Tax Evasion;
(i) Cybercrime;

Prevention of such risks:

STEP 1	STEP 2	STEP 3

Identify inherent risks	Identify and assess controls	Determine residual risks
• **Customers** • **Products** • **Channels** • **Geography** • **Qualitative**	• **Policies** • **Processes** • **Training** • **Systems** • **KYC/Due diligence** • **Record keeping** • **Investigations** • **STR Filings**	• **Recommendations** • **Risk appetite**

Customer due diligence: C&E must be able to establish and verify the identities of their customers and the beneficial ownership of customer entities. Higher-risk customers should be subject to enhanced due diligence (EDD) measures.

Transaction monitoring: C&E monitors its customers' transactions for indications that they are attempting to launder money. Unusual transaction patterns and amounts, or transactions that do not match a customer's risk profile, represent money laundering red flags.

Sanctions screening: C&E must ensure it does not facilitate the criminal activities of customers that are subject to international sanctions and other restrictions. Accordingly, C&E should screen customers and transactions against the relevant international sanctions and watch lists.

PEP screening: C&E must screen its customers to establish politically exposed person status and determine whether they present a higher AML risk. PEP screening includes customers' relatives and close associates.

Adverse media monitoring: Adverse or negative media stories often indicate that customers are involved in criminal activities and present a higher AML/CFT risk. C&E should monitor for adverse information from both traditional screen and print news media and online sources.

11. CUSTOMER RISK ASSESSMENT ('CRA')

11.1. Assessing customer money laundering risks

The C&E will take the following steps:

(a) undertake a risk-based assessment of every customer; and
(b) assign the customer a risk rating proportionate to the customer's money laundering risks.

11.2. Timing of the CRA

C&E will complete the CRA before undertaking Customer Due Diligence for new customers, and where, for an existing customer, there is a material change in circumstances.

An individual or business will be regarded as a customer when the onboarding process

begins, but no work will be completed until the business connection has been formally established by the execution of an engagement letter or customer-Company engagement agreement.

11.3. Conducting the CRA

C&E will undertake the following risk-based assessment which must:

(c) identify the customer and any beneficial owner(s);
(d) obtain information on the purpose and intended nature of the business relationship;
(e) the type of customer, its ownership and control structure, and its beneficial ownership (if any);
(f) the nature of the customer's business relationship with the Company;
(g) the customer's country of origin, residence, nationality, place of incorporation, or place of business;
(h) the relevant product, service, or transaction; and
(i) the outputs of the BRA set out above.

The Company will use the CRA findings to determine the level of CDD that should be applied in respect of each customer and beneficial owner.

Depending on the outcome of the CRA, relevant action will need to be undertaken.

11.4. Identification of Politically Exposed Persons (the 'PEP')

A PEP is a natural person (including a family member or known associate) who is or has been entrusted with a prominent public function, including but not limited to: a head of state or of government, senior politician, member of a legislative or constitutional assembly, senior government official, senior judicial official, senior military officer, ambassador, senior person in an international organisation, senior executive of a state-owned entity, a senior political party official, or an individual who has been entrusted with similar functions such as a director or a deputy director; at an international, national, or regional level.
This definition does not include middle-ranking or more junior individuals in the above categories.

The FATF defines a politically exposed person as *"an individual who is or has been entrusted with a prominent public function"*. Due to their position and influence, it is recognized that many PEPs are in roles that potentially can be abused for the purpose of laundering illicit funds or other and related predicate offences, including corruption and bribery, as well as conducting activity related to terrorist financing.

The AML team member should also consider additional risk factors for PEP when screening, which should include at a minimum the following:
a) any particular concern over the country where the particular PEP is from, taking into account his/her position;
b) any unexplained sources of wealth or income (i.e. a value of assets owned not in line with the PEP's income level);
c) expected receipts of large sums from governmental bodies or state-owned entities;
d) source of wealth described as commission earned on government contracts;
e) request by the PEP to associate any form of secrecy with a transaction; and
f) use of accounts at a government-owned bank or of government accounts as the source of funds in a transaction.

The Company will determine whether a customer or a beneficial owner is a PEP. If a transaction includes a PEP, sufficient evidence must be obtained to provide reasonable grounds for believing that the relationship with such PEP will not give rise to any risks of ML/TF. Anyone who is a PEP should also be reported to the MLRO for a determination on whether to proceed with such a customer. The process of establishing a business relationship when the customer is a PEP is described in clause 13.2.7.

11.5. Prohibition on relationships with Shell Banks

The Company undertakes not to establish or maintain a business relationship with Shell Banks.

11.6. Customer's Risk Level Identification

The C&E uses the following Risk Level Identification of customers:

Table with the Risk Levels

GREEN ZONE: Low Risk[7]	**YELLOW ZONE: Medium Risk**	**RED ZONE: High Risk**
The Risk level of the Customer can be low only if the Customer is: ● Kazakhstani State Enterprises; ● Kazakhstani State Authorities; ● Public Companies, which shares listed at KASE and/or AIX.	The Risk level of the Customer can be Medium in the following cases: ● The country of incorporation is not related to sanctions; ● The business activity of the Company has a medium risk of ML/FT; ● No bad adverse media in open sources about the Customer or/and about its employees, UBOs.	The Risk level of the Customer can be High in the following cases: ● The country of incorporation is sanctions related (see Annex 1); ● The country of incorporation is offshore jurisdiction; ● Identified PEP in the Customer's structure; ● Complex organisational structure (see Annex 1) ● High-Risk Business Activity (see Annex 1); ● Found negative media about the Customer or/and about its employees, UBOs; ● AML Personnel has some doubts about the reliability of Customer data; ● Religious associations/foundations ● The Branch or the representative office is located in a

[7] However, the C&E does not have and will not have any business activities with Kazakhstani natural and legal persons, including state authorities, state owned public companies, etc.

		sanctions-related country

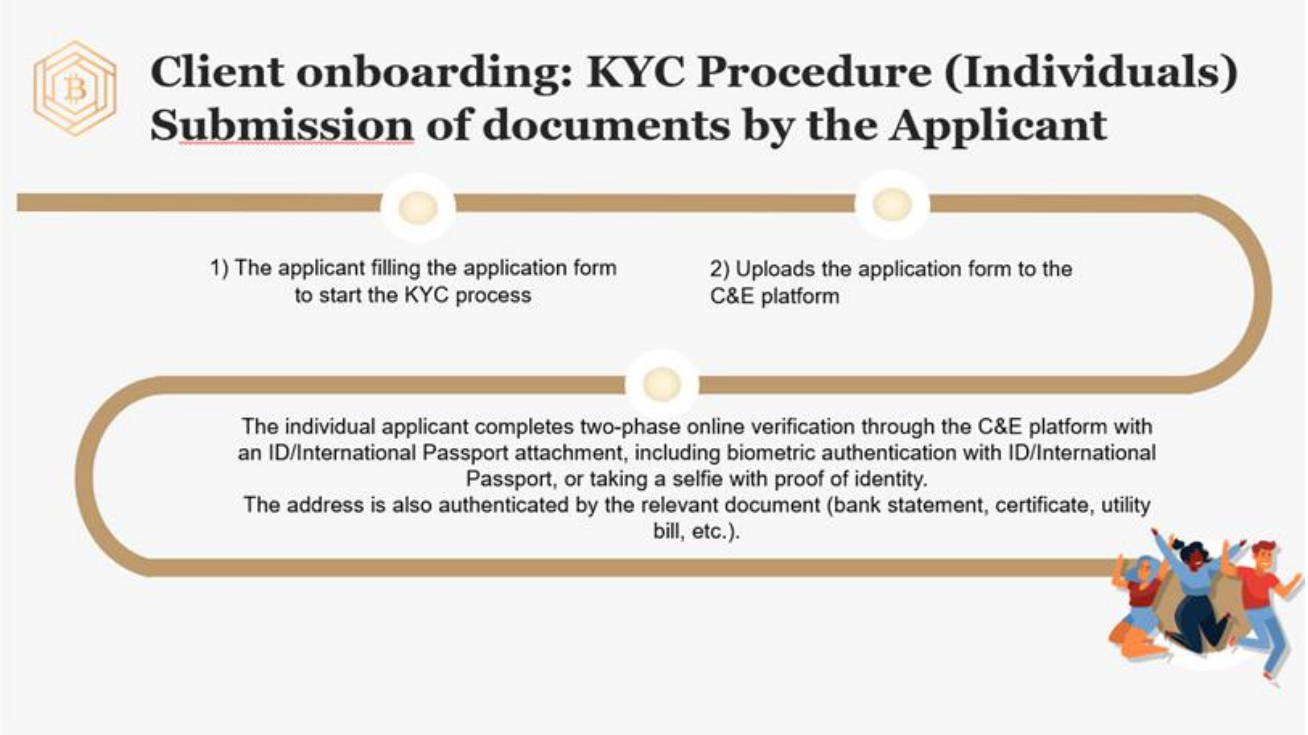
12. KNOW YOUR CUSTOMER (THE 'KYC')

12.1. The KYC Process

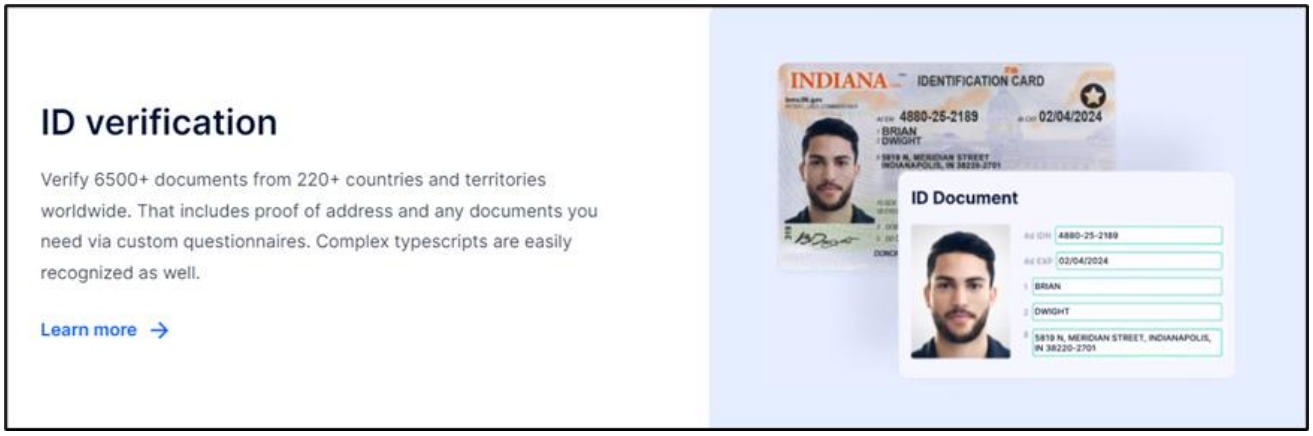
The KYC hereof specifies the checks that are carried out at the start of a customer relationship to identify and verify that such customers are who they say they are. It allows the Company to create a customer's risk profile by retrieving their data before initiating a business relationship in a digital onboarding process, on the Platform of C&E, by collecting their personal data and identity documents.

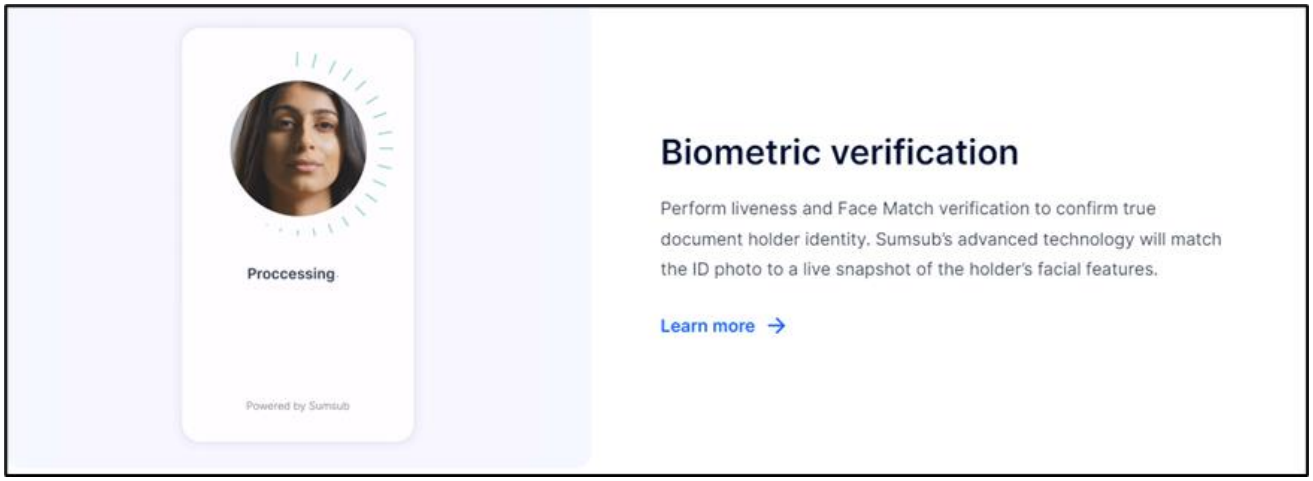
12.1.1. The steps of KYC that should be followed as illustrated and described below:

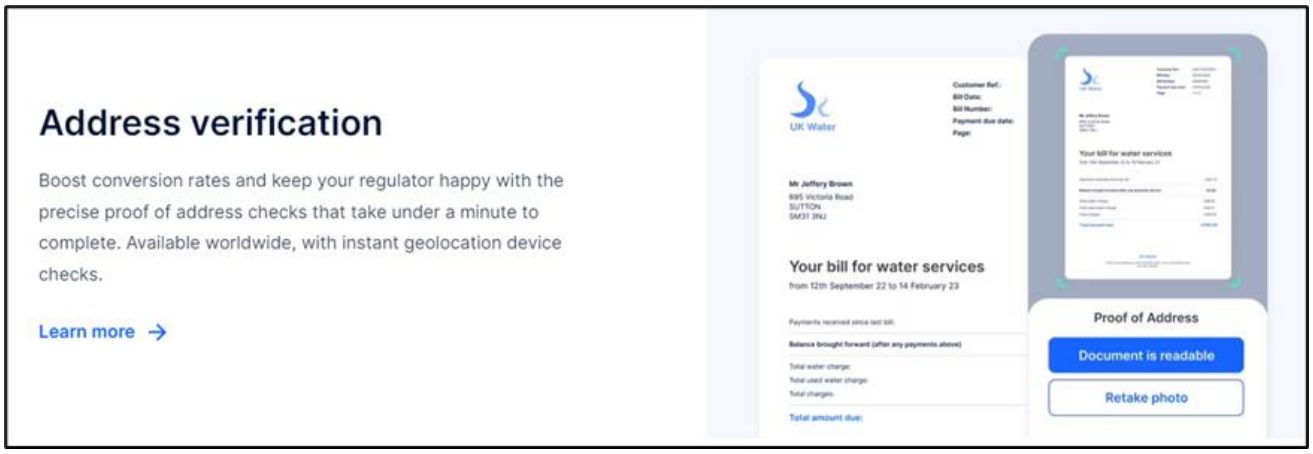
12.1.1.1. The applicant completes the following process to complete the KYC process (Individuals):



(a) The individual applicant filling the application form to start the KYC process;
(b) Uploads the application form to the C&E platform;
(c) The individual applicant completes two-phase online verification through the C&E platform with an ID/International Passport attachment, including biometric authentication with ID/International Passport, or taking a selfie with proof of identity. The address is also authenticated by the relevant document (bank statement, certificate, utility bill, etc.).







12.1.1.2. The member of the AML team conducts the following KYC process (Individuals):

(a) receives the documents of the applicant from the AML tool (Online Platform) (in the form of a report from the corresponding platform with an identity card / international passport attached, and documents confirming the address authentication;

sumsub

ONLINE SCREENING REPORT

ABIANOV RAMIS

ABIANOV RAMIS
Inspection report for May 12, 2023
Created for Collect&Pay Ltd

Verification Status APPROVED

Key findings

- **Document Review Check**
  - Images quality
  - Security features
  - Template
  - Fonts
- **Fraudulent Patterns**
- **Data Validation**
  - Document has not been recorded as expired, lost, stolen or compromised
  - Document hasn't been found on our blocklist
  - Data comparison
- **Compromised persons / organizations**
  - Warnings
  - Sanctions
  - Politically exposed persons (PEP)
  - Adverse media
- **Facial Check**
  - Face detection
  - Face match (score: 0.84)
  - Liveness check

Profile data

ID: 645e29fd0f0cea51fdd16f3d
Created for: Collect&Pay Ltd

Profile created: May 12, 2023
Last screened: May 12, 2023
Ongoing monitoring: Not active
Requested documents:
- ID card, Passport, Residence permit, Driver's license
- Selfie

Events

Approved (Took a minute)
Level name: basic-kyc-level
Backoffice:
May 12, 2023 12:01 PM (GMT+0)

a minute

Pending
Applicant:
May 12, 2023 12:00 PM (GMT+0)
macOS — Safari
Russia, Kazan'
91.225.77.119

19 seconds

Selfie
ID: 1920977398
Applicant:
May 12, 2023 12:00 PM (GMT+0)
macOS — Safari
Russia, Kazan'
91.225.77.119

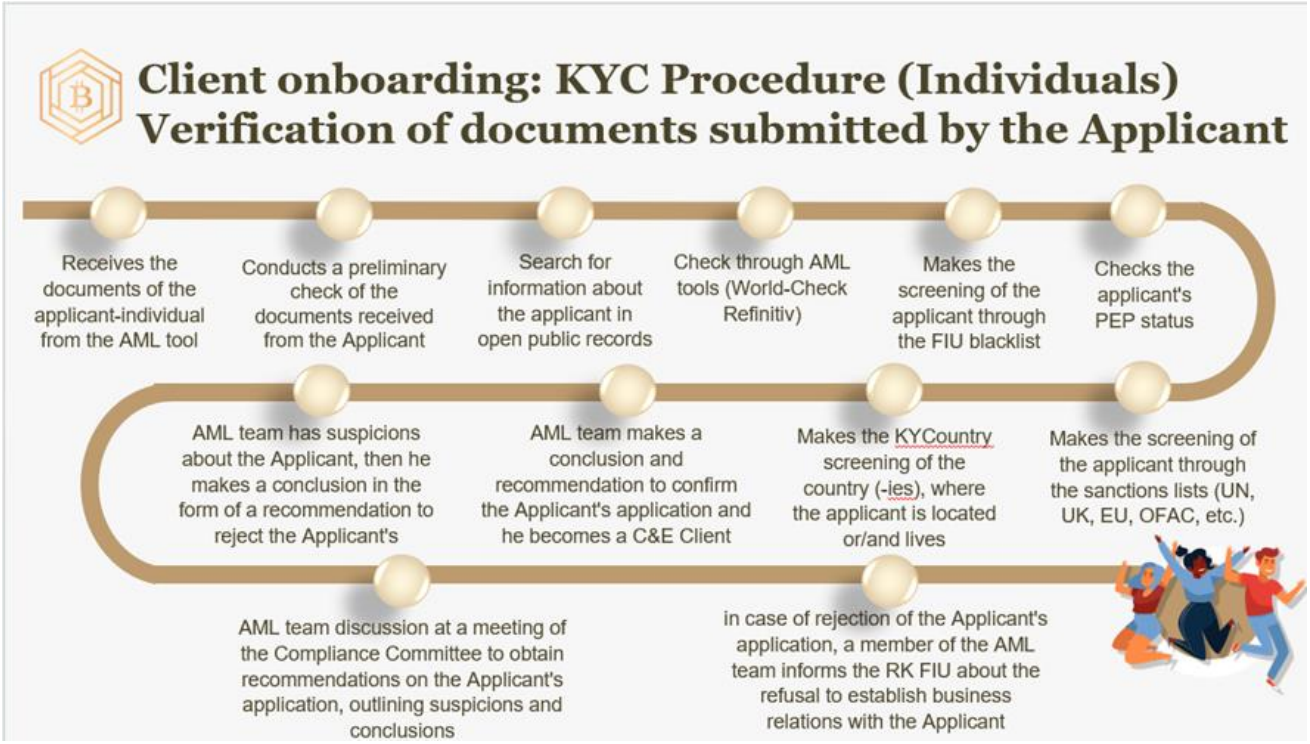
(b) conducts a preliminary check of the documents received from the applicant (identity card / international passport, and documents confirming the authentication of the address), the process of this check also includes the following procedures:

- search for information about the applicant in open public records (Google, Yandex and various social networks, articles in the media, etc.);
- check through AML tools (World-Check Refinitiv)[8];
- makes the screening of the applicant through the FIU blacklist[9];

[8] https://www.world-check.com/frontend/login/
[9] Kazakhstan FIU: https://afmrk.gov.kz/the-list-of-organizations-and-individuals-associa/

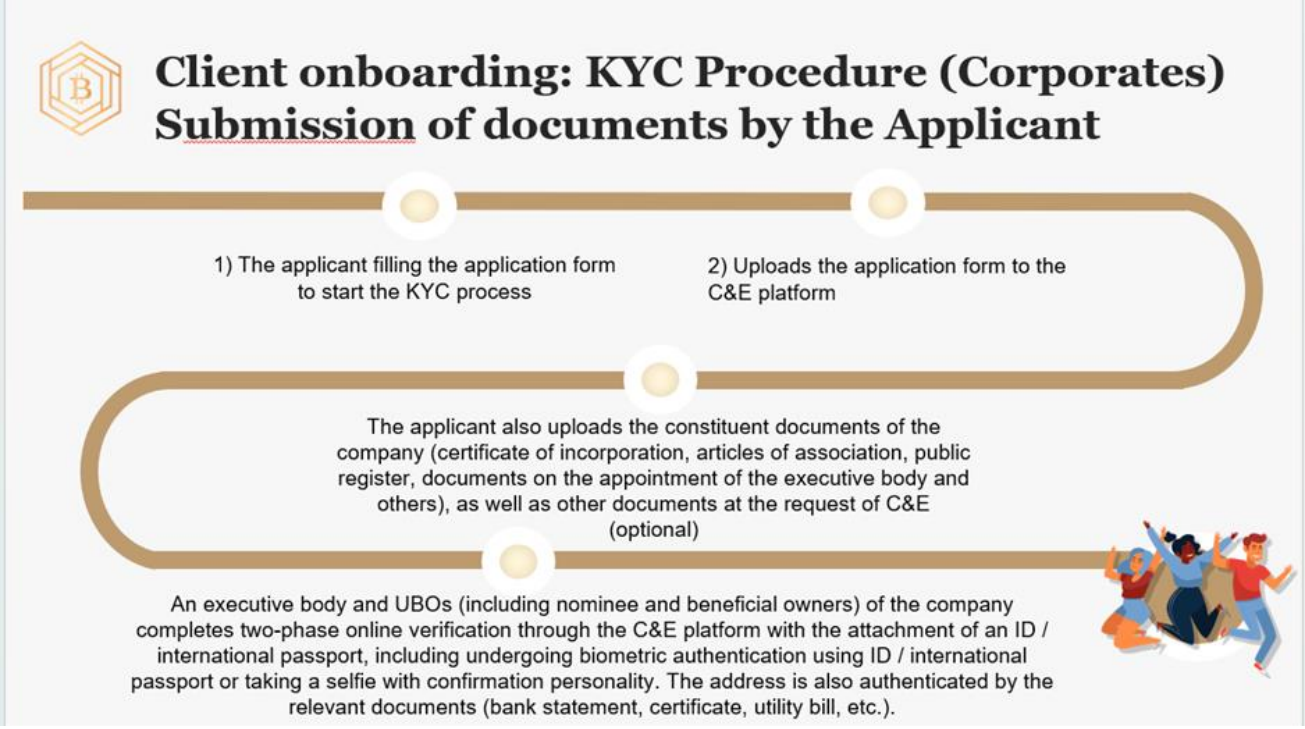
- makes the screening of the applicant through the sanctions lists (UN, UK, EU, OFAC, etc.);
- makes the KYCountry screening of the country (-ies), where the applicant is located or/and lives[10];
- checks the applicant's PEP status (if PEP, C&E needs the written approval of the CEO, by email can also be sent or the protocol of the committee);

(c) if all the required documents from the applicant have been provided, a member of the AML team makes a conclusion in the form of a recommendation to confirm the applicant's application and the applicant becomes a C&E Customer;
(d) if all the necessary documents from the applicant have been provided, but a member of the AML team has suspicions about the applicant, then the member of the AML team makes a conclusion in the form of a recommendation to reject the applicant's application with the provision of an appropriate conclusion;
(e) the member of the AML team initiates discussion at a meeting of the Compliance Committee to obtain further recommendations on the applicant's application, outlining suspicions and conclusions;
(f) In case of rejection of the applicant's application, a member of the AML team informs the RK FIU about the refusal to establish business relations with the applicant.



12.1.1.3. The applicant completes the following process to complete the KYC process (Corporates):

[10] The risk level of a country is defined considering the FATF recommendations, UN and other relevant countries' lists and reflected on the KYCountry Board (internal online platform) of the C&E, which is frequently updated from time to time.



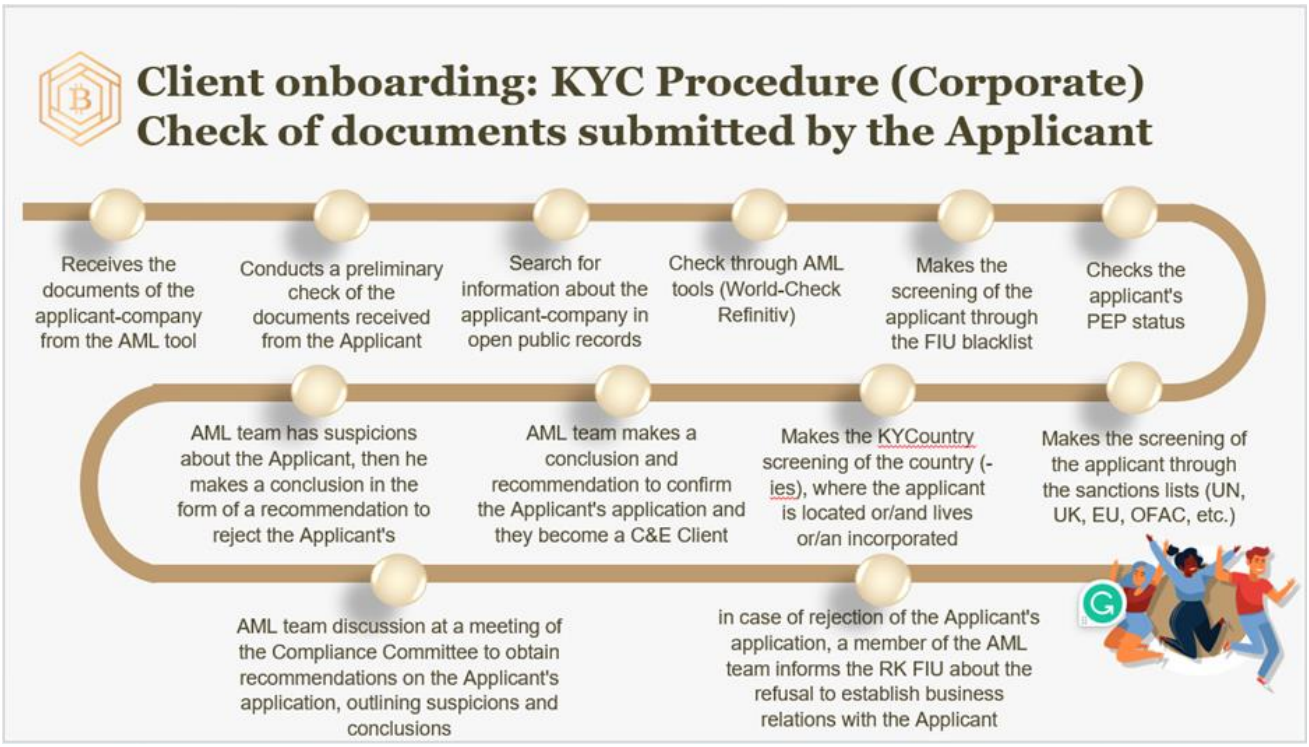
(a) The applicant filling the application form to start the KYC process;
(b) Uploads the application form to the C&E platform;
(c) The applicant also uploads the constituent documents of the Company (certificate of incorporation, articles of association, public register, documents on the appointment of the executive body and others), as well as other documents at the request of C&E (optional);
(d) An executive body and UBOs (including nominee and beneficial owners) of the company completes two-phase online verification through the C&E platform with the attachment of an ID / international passport, including undergoing biometric authentication using ID / international passport or taking a selfie with confirmation personality. The address is also authenticated by the relevant documents (bank statement, certificate, utility bill, etc.).

12.1.1.4. The member of the AML team conducts the following KYC process (Corporates):

(a) receives the documents of the applicant from the AML tool (Online Platform) (in the form of a report from the corresponding platform with an identity card / international passport attached, and documents confirming the address authentication and other founding documents of the applicant.
(b) conducts a preliminary check of the documents received from the applicant (identity card / international passport, and documents confirming the authentication of the address), constituent documents for the applicant the process of this check also includes the following procedures:
- search for information about the applicant (company, executive body, beneficial owners and other persons of the company) in open public records (Google, Yandex, and various social networks, articles in the media, etc.);
- check through AML tools (World-Check Refinitiv);
- makes the screening of the applicant through the FIU blacklist;
- makes the screening of the applicant through the sanctions lists (UN, UK, EU, OFAC, etc.);

- makes the KYCountry screening of the country (-ies), where the applicant is located or/and lives or/and incorporated;
- checks the applicant's PEP status (if PEP, C&E needs the written approval of the CEO, by email can also be sent or the protocol of the committee);

(c) if all the required documents from the applicant-company have been provided, a member of the AML team makes a conclusion in the form of a recommendation to confirm the applicant's application and the applicant becomes a C&E Customer;
(d) if all the necessary documents from the applicant have been provided, but a member of the AML team has suspicions about the applicant, then the member of the AML team makes a conclusion in the form of a recommendation to reject the applicant's application with the provision of an appropriate conclusion;
(e) the member of the AML team initiates discussion at a meeting of the Compliance Committee to obtain further recommendations on the applicant's application, outlining suspicions and conclusions;
(f) In case of rejection of the applicant's application, a member of the AML team informs the RK FIU about the refusal to establish business relations with the applicant.



12.2. Conducting KYC

The detailed KYC Identification Program is set out in Annex 1 to this AML Policy.

12.3. Additional KYC Required in certain circumstances

In any of the situations set out in the Enhanced Due Diligence part of our AML Policy, and subject to discussion with the MLRO, the AML team must carry out additional due diligence.

Firstly, an electronic check against the relevant entity or individual shall be carried out. These are online checks which verify information obtained as part of the KYC due diligence (Online Check). The online check involves public registers that are available.

Secondly, the following additional individuals shall be identified:

- **Partnerships**. Identify every individual partner. To do this, the requirements for identifying individuals as set out in Annex 1 shall be followed.
- **Trusts**. Identify all the beneficial owners. To do this, the requirements for identifying individuals as set out in Annex 1 shall be followed.

Thirdly, where the transaction involves a group of entities, the AML team must obtain a corporate structure chart and verify this chart using an Online Check and/or publicly available information, in the same way, that all the relevant entities within a complex group structure as provided in Annex 1.

13. THE CUSTOMER DUE DILIGENCE (THE 'CDD')

The **CDD** is the process where relevant information about the customer is collected and evaluated for any potential risk for the Company or ML/TF activities. CDD checks must be performed on an ongoing basis for as long as there is a customer relationship, requiring a record of transactions to be kept and updated.

The CDD is essential as it is important that we understand who we are dealing with and what they do.

13.1. Obligation to undertake CDD

The C&E will undertake CDD:

1) for each of the Company's customer's verification, which includes:
   a) verifying the identity of the customer and of any beneficial owner based on original or properly certified documents, data, or information issued by or obtained from a reliable and independent source;
   b) getting information on the purpose and intended nature of the business relationship;
   c) understanding the customer's sources of funds;
   d) understanding the customer's sources of wealth; and
   e) undertaking ongoing due diligence of the customer business relationship.

2) C&E must:
   a) conduct CDD under AIFC AML Rules for each of its customers including when the customer is carrying out occasional transactions the value of which singularly or in several linked operations (whether at the time or later), equal to or exceed USD 15,000; and
   b) in addition to mandatory CDD, C&E must conduct Enhanced Due Diligence (the 'EDD') in respect of the following:
      i. each customer it has assigned as High Risk;
      ii. business relationships and transactions with persons from countries with high geographical risk factors.

The C&E's broad objective is knowing at the outset of the relationship who our customers (and, where relevant, beneficial owners) are, where they operate, what they do, and their expected level of activity. The Company will then consider how the customer's financial behaviour profile builds up over time, and identify transactions or activity that may be suspicious.

The initial stage of the CDD is to be performed on the basis of the provided information of an

external person under the C&E Questionnaire, which is already integrated into the C&E Platform during the onboarding of an external person, along with other questions regarding registration details of an external person (corporate structure; authorised signatory details; director details; ultimate beneficiary details; etc). However, the Questionnaire or its relevant part may be provided separately to an external person in other cases if necessary. The Questionnaire is indicated in Annex 7.

13.2. Timing of CDD

13.2.1. Establishment of the business relationship

The company must undertake CDD:

a) when establishing a business relationship with a customer; and
b) after establishing a business relationship with a customer as set out below.

13.2.2. After the establishment of a business relationship

Appropriate CDD must be undertaken if, at any time:

(a) in relation to an existing customer, the company doubts the veracity or adequacy of documents, data or information obtained for the purposes of CDD;
(b) it suspects money laundering; or
(c) there is a change in the risk rating applied by the company to an existing customer, or it is otherwise warranted by a change in circumstances of the customer.

13.2.3. Verification of customers:

The MLRO of the Company must conduct CDD:

(a) Verify the identity of the customer;
(b) Verify the identity of any beneficial owners;
(c) Understand the customer’s sources of funds;
(d) Understand the customer’s sources of wealth;
(e) Conduct ongoing due diligence of the relationship with the customer.

For higher-risk situations, identification information is to be independently verified, using both public and non-public sources.

13.2.4. C&E will obtain customer identification information for a natural person which includes the following:

(a) full name (including any alias);
(b) date of birth;
(c) nationality;
(d) legal domicile; and
(e) current residential address (not a P.O. box).

Items (a) to (c) above should be obtained from a current valid passport or an official identification document that includes a photograph. The domicile is a person's permanent home and with which he has the closest ties or which is his place of origin.

13.2.5. C&E will obtain customer identification information for a legal person which includes the following:

(a) full business name and any trading name;
(b) registered or business address;
(c) date of incorporation or registration;
(d) place of incorporation or registration; and copy of the certificate of incorporation or registration;
(e) a valid commercial or professional licence;
(f) the identity of the directors, partners, trustees or equivalent persons with executive authority of the legal person; and
(g) for a trust, a certified copy of the trust deed to ascertain the nature and purpose of the trust and documentary evidence of the appointment of the current trustees.

For higher-risk situations, identification information is to be independently verified, using both public and non-public sources.

13.2.6. Electronic verification of identification documentation:

(a) the C&E may rely on an electronic verification of identification documentation if it complies with the RBA and other requirements of the applied rules.
(b) the C&E will make and keep a record that clearly demonstrates the basis on which it relies on the electronic verification of identification documentation.

13.2.7. The customer is a Politically Exposed Person

C&E is committed to ensure where a customer, or a beneficial owner of the customer, is a PEP the Company also:

(a) increases the degree and nature of monitoring of the business relationship, in order to determine whether the customer's transactions or activities appear unusual or suspicious; and
(b) obtains the approval of the Director/CEO to commence a business relationship with the customer.

Individuals who have had a high political profile, hold or have held a public office, can pose a higher money laundering risk to the company as their position may make them vulnerable to corruption. This risk also extends to members of their families and their close associates. PEP status itself does not incriminate individuals or entities. It does, however, put the C&E's customer into a higher risk category.

In Annex 1 to this AML Policy C&E has established KYC identification requirement procedures – required in all situations when conducting a CDD. The requirements are based on the type of legal entity/individual and are to be updated with the policy to reflect the changes to the applicable regulations as well as the established practice.

When checking and identifying a person for belonging to the PEP, a member of the AML team must verify the identity through the World Check system, but it must be borne in mind that the use of these databases does not replace traditional CDD processes (e.g. understanding the occupation and employer of a person), it is also necessary to conduct a search for information in public sources, social networks and apply other available information.

An integral part will be the use and search of information in relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations to assess which countries are most vulnerable to corruption (an

example of which is Transparency International's "Corruption Perceptions Index", which ranks countries according to their perceived level of corruption).

It is important to be vigilant in cases where either the country with which the client has business, or the business/industrial sector is more vulnerable to corruption.

13.3. On-going CDD

13.3.1. On-going obligation

The C&E will conduct ongoing CDD, using a risk-based approach by the following:

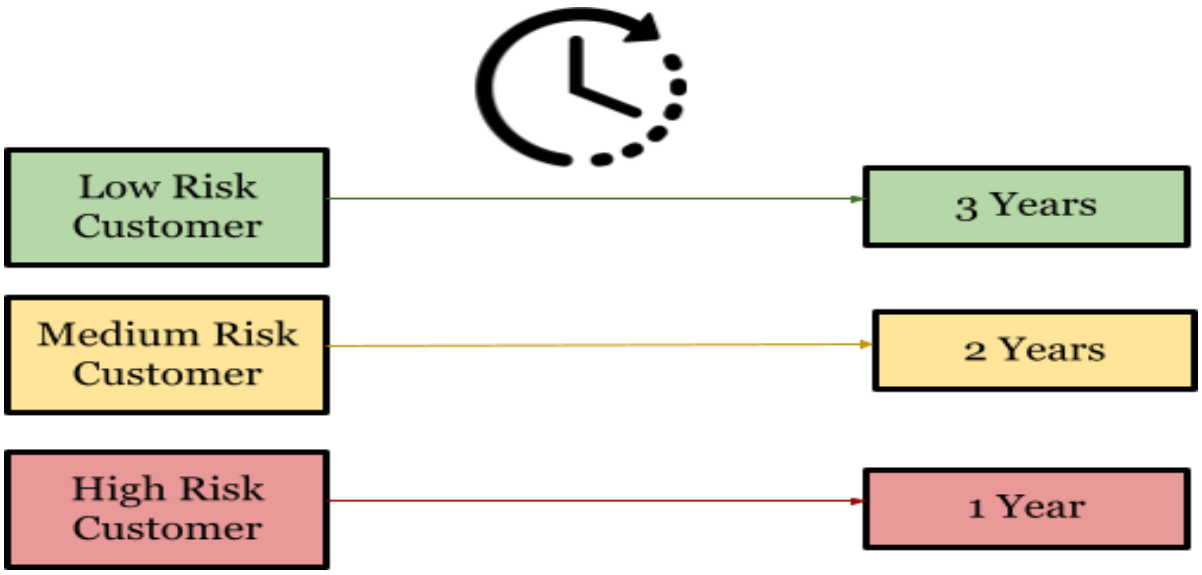
a) monitoring and reviewing transactions undertaken during the course of the customer relationship;
b) ensuring transactions are consistent with the customer and its business;
c) enquiring into the background and purpose of the transactions;
d) studying complex and unusual transactions;
e) studying transactions with no apparent or visible economic or legitimate purpose;
f) reviewing and updating CDD information;
g) reviewing the AML risk of the customer.

C&E will undertake a review, particularly when:

a) the company changes CDD documentation requirements;
b) an unusual transaction with a customer is expected to take place;
c) there is a material change in the business relationship with the customer; or
d) there is a material change in the nature or ownership of the customer.

13.3.2. Timing of ongoing monitoring:

The C&E undertakes planned ongoing monitoring depending on the risk level of the Customer as illustrated below:

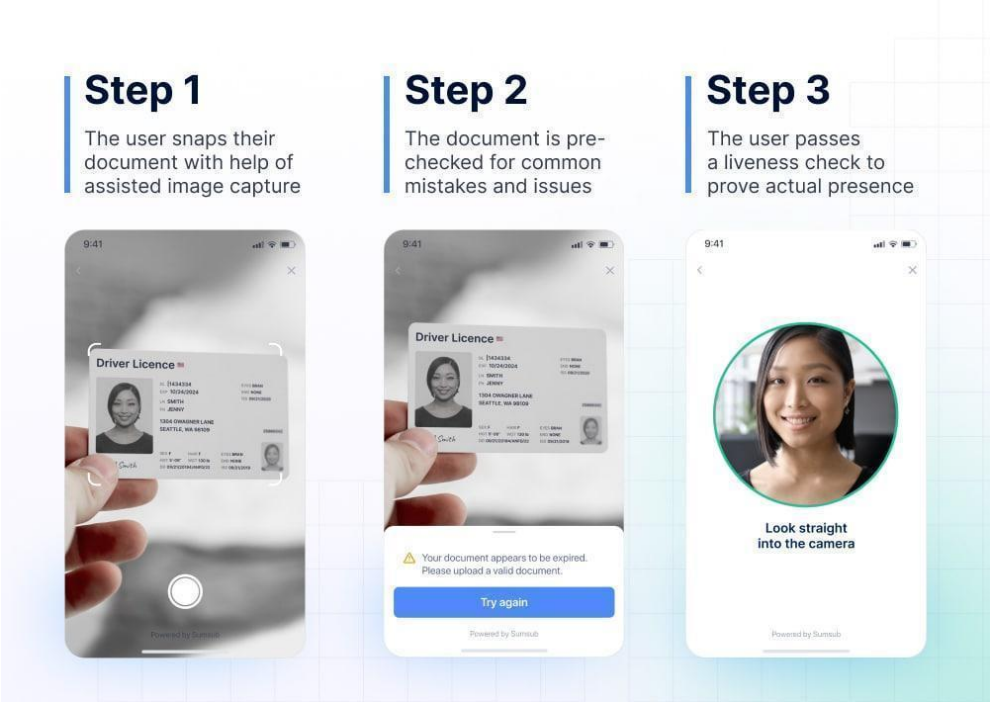


13.3.3. Distance onboarding procedure[11]

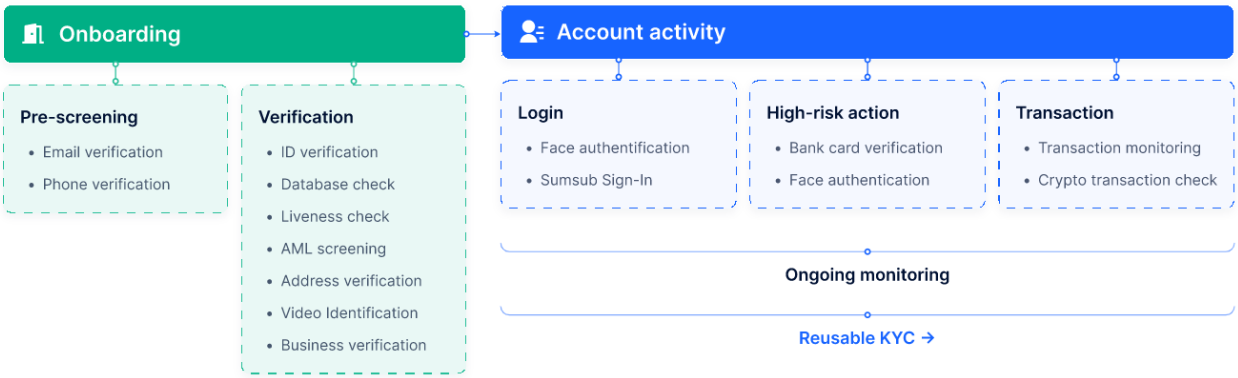
[11] https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf

This Distance Onboarding Procedure for applicants, specifically adapted to C&E services, for complying with Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) laws, involves specific steps and measures to ensure regulatory compliance and mitigate the risk of financial crimes.

C&E uses SUMSUB System[12] for verification individuals,including UBO, shareholders (company & individuals), directors, authorized signatories



An example of automated KYC that's completed in three stages within approximately 50 seconds via SUMSUB System.



An adapted scheme of procedure for C&E services includes:

[12] https://sumsub.com

(a) Application and Document Collection:
Applicants submit their applications electronically through secure Online Platforms specifically designed for C&E services. The C&E collects and verifies essential identity, background, and founding information (individuals and corporate), including personal details, address history, financial and other information, as required by AML/CFT regulations.

(b) Enhanced Due Diligence (EDD) for C&E services:
Given the nature of C&E services, which involve the exchange of various types of assets and/or currencies, the C&E applies enhanced due diligence measures. This must/may include gathering additional information about the applicant's business model, the types of assets or currencies involved, and the parties involved in those transactions.

(c) Risk Assessment and Mitigation:
The C&E conducts a risk assessment specific to C&E services. This involves evaluating the potential risks associated with the applicant's business activities, such as the risk of money laundering, fraud, or terrorist financing. Mitigation measures are implemented based on the identified risks.

(d) Compliance with Regulatory Requirements:
The C&E ensures compliance with AML/CFT laws and regulations applicable to C&E services. This includes understanding the regulatory framework, such as customer identification requirements, transaction monitoring, and reporting obligations. Policies and procedures are developed to align with these requirements.

(e) Screening and Sanctions Checks:
The C&E conducts thorough screening of the applicant and any related parties against various international sanctions lists, watchlists, and politically exposed person (PEP) databases. This step helps identify and mitigate the risk of engaging with individuals or entities involved in illicit activities.

(f) Remote Identity Verification:
To verify the applicant's identity remotely, the C&E employs secure digital identification technologies specific to C&E services. These technologies include biometric verification, video calls, and/or digital document verification, ensuring a reliable and secure means of confirming the applicant's identity without a physical presence (for more details see 12.1 The KYC Process of this Policy)

(g) Ongoing Monitoring:
Once the applicant is successfully onboarded, the C&E implements ongoing monitoring processes specific to C&E services. This includes continuous transaction monitoring, periodic reviews of customer information, and detecting any suspicious activities or changes in the applicant's risk profile related to C&E transactions.

(h) Staff Training and Awareness:
The C&E ensures that its employees, particularly those involved in C&E services, receive comprehensive training on AML/CFT policies and procedures. Regular training sessions and updates are provided to enhance their understanding of regulatory requirements and their role in preventing financial crimes within the context of C&E services.

Additionally, C&E adheres to the Four Eyes Principle[13]. C&E's Online Platform uses machine learning to detect spoofing attempts and confirm matches between user IDs and users' faces. The KYC specialist always adds a final confirmation ensuring that everything is in check.

In rare cases, as an alternative to verification through an AML tool, the following can be applied, C&E will arrange for the identification of the applicant via videoconference.

The applicant meets via videoconference with the responsible C&E person in the person of the director / CEO / business development manager / manager of the sales department and provides ID / international passport for identification, this videoconference is recorded, also the responsible C&E person verifies the adequacy of the person on the videoconference regarding the legal capacity of the person, and this person really understands the business of the company.

This video is then sent to a member of the AML team for the appropriate verification of compliance with the AML Policy.

The C&E conducts further KYC in accordance with clause 12.1 The KYC Process of this Policy.

13.3.4. The process of Verification:

A person submits a selfie with a valid identifying document during a verification guided by the AML tool's customer-side integration (biometric authentication using identity documents, selfie or selfie with identity verification (including UBO, shareholders (company & individuals), directors, authorized signatories).

Once all the necessary documents are submitted, Data points are extracted, digitized, and authenticated. These Data points then become part of the person's Identity. The person then consents to share documents and/or Data points from their Identity with C&E.

13.4. Failure to conduct or complete CDD

13.4.1. In the case of C&E 's failure to conduct CDD, the C&E must not:

(a) carry out a transaction with or for a customer through a bank account or in cash
(b) open an account or otherwise provide a service
(c) otherwise, establish a business relationship or carry out a transaction
(d) terminate any existing business relationship with a customer

[13] https://www.unido.org/overview/member-states/change-management/faq/what-four-eyes-principle

(e) consider whether the inability to complete CDD requires the submission of a Suspicious Transaction Report (the 'STR').

In the event the Company is unable to properly undertake the CDD, the C&E will not:

a) establish a business relationship with a customer;
b) establish or maintain a business relationship with a Shell Bank;
c) tip off the customer.

It is strictly forbidden for anyone in the Company to keep anonymous accounts or accounts in obviously fictitious names.

14. ENHANCED DUE DILIGENCE (THE 'EDD')

14.1. Conducting EDD

14.1.1. Obligation to conduct EDD

It is our obligation to conduct and undertake EDD where money laundering risks are higher. Where this is the case the company must:

(a) obtain and verify additional:
    i. identification information on the customer and any beneficial owner;
    ii. information on the intended nature of the business relationship; and
    iii. information on the reasons for a transaction;
(b) update the CDD information which the company holds in respect of the customer and any beneficial owners more regularly;
(c) will verify information on:
    i. the customer's sources of funds;
    ii. the customer's sources of wealth;
(d) increase the degree and nature of monitoring of the business relationship
(e) obtain the approval of senior management to commence a business relationship.

EDD measures are only mandatory to the extent that they apply to the relevant customer or the business relationship's circumstances and to the extent that the risks would reasonably require it.

For high-risk customers, the company should mitigate the perceived and actual risks, exercise a greater degree of diligence throughout the customer relationship, and endeavor to understand the nature of the customer's business and consider whether it is consistent and reasonable.

14.2. Modifications to the requirement to conduct CDD

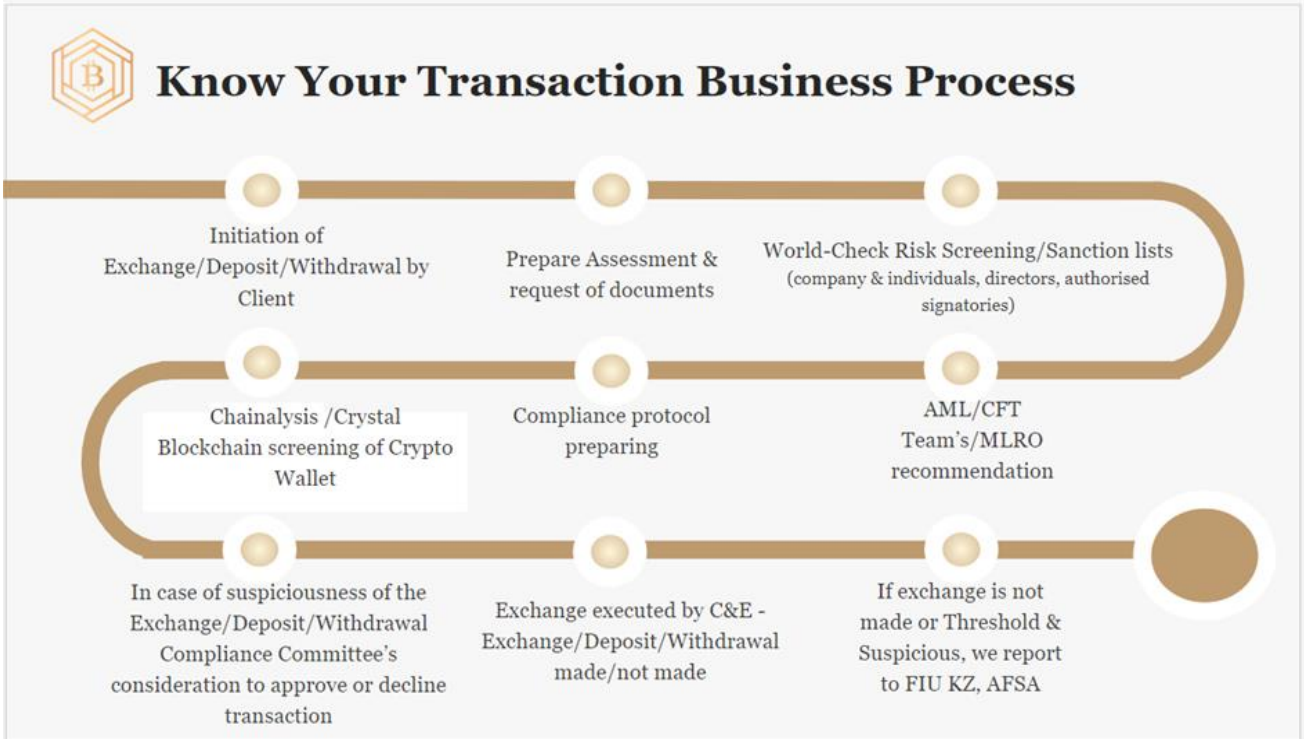
The requirement to conduct CDD may be modified by:

(a) verifying the identity of the customer and identifying any beneficial owners after the establishment of the business relationship;
(b) reducing the frequency of, or as appropriate not undertake, customer identification updates;
(c) deciding not to verify an identified beneficial owner;
(d) deciding not to verify an identification document other than by requesting a copy;
(e) not enquiring as to a customer's source of funds or source of wealth;
(f) reducing the degree of ongoing monitoring of transactions, based on a reasonable monetary threshold or on the nature of the transaction; or

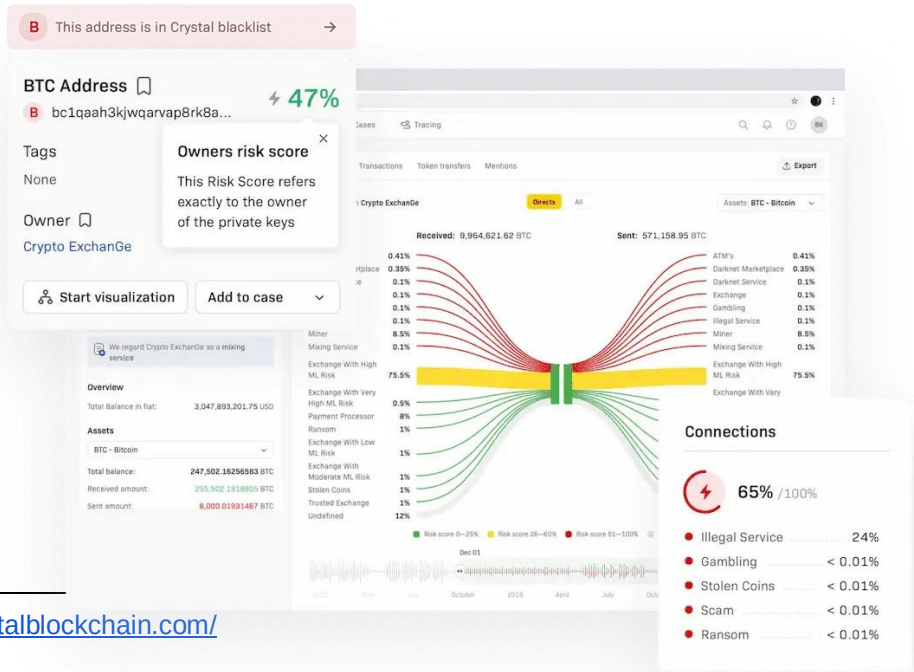
(g) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring such purpose and nature from the type of transactions or business relationship established.

The customer's money laundering concerns must be taken into account before any modifications to the conventional CDD standards are made. In order to change CDD in accordance with customer risks, the organization may potentially take various actions.

15. TRANSACTION DUE DILIGENCE (THE 'TDD')

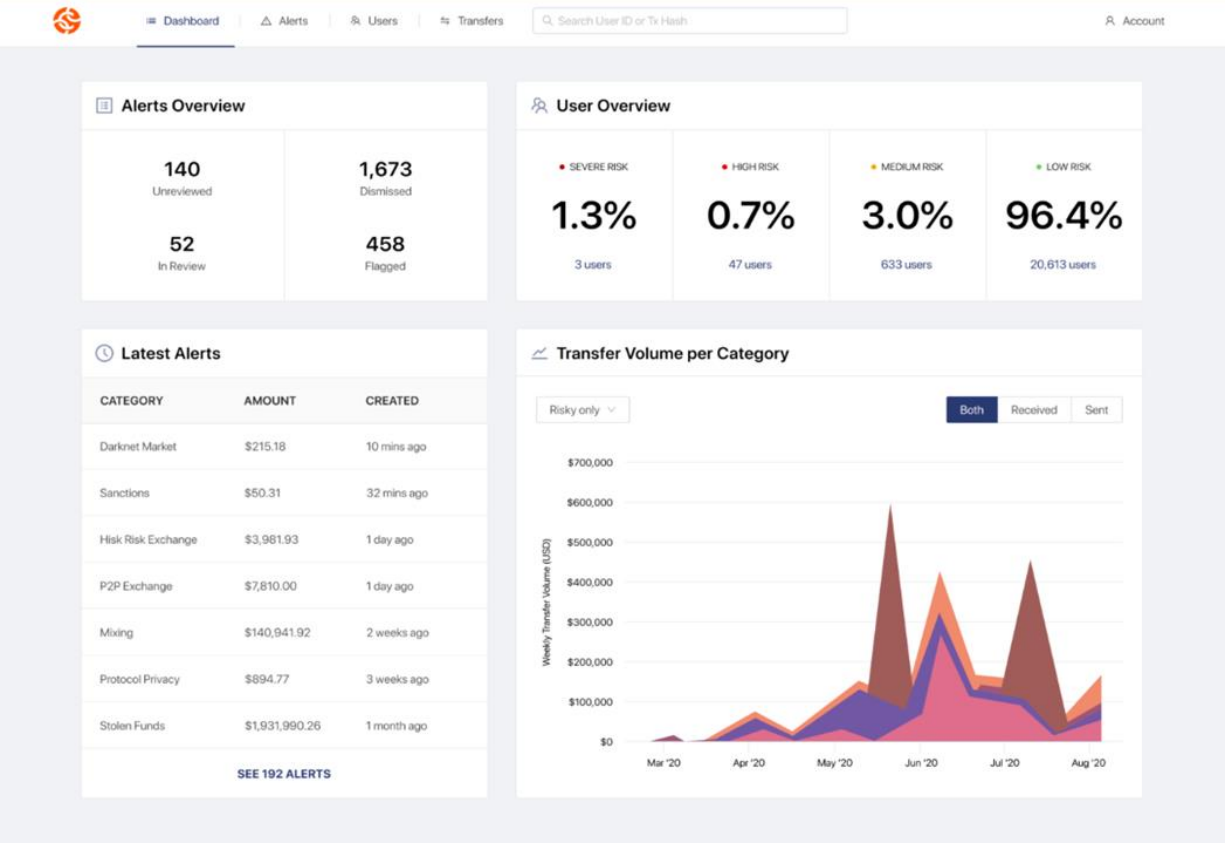


How is the check in the Crystal system and what the report looks like?[14]



[14] https://crystalblockchain.com/

How is the check in the Chainalysis system and what the report looks like?[15]



15.1. Transaction Processes

15.1.1. The C&E employees shall follow the transaction process prescribed below and process the information provided by the Customer (fiat to digital asset and vice versa):

1) Customer initiates the transaction from his account on the Online Platform, indicating the following information (fiat to digital asset):
   (a) The Customer to deposit his own digital account on the Company's Online Platform in fiat currency (by depositing via bank card and / or otherwise).
   (b) Fiat funds are displayed on the Company's Online Platform;
   (c) The Customer chooses the digital currency for which he wants to exchange;
   (d) Carries out the exchange of fiat currency for digital currency on the Company's Online Platform;
   (e) The Customer specifies the address of his own digital wallet opened on another platform (for example, Binance)
   (f) C&E checks the digital wallet address through the systems integrated into the Company's Online Platform (Crystal blockchain, Chainalysys), also screening through World-Check Risk Screening / Sanction lists, etc.
   (g) After AML / CFT team's, MLRO recommends the digital currency is sent to his own the digital wallet opened by the Customer's on another platform.

[15] https://www.chainalysis.com/

2) Customer initiates the transaction from his account on the Online Platform, indicating the following information (digital asset to fiat):
   (a) The Customer to deposit his own digital account on the Company's Online Platform in digital asset (crypto currency) (by depositing via Customer's on another platform).
   (b) C&E checks the digital asset address through the systems integrated into the Company's Online Platform (Crystal blockchain, Chainalysys), also screening through World-Check Risk Screening / Sanction lists, etc.
   (c) Digital asset funds are displayed on the Company's Online Platform;
   (d) The Customer chooses the fiat currency for which he wants to exchange;
   (e) Carries out the exchange of digital asset for fiat currency on the Company's Online Platform;
   (f) The fiat currency is sent to the Customer's bank account.

3) In addition to the above, the AML Team carries out the following actions:
   (a) Makes a screening by the AML tool (AML IT service provider);
   (b) Makes a screening of the third party through the FIU Blacklist;
   (c) Makes a KYCountry screening of the Country, where the third party is located;
   (d) Checks for the PEP status of the third party;
   (e) Send a report to FIU (if the transaction is suspicious).

4) When all needed information is collected the AML team prepares KYT Protocol (as set out in Annex 4).

15.1.2. Suspicious transaction

A suspicious transaction with money and (or) other property - a Customer transaction (including an attempt to perform such an operation, a transaction in the process of being completed, or an already completed transaction), in relation to, if there are suspicions that money and (or) other property used for its commission is the proceeds of criminal activity, or the operation itself is aimed at legalization (laundering) of proceeds from crime or financing of terrorism or other criminal activity.[16]

As required by applicable law, an AML Team member who becomes aware or suspects that any property, in whole or in part, directly or indirectly, was the income of any person, was used or intended for criminal activities, or is the property of terrorists, must report the Suspicious transaction reports to the FIU within 24 hours from the date of the suspicious transaction (the Suspicious transaction reports must be filed with any matter on which knowledge or suspicion is based).

The C&E is aware that the failure to report suspicions of money laundering or terrorist financing may constitute a criminal offence.

15.1.3. Knowledge vs. suspicion

Generally speaking, knowledge is likely to include:
(a) actual knowledge;
(b) knowledge of circumstances which would indicate facts to a reasonable person; and
(c) knowledge of circumstances which would put a reasonable person on inquiry.

[16] https://online.zakon.kz/Document/?doc_id=30466908&pos=45;117#pos=45;117

A member of an AML team, including the MLRO, who believes that any person is or is engaged in activities that he knows or suspects is suspicious should not know the exact nature of the criminal offense or that specific funds were definitely received in the result of the crime of money laundering or terrorist financing.

15.1.4. Disclose information

It is considered an offense, known as "tipping-off," to disclose information that could potentially hinder an investigation.

AML team members and all C&E employees who become aware of the "tipping-off" violation must not disclose to anyone any information that could prejudice an ongoing investigation. If the Customer is informed that a report has been filed, this will jeopardize the investigation and be considered a misdemeanor.

It also applies in situations where suspicion has arisen within C&E but has not yet been reported to the Financial Intelligence Unit (FIU).

C&E does not maintain anonymous accounts or accounts in clearly fictitious names.

15.1.5. Identifying suspicious transactions

Appendix 2 contains a list of circumstances and actions that can help identify suspicious transactions, however, this list is not an instruction, it can only be used as an example of red flags that may signal that a transaction/activity would arouse suspicion.

An AML team member shall check the accuracy of the information received about the customer in the following cases:

(a) customer performing a threshold operation (transaction), as set out in Annex 2;
(b) customer performing (or attempting to perform) a suspicious operation (transaction);
(c) customer performing an unusual operation (transaction);
(d) the customer's operation (transaction) having characteristics that correspond to typologies, schemes and methods of legalisation (laundering) of proceeds from crime and the financing of terrorism.

In order to classify a transaction/action as a suspicious transaction, a member of the AML team must take into account the nature of the customer relationship, the risk profile of the customers and the business relationship, apply the tools to analyze the transaction/action, conduct an investigation based on their experience, while considering and analyzing recommendations FATF, member of the AML team refer to the up-to-date information provided on the FATF website.[17]

This set of indicators demonstrates how red flags traditionally associated with transactions involving more conventional means of payment remain relevant to detecting potential illicit activity related to Digital Assets.

15.1.5.1. Size and frequency of transactions[18]:

(a) Structuring Digital Assets transactions (e.g. exchange or transfer) in small amounts, or in amounts under record-keeping or reporting thresholds, similar to structuring cash

[17] https://www.fatf-gafi.org/en/home.html

[18] https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf

transactions.
(b) Making multiple high-value transactions:
- in short succession, such as within a 24-hour period;
- in a staggered and regular pattern, with no further transactions recorded during a long period afterwards, which is particularly common in ransomware-related cases; or;
- to a newly created or to a previously inactive account.

(c) Transferring Digital Assets immediately to multiple VASPs, especially to VASPs registered or operated in another jurisdiction where:
- there is no relation to where the customer lives or conducts business; or
- there is non-existent or weak AML/CFT regulation.

(d) Accepting funds suspected as stolen or fraudulent:
- depositing funds from VA addresses that have been identified as holding stolen funds, or VA addresses linked to the holders of stolen funds.

A transaction that appears unusual is not necessarily suspicious. Even customers with a stable and predictable transaction profile may have occasional transactions that are unusual for them. Many customers will, for perfectly good reasons, have an erratic pattern of transactions or account activity. Unusual behaviour is, in the first instance, only a basis for further inquiry, which may in turn require judgement as to whether it is suspicious. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report them then arises.

Effective CDD measures may provide the basis for recognising unusual and suspicious activity. Where there is a customer relationship, suspicious activity will often be one that is inconsistent with a customer's known legitimate activity, or with the normal business activities for that type of account or customer. Therefore, the key to recognising 'suspicious activity' is knowing enough about the customer and the customer's normal expected activities to recognise when their activity is abnormal.

C&E must freeze without delay and without prior notice, the funds or other assets of designated persons and entities pursuant to relevant resolutions or sanctions issued by the United Nations Security Council, by the Republic of Kazakhstan, or if relevant by other jurisdictions.

15.1.5.2. Red Flag Indicators Related to Anonymity[19]

This collection of indicators is based on the inherent traits and weaknesses linked to the underpinning technology of Digital Assets. The many technology elements listed below make it harder for law enforcement to uncover illicit conduct and promote anonymity. Digital Assets are appealing to thieves wanting to conceal or store their money because of these considerations. However, the sheer existence of these characteristics in an activity does not imply an illegal transaction by default. For instance, using a hardware or paper wallet to protect Digital Assets from thefts may be appropriate. Once more, the existence of these indicators should be taken into account in the context of other customer and relationship characteristics, or a legitimate business justification.
- Transactions by a customer involving more than one type of Digital Asset, despite additional transaction fees, and especially those Digital Assets that provide higher anonymity, such as anonymity-enhanced cryptocurrency (AEC) or privacy coins.
- Moving a Digital Assets that operates on a public, transparent blockchain, such as Bitcoin, to a centralised exchange and then immediately trading it for an AEC or privacy

[19] https://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-assets-red-flag-indicators.html

coin.

- Customers that operate as an unregistered/unlicensed VASP on peer-to-peer (P2P) exchange websites, particularly when there are concerns that the customers handle huge amount of Digital Asset transfers on its customer's behalf, and charge higher fees to its customer than transmission services offered by other exchanges. Use of bank accounts to facilitate these P2P transactions.
- Abnormal transactional activity (level and volume) of Digital Assets cashed out at exchanges from P2P platform-associated wallets with no logical business explanation.
- Digital Assets transferred to or from wallets that show previous patterns of activity associated with the use of VASPs that operate mixing or tumbling services or P2P platforms.
- Transactions making use of mixing and tumbling services, suggesting an intent to obscure the flow of illicit funds between known wallet addresses and darknet marketplaces.
- Funds deposited or withdrawn from a Digital Asset address or wallet with direct and indirect exposure links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (e.g. ransomware) and/or theft reports.
- The use of decentralised/unhosted, hardware or paper wallets to transport Digital Assets across borders.
- Users entering the VASP platform having registered their Internet domain names through proxies or using domain name registrars (DNS) that suppress or redact the owners of the domain names.
- Users entering the VASP platform using an IP address associated with a darknet or other similar software that allows anonymous communication, including encrypted emails and VPNs. Transactions between partners using various anonymous encrypted communication means (e.g. forums, chats, mobile applications, online games, etc.) instead of a VASP.
- A large number of seemingly unrelated Digital Asset wallets controlled from the same IP-address (or MAC-address), which may involve the use of shell wallets registered to different users to conceal their relation to each other.
- Use of Digital Assets whose design is not adequately documented, or that are linked to possible fraud or other tools aimed at implementing fraudulent schemes, such as Ponzi schemes.
- Receiving funds from or sending funds to VASPs whose CDD or KYC processes are demonstrably weak or non-existent.
- Using Digital Asset ATMs/kiosks (1) despite the higher transaction fees and including those commonly used by mules or scam victims; or (2) in high-risk locations where increased criminal activities occur.

A single use of an ATM/kiosk is not enough in and of itself to constitute a red flag, but would be if it was coupled with the machine being in a high-risk area, or was used for repeated small transactions (or other additional factors).

15.1.6. Internal reporting

All employees are made aware of the identity of the MLRO and of the procedures to follow when making an internal report.

All internal reports must reach the MLRO without undue delay.

15.1.6.1. The MLRO, when evaluating an internal report, must take the following steps

to process the information received, including the CDD, which may include:
(a) a review of other transaction patterns and volumes through connected accounts, preferably adopting a relationship-based approach rather than on a transaction-by-transaction basis;
(b) making reference to any previous patterns of instructions, the length of the business relationship and CDD, and ongoing monitoring information and documentation; and
(c) appropriate questioning of the customer per the systematic approach to identify suspicious transactions recommended by the FIU.

15.1.6.2. An AML team member must:
(a) Explore the background and purpose of the transaction, risk profile and/or source of funds. to determine if there are grounds for suspicion, also identify transactions that (i) are complex, unusually large in value, or of an unusual nature and (ii) have no apparent economic or legal purpose;
(b) notify MLRO directly on a daily basis, via email, of a situation where a business relationship has not been established due to suspicious circumstances, and the internal report must include sufficient details of the Customer concerned and suspicious information, while MLRO must acknowledge receipt of the internal report;
(c) conducting transfers shall identify all transactions of all customers to the grounds as set out in Annex 2;
(d) must indicate in the STR that the account is part of an ongoing law enforcement investigation that requires urgent reporting;
(e) conduct due diligence on the business relationship following the filing of an STR with the FIU, regardless of any subsequent feedback provided by the FIU, and apply appropriate risk mitigation measures.

15.1.7. AML/CFT Systems in relation to suspicious transaction reporting

In order to comply with reporting laws and to manage and mitigate the risks associated with any Customer or transaction related to STRs, C&E applies the following AML/CFT systems in relation to reporting suspicious transactions:

- MLRO and AML team members, whose functions and responsibilities are specified in section 20 of this Policy, which is also a tool for reducing and managing C&E risks, and responsible for STRs.
- This Policy is also one of the AML/CFT systems regarding the reporting of suspicious transactions.

15.1.8. Making Suspicious transaction reports (the 'STR')

In most cases, before deciding to make a report, the MLRO is likely to need access to the relevant business information. C&E must therefore take reasonable steps to give its MLRO access to such information. Relevant business information may include details of:

(a) the financial circumstances of a customer or beneficial owner, or any person on whose behalf the customer has been or is acting;
(b) the features of the transactions, including, where appropriate, the jurisdiction in which the transaction took place; and
(c) the underlying CDD information, and copies of the actual source documentation in respect of the customer.

In addition, the MLRO may wish:

(a) to consider the level of identity information held on the customer, and any information on his personal circumstances that might be available to the

company; and

(b) to review other transaction patterns and volumes through the account or accounts in the same name, the length of the business relationship and identification records held.

15.1.9. Reporting to the FIU

A member of the AML team making transfers must identify suspicious and threshold transactions and report them to the MLRO, which then monitors, examines the data received, and, if such a transaction/action is suspicious, sends a report to the STR.

The MLRO shall fill out the STR on the C&E account opened on the FIU's website. In the preparation of an STR, in case the MLRO knows or assumes that the funds which form the subject of the report do not belong to a customer but to a third party, this fact and the details of C&E's proposed course of further action in relation to the case should be included in the report.

If a member of the AML team cannot obtain a satisfactory explanation for the transaction or activity, they may conclude that there are grounds for suspicion. In any case, if during the monitoring of the transaction any suspicions are revealed, the STR should be sent to the FIU.

As soon as knowledge and suspicions are formed, a member of the AML team must file an STR even if no operation has been performed, and an STR must be sent after the first suspicion is detected.

When submitting an STR, it is recommended that any intent to terminate the business relationship be indicated at the time of initial disclosure to the FIU, allowing the FIU to comment on this course of action at an early stage

In the event that the FIU has requested additional information based on the results of a previously sent report by letter, the MLRO should act on the contents of the letter and provide additional information or, if necessary, seek legal advice.

Filing a report to the FIU provides MLRO and/or members of AML team with a statutory defense to the offence of ML/TF in respect of the acts disclosed in the report, provided:
(a) the report is made before the MLRO and/or members of AML team undertakes the disclosed acts and the acts (transaction(s)) are undertaken with the consent of the FIU; or
(b) the report is made after the MLRO and/or members of the AML team has performed the disclosed acts (transaction(s)) and the report is made on the MLRO and/or members of the AML team's own initiative and within a time frame specified by the AML Law.

If the MLRO has reported suspicion to FIU, the FIU may instruct C&E on how to continue its business relationship, including effecting any transaction with a person. If the customer in question expresses his wish to move the funds before C&E receives instruction from the FIU on how to proceed, the C&E should immediately contact the FIU for further instructions.

Transfer of information between C&E departments regarding suspicious transactions/actions

If there are grounds to suspect a customer in relation to AML matters, the Sales team should immediately report on this matter to the MLRO in the form of protocol. In case of a number threshold or suspicious operations, employees of the AML/CFT team should report to MLRO

immediately in the form of protocol.

For the Operational Day, we mean the time during which operations are accepted and carried out for transferring customer funds and transactions:

Opens (GMT +6)	Closes (GMT +6)
9:00	16:30

15.10. Outgoing transfers

15.10.1. Any Transfer shall contain the following:

(a) the name of the payer;
(b) the payer account number where such an account is used to process the transaction (or unique transaction reference number that allows traceability of the transaction if no account exists);
(c) the name of the payee; and
(d) the payee account number where such an account is used to process the transaction (or unique transaction reference number that allows traceability of the transaction if no account exists); information containing the payer's address or national identity number (individual identification number or passport number), or customer identification number, or date and place of birth.

15.10.2. If several individual cross-border wire transfers from a single-payer are bundled in a batch file for transmission to payees, then C&E must ensure that transfers contain the following:

(a) the name of the payer;
(b) the payer account number where such an account is used to process the transaction (or unique transaction reference number that allows traceability of the transaction if no account exists);
(c) the name of the payee; and
(d) the payee account number where such an account is used to process the transaction (or unique transaction reference number that allows traceability of the transaction if no account exists); information containing the payer's address or national identity number (individual identification number or passport number), or customer identification number, or date and place of birth; (ii) it has verified the payer information referred to in (i); and (iii) the batch file contains the payee information required under (a) for each payee and that information is fully traceable in each payee's jurisdiction.

C&E should maintain all Originator and Beneficiary information collected, in accordance with the FATF Recommendation 11: Record-keeping[20].

C&E should not be allowed to execute the wire transfer if it does not comply with the

[20] FATF (2012-2019), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, www.fatf-gafi.org/recommendations.html, page 13

requirements specified above[21].

As part of the programme for monitoring and analysing customer operations, C&E shall carry out activities aimed at setting goals and grounds for all threshold, unusual, suspicious transactions, and operations, that have characteristics corresponding to the typologies, schemes, and methods of legalisation (laundering) of proceeds from crime and the financing of terrorism, and in case of necessity the source of financing.

16. KNOW YOUR SUPPLIER (THE 'KYS')

The C&E enters into business relationships with individuals and entities who engage in ethical business practices, are not sanctioned individuals or entities and who comply with all applicable laws and regulations.

The KYS should be prepared before the relationship with the supplier.

16.1. Process of the KYS

1. The Business Development Manager (the 'BDM') provides and notifies the AML team about the new supplier and provides documents, that were provided by the supplier;
2. AML Team makes a preliminary check on the new supplier if needed AML team asks for additional information or documents;
3. In the process of the preliminary check, the AML team is searching the information regarding the supplier in open public records and makes the screening by the AML tool (AML IT service provider);
4. Makes a screening of the supplier through the FIU Blacklist;
5. Makes a KYCountry screening of the country(-ies), where the supplier is located or/and incorporated;
6. Checks for the PEP status of the employees of the supplier and the supplier itself;
7. If all necessary data was submitted AML team prepares the KYS protocol (see Annex 5);
8. If the Risk level of the customer is High-Risk, the AML team provides the protocol to the BDM.

16.2. Process of KYS with Kazakhstani Banks

1. The BDM provides and notifies the AML team about the new Bank and provides documents, that are publicly available on the official website of the Bank;
2. AML Team checks the documents and rate of the Bank via KASE rate;
3. In the process of the preliminary check, AML team searches the information regarding the Bank in open public records and makes the screening by the AML tool (AML IT service provider);
4. If all necessary data was submitted AML team prepares the KYS protocol (see Annex 5);

17. KNOW YOUR EMPLOYEE ('KYE')

KYE checks play a vital role in assessing the employee's background, which helps prevent

[21] FATF (2012-2019), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, www.fatf-gafi.org/recommendations.html, page 74, Sub Section 14 Ordering financial institution, Section E. RESPONSIBILITIES OF ORDERING, INTERMEDIARY

corporate fraud and losses. KYE ensures safer employee onboarding which can help managers find a productive and trusted resource.

The KYE should be prepared before hiring such an employee.

17.1. Process of KYE

1. The Human Resources Manager (the 'HR') provides and notifies the AML team about the new employee and provides documents, that were provided by the employee;
2. AML Team makes a preliminary check on the new employee if needed AML team asks for additional information or documents;
3. In the process of the preliminary check, the AML team is searching the information regarding the employee in open public records and makes the screening by the AML tool (AML IT service provider);
4. Makes a screening of the employee through the FIU Blacklist;
5. Checks for the PEP status of the employee;
6. If all necessary data was submitted AML team prepares the KYE protocol (see Annex 6);
7. If the Risk level of the employee is High-Risk, the AML team provides the protocol to HR.

18. SANCTIONS COMPLIANCE

18.1. Sanctions systems and controls

The C&E undertakes to establish and maintain effective systems and controls to ensure that, on an ongoing basis, it is properly informed as to, and takes reasonable measures to comply, with relevant resolutions or sanctions issued by the United Nations Security Council and (or) by the Republic of Kazakhstan.

Furthermore, the C&E considers and takes steps to ensure compliance in relation to unilateral sanctions imposed by the European Union, the United Kingdom (HM Treasury), the United States of America (Office of Foreign Assets Control of the Department of the Treasury), Canada (FINTRAC), and other relevant jurisdictions where appropriate and relevant.
The C&E ensures that the company's compliance team receive adequate resources including in the form of human capital, expertise, information technology, relevant database(s) and other resources.

The MLRO and Deputy MLRO will be half-manually & half-automatized by the screening systems to check every potential customer against the relevant sanctions lists before onboarding the potential customers and suppliers of the company, as well as during the TDD.

18.2. Checking sanctions lists

It is our obligation to review our customers, their business, and transactions against sanctions imposed by the United Nations Security Council, relevant authorities of Kazakhstan, as well as other relevant jurisdictions, such as the European Union, United States, and the United Kingdom when undertaking ongoing CDD.

To mitigate the risk of secondary sanctions or reputational risk, sanctions screening must be conducted not only at the beginning of a new relationship or operation but on an ongoing

basis.

The AML team perform the Sanctions screening after receiving the required documents and during the Due Diligence via the AML Tool[22], of which Protocol shall be an integral part of the process of Due Diligence. Furthermore, the AML team performs additional screening through the Kazakhstani FIU list[23] and, if necessary, Adverse media screening on publicly open sources.

The C&E personnel shall familiarise themselves with the 'Rule of 50%'[24], as illustrated in Annex 6, and consider before and after entering a legal relationship and(or) having an operation with an external person. The Compliance Officer shall ensure that the data on Sanctions Compliance, including the 'Rule of 50%' is relevant and up to date.

18.3. Risk Zones

A risk zone is determined based on a threat of secondary sanctions and(or) reputational risks that may be imposed and affected the company, the severity of potential consequences, the likelihood of a hazard occurring, mitigating factors, and impact on the C&E's objectives and strategy.

The C&E personnel must follow the following approaches during the preliminary, ongoing, and final assessments on Sanctions Compliance:

GREEN ZONE: Low Risk	YELLOW ZONE: Medium Risk	RED ZONE: High Risk
➢ any operation or legal relationship with an external person may be maintained.	➢ any operation or legal relationship with an external person not in the Sanctions List(s) but residents of countries associated with sanctions may be maintained with caution; ➢ any operation or legal relationship with an external person not in the Sanctions List(s) but closely working with sanctioned persons may be maintained with caution; ➢ any operation or legal relationship with an external person with potentially high risks of being included in the Sanctions List(s) may be	➢ any operation or legal relationship with an external person that in the Sanctions List(s) needs to be rejected, suspended, limited, or stopped; ➢ any operation or legal relationship with an external person falling under the 50% Rule needs to be rejected, or suspended, or limited, or stopped.

[22] The C&E has a full subscription to Refinitiv World Check services, which provides up-to-date data on sanctions lists of the United Nations, US OFAC, EU, UK, and other relevant overall 240 jurisdictions

[23] https://www.web-sfm.kfm.kz/

[24] A person whose property and interests in a property are blocked by the relevant sanctions authority's regulations is considered to have an interest in the property, and interests in the property of the final legal person, in which the blocked person owns or controls, directly or indirectly, a 50 % or greater interest. It is reasonable to expect that the controlling person would be able to ensure the affairs of the legal person are conducted in accordance with this person's wishes

	maintained with cautions.	

The Compliance Committee considers and determines the risks provided for by this AML Policy in the following cases:

(a) an operation may entail a positive outcome for the C&E's development and its strategic purposes, and the level of such outcome may be evaluated as is higher than the potential risks; and

(b) cooperation of being involved in operations with a sanctioned person does not entail or entails minimum risks of secondary sanctions or reputational risks to the C&E that should not worsen conditions of the company.

18.4. Non-Compliance

Upon becoming aware of being listed in one or more of the Sanctions List(s), any breach or suspected potential non-compliance, the C&E personnel informs the Compliance Officer about such situation, breach, or suspected potential breach.

In case the C&E personnel knowingly or intentionally or unintentionally breaches this AML Policy or any other applicable laws and regulations, the management of the C&E may address disciplinary liability measures toward a breacher in accordance with the C&E's internal policies and Acting Law of the AIFC.

In case the C&E has already started an operation or legal relationship with an external person, and later that external person is included in one or more of the Sanctions Lists, the C&E personnel immediately reports thereof to the Compliance Officer.

The C&E personnel will take all necessary steps to address a breach, including steps to suspend, freeze, reject, stop, or terminate the relevant operation or legal relationship to ensure that there is no contravention of this AML Policy or applicable laws and regulations.

The C&E AML team evaluates existing circumstances, factors, and possible consequences, and provides analysis results to relevant departments of C&E on cases prescribed herein of this AML Policy.

Taking into account the results of the risk assessment, the Compliance Committee decides to start or continue the operation and (or) maintenance of the legal relationship.

In the event that a C&E is listed inappropriately on one or more of the sanctions lists, the Compliance Officer and the AML team must take immediate action to remove the company from the lists. These actions are taken in cases that were not proven and / or committed erroneously.

18.5. Notification obligation

The C&E will report to the Financial Intelligence Unit of the Republic of Kazakhstan ('FIU') on any assets that have been frozen, or actions taken in compliance with the prohibition requirements of the relevant resolutions or sanctions issued by the United Nations Security Council or by the Republic of Kazakhstan, including attempted transactions.

GENERAL PROVISIONS

19. COMPLIANCE OFFICER

19.1. The C&E Compliance Officer oversees the compliance monitoring program within the company, ensures the compliance of the company's activities, strategy, and internal policies with the AIFC AML Rules, AML Law, and other relevant laws and regulations, as well as endeavours the implementation of best international standards.

19.2. The Compliance Officer fulfils several functions:

(a) monitors all operational processes and procedures to ensure that the company complies with all legal regulations and ethical standards;

(b) manages information flow by researching, recording and analysing data and information. With a regular flow of information and conducting compliance risk assessments, they ensure that the business runs smoothly;

(c) train and educate the C&E personnel so that they are informed of any legal changes and updates to compliance guidelines;

(d) acts as a contact person and liaison between department heads and the senior management of C&E;

(e) conducts regular assessments to determine whether the C&E internal policies are compliant with the relevant laws and regulations as well as international best practices.

The Compliance Officer's detailed objectives and functions are prescribed in the C&E Compliance Functions Policy.

20. MONEY LAUNDERING REPORTING OFFICER, SUSPICIOUS TRANSACTIONS AND TIPPING OFF

20.1. Money Laundering Reporting Officer (MLRO)

20.1.1. The MLRO provides oversight of the company's anti-money laundering systems and acts as a focal point for related inquiries. The role involves a significant amount of responsibility: MLRO must have access to the company's financial records to provide oversight and make strategic decisions about activities relating to money laundering and financial crime

20.1.2. C&E's MLRO function must be performed by the Principal Representative of C&E and responsible for the implementation and oversight of the C&E's AML Policy, procedures, systems, and controls.

20.2. Appointment of MLRO

20.2.1. C&E's Director will appoint an individual as MLRO, with responsibility for the implementation and oversight of its compliance with the AIFC AML Rules and other relevant laws and regulations.

20.2.2. The Company shall also appoint the Deputy MLRO in order to ensure the fulfilment of the MLRO function during the absence of the MLRO. Also, the company ensures the hiring of employees, other than MLRO and Deputy MLRO, as the company sees it appropriate and depending on the company's activities, to fulfil and strengthen the AML team and overall the AML function.

20.3. Obligation of co-operation

The MLRO must deal with the AFSA, FIU, and other authorities (if relevant) in an open,

responsive, and cooperative manner and must disclose appropriately any information of which the AFSA, FIU, and other authorities (if relevant) would reasonably be expected to be notified.

20.4. Qualities of an MLRO

The company's MLRO has the following:

(a) direct access to senior company management;
(b) a level of seniority and independence within the company to enable him to act on his authority and to act independently in carrying out his responsibility;
(c) sufficient resources, including appropriate staff and technology; and
(d) timely and unrestricted access to enough information to enable him to carry out his duties as indicated below:

MLRO implements and oversees the following matters:

1) review of internal disclosures and exception reports and, in light of all available relevant information, determination of whether or not it is necessary to make a report to the FIU;
2) maintenance of all records related to such internal reviews;
3) provision of guidance on how to avoid tipping-off;
4) day-to-day operations to comply with AML policies, procedures, systems and controls;
5) act as a point of contact for receiving notices from employees;
6) taking appropriate action in accordance with this policy upon notification from an employee;
7) filing an STR in accordance with the applicable laws of Kazakhstan;
8) act as a point of contact for the AFSA and any other competent authority on money laundering matters;
9) respond promptly to any request for information made by the AFSA and any other competent authority;
10) receiving and taking action in accordance with any relevant findings, recommendations, directions, directives, resolutions, sanctions, notifications or other findings, in accordance with the current legislation of the AIFC; and
11) establishing and maintaining an adequate money laundering training program and adequate awareness raising activities.

20.5. Responsibilities of an MLRO

20.5.1. The MLRO implements and has oversight of, and is responsible for, the following matters:

(a) ensures compliance by every member of the company with the AML Policy, procedures, and processes;
(b) undertakes appropriate action following the receipt of a notice from an employee of a potentially suspicious transaction;
(c) initiates STRs and reports to FIU independently in compliance with applicable Kazakhstani Law (see Annex 2);
(d) acts as the point of contact within the company for the AIFC, the AFSA, and any other competent authority regarding money laundering issues;
(e) responds promptly to any request for information from the AIFC, the AFSA, and any other competent authority;
(f) receives and acts upon any relevant findings, recommendations, guidance, directives, resolutions, sanctions;

(g) establishes and maintains an appropriate money laundering training program and adequate awareness arrangements;
(h) on an ongoing basis, checks that the AML / CFT systems for reporting suspicious transactions that apply C&E comply with legal and regulatory requirements and also that they work effectively (including the type and extent of measures taken should be appropriate to the risk of ML / TF, as well as the nature and size of the business);
(i) maintain proper records of the discussions and actions taken to demonstrate that it acted reasonably in determining that a particular transaction or operation was suspicious.

21. ANNUAL AML RETURN

The MLRO prepares the Annual AML Return for further submission to AFSA on an annual basis and submission it to the AFSA within two months of our financial year-end.

22. GENERAL OBLIGATIONS of C&E

22.1. Reporting Obligations

Reporting Obligation when there is:

(a) Threshold Transaction.
(b) Suspicious transaction/activity.

Threshold Transactions Controls

The Company will establish and maintain procedures, systems, and controls to monitor, detect, and report transactions above-defined thresholds to the FIU under the AML/CFT Law.

Suspicious Activity Controls

The Company will maintain policies, procedures, systems, and controls to monitor suspicious activity or transactions concerning potential money laundering or terrorist financing.

Suspicious Transaction Monitoring

Subject to the algorithms and sensitivity of suspicious transaction monitoring procedures:

1. Transaction amount
2. Transaction frequency
3. Transaction purpose
4. Customer behaviour and profile
5. Transaction counterparty

Immunity from liability for disclosure of information

The disclosure by C&E to the competent authorities of information relating to money laundering/terrorist financing is not a breach of the obligation of secrecy or non-disclosure or (where applicable) of any enactment by which that obligation is imposed.

22.2. Record keeping

22.2.1. The Company will maintain the following records:

(a) Electronic copies of all documents and information obtained in undertaking initial and ongoing CDD;

(b) the supporting records in respect of customer business relationships, including transactions;

(c) threshold transaction reports;

(d) STRs and any relevant supporting documents and information, including internal findings and analysis;

(e) any relevant communications with the FIU; and

(f) the documents required under the 23.1.;

(g) for at least six years from the date on which the notification or report was made, the business relationship ends, or the transaction is completed, whichever occurs last.

22.2.2. It is our obligation to document and provide to the AFSA on request any of the following:

a) the risk assessments of its business are undertaken (RBA);

b) how the assessments in (a) were used to undertake risk based assessments of each customer; and

c) every customer RBA and determination.

22.2.3. The Company will demonstrate that it has complied with the training and awareness requirements through appropriate measures, including the maintenance of relevant training records.

22.3. Audit

It is our obligation to ensure that the Company's audit function (internal or external), includes regular reviews and assessments of the effectiveness of the Company's AML Policy, procedures, systems and controls and its compliance therewith.

22.4. Communication with the Regulator

The C&E must be open and cooperative in all the Company deals with the Regulator; and ensure that any communication with the Regulator is conducted in the English language.

22.5. Employee Disclosures

The Company will undertake to ensure that it does not prejudice an employee who discloses any information regarding money laundering to the AFSA or any other relevant body involved in preventing money laundering.

23. AML POLICY OF GROUPS, BRANCHES, AND SUBSIDIARIES

The C&E must ensure that its AML Policy applies to all of its branches or subsidiaries; and all of its Group entities that are AIFC participants.

The indicated requirement does not apply if can satisfy the AFSA that the relevant branch, Subsidiary or Group entity is subject to regulation, including AML, by a Financial Services Regulator or other competent authority in a country with AML regulations which are equivalent to the standards set out in the FATF Recommendations and is supervised for compliance

with such regulations.

Where the law of another jurisdiction does not permit the implementation of AML Policy, C&E must inform AFSA in writing; and apply appropriate additional measures to manage the AML risks posed by the relevant branch or subsidiary.

The C&E must ensure that its branches and majority-owned subsidiaries in host countries implement the requirements of the AIFC. If the host country does not permit the proper implementation of the mentioned measures, financial groups should apply appropriate additional measures to manage the money laundering risks and inform the AFSA of such measures. Group's AML policies must adequately mitigate any high geographical risk factors.

23.1. Communication and documentation

The C&E must communicate its AML Policy maintained in accordance with AIFC AML Rules to its Group entities, branches, and subsidiaries; and document the basis for its satisfaction that the requirement in AIFC AML Rules 14.1.1(b) is met.

23.2. Enforcement

In relation to the C&E's branches and subsidiaries, if AFSA is not satisfied in respect of AML compliance of its branches and subsidiaries in a particular jurisdiction, it may take action, including making it a condition on the C&E's Licence that it must not operate a branch or subsidiary in that jurisdiction.

24. Training and Awareness of the Employees

The AML training shall be conducted on the regular basis. The MLRO is responsible for designing the compliance training and delivering it to the employees.

The training shall be done on a quarterly basis, in case of hiring a new employee, the MLRO shall provide appropriate training during the recruiting week.

The MLRO shall ensure the delivery of the appropriate material to increase awareness of AML Compliance.

The MLRO shall ensure that employees of the Company are familiarized with:

(a) Law on AML/CFT;
(b) How to recognize and deal with activities that may be related to ML/CTF;
(c) Policies, procedures, and systems and controls of AML in the Company;
(d) STR and the types of activities that should be reported;
(e) relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions; and
(f) The roles and responsibilities of employees.

Training Obligations

The Company will take appropriate measures to ensure that our relevant employees are:

a) made aware of the law relating to money laundering and terrorist financing;
b) regularly given training in recognizing and dealing with transactions and other activities or situations that may be related to ML/TF;
c) understand our AML Policy and any changes thereto;
d) understand the risk of tipping-off and how to avoid informing a customer or

potential customer that it is or may be the subject of an STR;

e) understand the roles and responsibilities of employees in combating money laundering, including the identity and responsibility of the Company's MLRO and deputy, where applicable; and

f) using the policies, and information gained during the training, understanding their responsibilities as well as apply common sense and standards of conducting a regulated business.

Following FIU Order dated 9 August 2021 No 6., there is an obligation for the AML members to be tested according once in 3 (three) years at the National Centre for Civil Service Personnel Management.

Responsible person of the C&E conducts appropriate AML training for each new employee during the first two months after the official registration of such an employee.

C&E will take a risk-based approach to AML training. The company will provide AML training to each employee at intervals appropriate to their roles and responsibilities and no less than once per annum.

ANNEX 1.

KYC IDENTIFICATION REQUIREMENTS – REQUIRED IN ALL SITUATIONS

Although this Annex sets out the fundamental identification requirements, you should note the principles explained in the main body and ensure you understand the structure and ownership. Note that in this Annex 'current' means no older than three months. All documents with expiry dates (such as passports, driving licences and identity cards) must be in force as of the date of receipt.

Entity type	Documents to request	Notes
Individual	Proof of name and identity the original (or if that is not available a certified copy) of one of the following: ● Signed passport;	If any of the original documents cannot be obtained other original documentation not listed here or an entry on the electoral register may be acceptable but you will need the consent of the MLRO to accept any documents not listed in this table.
	AND Proof of address of the original (or if that is not available a certified copy) of one of the following: ● Current council tax or utility bill; ● Current bank or building society statement containing current address; ● Current mortgage statement; Proof of address from an official overseas source;	It is understood that postal addresses are not available in all jurisdictions and that in some jurisdictions utility bills will often be in the name of an employer rather than an individual. In those circumstances, a signed passport is acceptable as evidence of identity and an identity card, if it shows an address, a residence permit or other current verifiable government document, as evidence of the location of the individual.
Partnerships	You must verify the identity of the partner with whom you are dealing in relation to the transaction plus one other partner plus any other partner who owns or controls 25% more of the partnership in terms of capital, voting rights or profits. You should do this in the same way as verifying the identity of an individual as set out above	If the partnership is made up of regulated professionals (solicitors, accountants, estate agents, tax advisors and insolvency practitioners) proof of its existence and current business address from the relevant professional directory or reputable professional directory is sufficient.
Trusts	You must verify the identity of at least two of the trustees, including one with whom you are dealing in relation to the transaction. The identification requirements you need will depend on the nature of the trustee, so for example, if the trustee is a private company, follow the requirements in this table for private companies, and if the trustee is an individual, follow the requirements in this table for individuals. You must check and understand the documents establishing trust. This is likely to involve a request for a trust structure chart.	

	You must also identify any ultimate beneficial owner with 25% or more interest in the trust. You should do this in the same way as verifying the identity of individual loan or recoverable grant recipients as set out above	
Companies listed on a recognized stock exchange	You must obtain: ● Certificate of Incorporation Evidence of the listing which can be found in most newspapers or on the relevant exchange website	
Majority owned subsidiaries of companies listed on a regulated market	You must identify the parent company (see above requirements): Companies registered on a recognised Stock Exchange. You must also obtain proof of the parent/subsidiary relationship such as the last filed annual report or a note from the parent's last audited accounts.	If the company structure is complex, ask to see a corporate structure chart (you need to ask the applicant to provide this). Once you receive the structure chart you should check it against publicly available information at Companies House (eg you can do this by searching the company names at the relevant public companies house equivalent) and/or using an Online Check.
Private companies	You must obtain the following: ● Certificate of Incorporation ● A current Companies House or equivalent search. To do this you need to search the company name at https://beta.companieshouse.gov.uk /to prove the company remains active and registered. You must also verify the identity of the officer with whom you are dealing in relation to the transaction. You should do this in the same way as verifying the identity of the individual as set out above You must also identify any ultimate beneficial owner, being a living individual who owns 25% or more of the shares in the company or otherwise controls 25% or more of the company. You should do it in the same way as verifying the identity of an individual as set out above	If the company structure is complex, ask to see a corporate structure chart (you need to ask the applicant to provide this). Once you receive the structure chart you should check it against publicly available information at Companies House or equivalent (you can do this by searching the company names at Companies House online) and/or using an Online Check. If it is not possible to identify any of the group entities using these sources then this must be discussed with the MLRO. Once you have checked the structure chart, you need to verify the identity of all of the UBOs – i.e. the bottom of the ownership chain. See the Guidance Notes at the foot of this table for practical guidance on carrying this out
Companies listed overseas – European Economic Area (EEA)	If the company is listed (or is a subsidiary of a listed company) on a regulated market in an EEA state, the evidence required is the same as should be. obtained for companies as set out above You must also verify the identity of the officer with whom you are dealing in relation to the transaction. You should do this in the same way as verifying the identity of an individual as set out above.	If the company structure is complex, ask to see a corporate structure chart (you need to ask the applicant to provide this). Once you receive the structure chart you should check it using an Online Check. If it is not possible to identify any of the group entities using these sources then this must be discussed with the MLRO.
Companies listed overseas – outside	You must obtain: ● A company search of the local	If the company structure is complex, ask to see a corporate

EEA	registry or reputable listing (to include the listing of directors); Proof from the company that the director we are dealing with is authorised on behalf of the company. This should be a written Letter-confirmation on company letterhead or a suitable board minute You must also verify the identity of the officer with whom you are dealing in relation to the transaction. You should do this in the same way as verifying the identity of individual loan or recoverable grant recipients as set out above.	structure chart (you need to ask the customer to provide this). Once you receive the structure chart you should check it using an Online Check. If it is not possible to identify any of the group entities using these sources then this must be discussed with the MLRO.
Unlisted and private overseas companies	You must obtain: ● Official evidence of a registered address; ● Copy of documents required by law to form the company (and details of any change of name); ● Copy of the register of shareholders/members and directors; Proof from the company that the director we are dealing with is authorised on behalf of the company. This should be a written Letter-confirmation on the company letterhead or a suitable board minute You must also verify the identity of the officer with whom you are dealing in relation to the transaction. You should do this in the same way as verifying the identity of individual loan or recoverable grant recipients as set out above. You must also identify any ultimate beneficial owner being a living individual who owns 25% or more of the shares in the company or otherwise controls 25% or more of the company. You should do this in the same way as verifying the identity of individual loan or recoverable grant recipients as set out above.	If the company structure is complex, ask to see a corporate structure chart (you need to ask the customer to provide this). Once you receive the structure chart you should check it using an Online Check. If it is not possible to identify any of the group entities using these sources then this must be discussed with the MLRO. Once you have checked the structure chart, you need to verify the identity of all of the UBOs – i.e. the bottom of the ownership chain.

High-Risk Business Activity

Private Banking	is generally understood to be the provision of personalised banking and/or investment services to high-net-worth customers in a closely managed relationship. It may involve complex, bespoke arrangements and high-value transactions across multiple countries and territories. P.B.: is offered or proposed to personal, private customers, customers (either directly or through a legal person or legal arrangement) identified by the firm as being eligible for the service on the basis of their net worth; (b) involves high-value investment; (c) is non-standardised; and (d) is tailored to the customer's needs
Concerns that company's formation is outside of companies incorporation country	If Company has registered in one place and is regulated by the other jurisdiction.

Involving third-party business activity	any business arrangement between an organization and another entity, by contract or otherwise. You already recognize that companies with which you have contracts and business transactions such as vendors, suppliers, distributors and contractors are third parties.
Remote Customer services	Applicants conducting services to its customer remotely
Personal Brokerage Services in International Market	means a private business entity offering contract auditor recruitment services.
Asset Trust Management	An asset management company (AMC) is a firm that invests pooled funds from customers, putting the capital to work through different investments including stocks, bonds, real estate, master limited partnerships, and more. Trust Management is a legal entity that can serve as an agent or trustee on behalf of a trust
Product or operation which is subject to anonymity[25]	Is a service which is assigned to an anonymous customer. The customer is still unknown, so no customer ID is assigned to the service.
The new product includes new tech	IS service involving the use of new technologies.
Concerns that Company is incorporated outside of KZ	Applicant that is incorporated outside of KZ
Concerns that companies formation is outside of the country of effective management	Applicant is registered in one jurisdiction but operating and conducting business in another jurisdiction
Undocumented service	Service that is not written and documented in any of Company documents
Service engages nominee management and Shareholder	If Director or Shareholder is nominee

Guidance Notes on carrying out CDD on complex group structure charts.

a. If it is not possible to identify any of the group entities using these sources then this must be discussed with the MLRO.
b. Once you have checked the structure chart, you need to verify the identity of all of the relevant UBOs. For example, if a company is owned by two 50% parent companies, and one of those is jointly owned by two individuals, whereas the other is jointly owned by 5 individuals, then the two individuals would each be UBOs, owning 25% of the recipient (i.e. 50% x 50%), whereas the 5 individuals would not be UBOs, owning only 10% of the recipient each (i.e. 20% x 50%), and so their identities would not require verification (See Diagram A below).

c. You need to consider all shareholdings held by each individual. For example, if a company (the 'C&E's Customer') is owned by two 50% parent companies, which each, in turn, have two 50% parent companies, each of which is owned by the same two individuals, then each individual ultimately owns 50% of the loan recipient company via their aggregated shareholdings, and so are each UBOs (See Diagram B below).

[25] https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-A ML-CFT.pdf

d. Whilst you do need to check the group structure chart, you do not need to verify the identity of each entity within the group (except the EDD case), just the direct recipient of the funds and any UBOs.

Diagram A

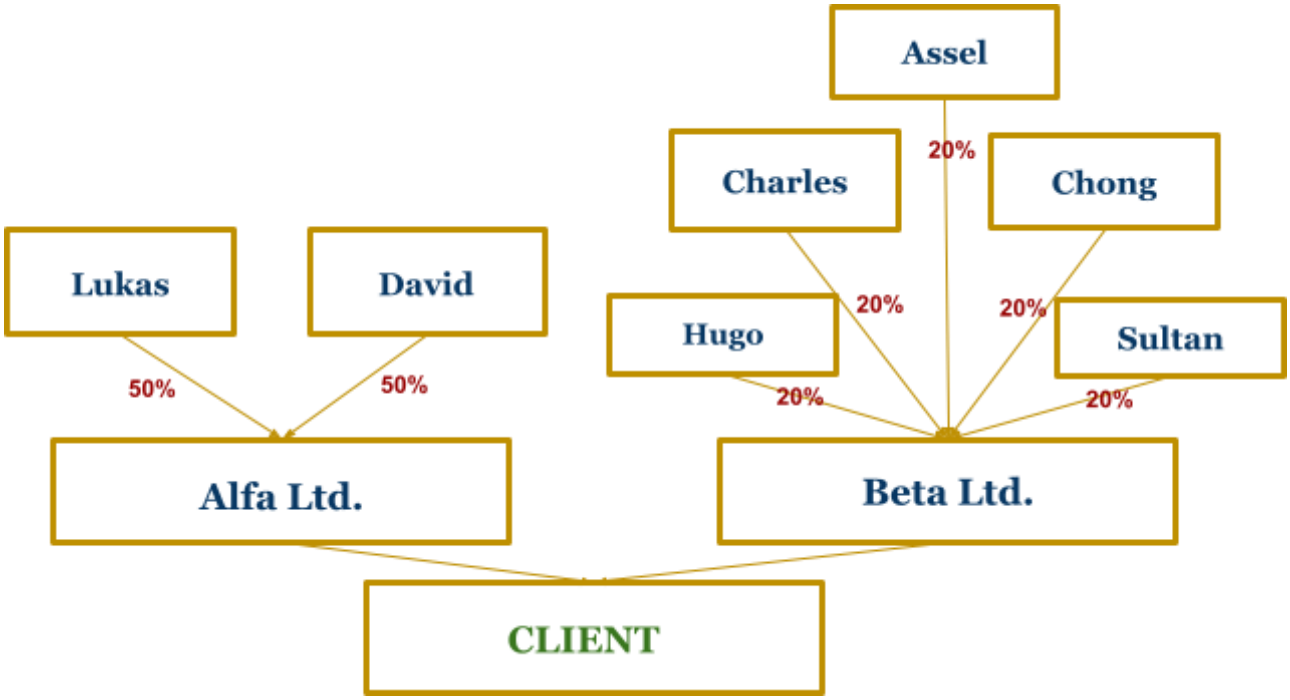
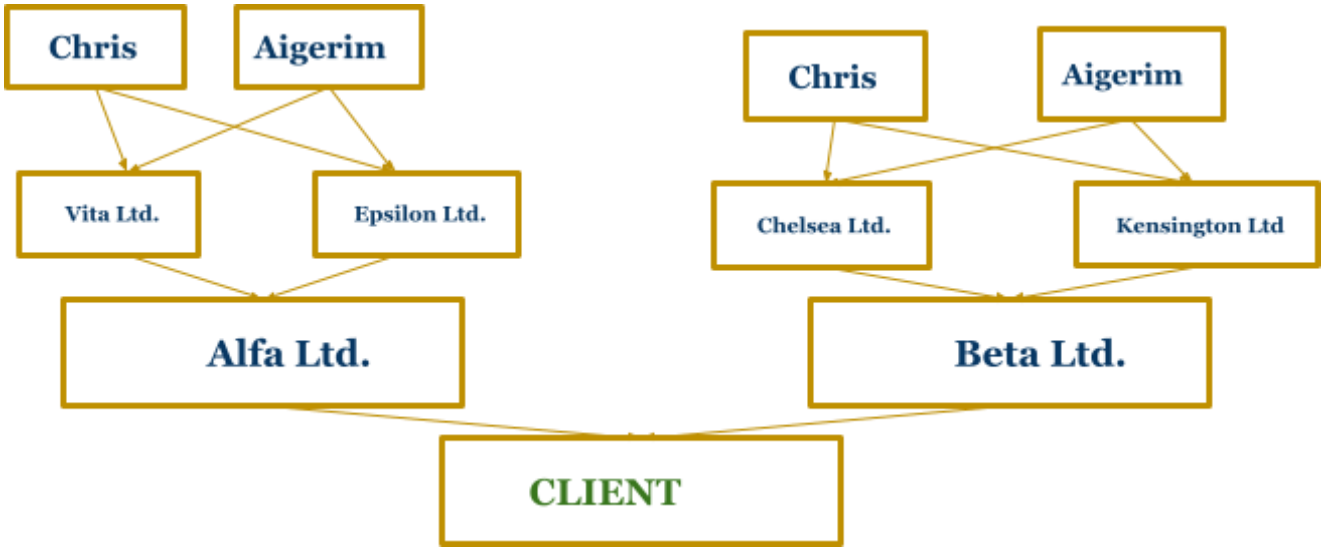


Diagram B



High-Risk Business Jurisdictions

Company considers Customers that are organized or conduct business in any of the jurisdictions, mentioned in the following lists, to have inherent higher ML/TF risk:

- United Nations Security Council Sanctions list based on the resolutions against terrorism https://www.un.org/securitycouncil/content/un-sc-consolidated-list;
- FATF High-Risk Jurisdictions subject to a Call for Action (FATF „blacklist") https://www.fatf-gafi.org/en/countries/black-and-grey-lists.
- European Union restrictive measures https://www.sanctionsmap.eu/;
- The Office of foreign Assets Control of the US Department of the US Department of the Treasury (OFAC) sanctions list https://sanctionssearch.ofac.treas.gov;
- United Kingdom sanctions list https://www.gov.uk/government/publications/the-uk-sanctions-list;

ANNEX 2.

I. LISTS OF TRANSACTIONS/OPERATIONS AS A SUSPICIOUS

1) Customer-related:

- A customer who has requested, without reasonable explanation, transactions that are out of the ordinary range of services normally requested, or are outside the experience of the financial services business in relation to the particular customer;
- A customer's legal or mailing address is associated with other apparently unrelated accounts; or does not seem connected to the customer;
- The source of the funds is unclear or not consistent with the customers' profile and apparent standing;
- Customer, who is a public official, opens account in the name of a family member who begins making large deposits not consistent with the known sources of legitimate family income;
- Transaction involves unfamiliar countries or islands that are hard to find on an atlas or map;
- Agent, attorney or financial advisor acts for another person without proper documentation, such as a power of attorney;
- A customer who refuses to provide the information requested without reasonable explanation or who otherwise refuses to cooperate with the CDD and/or ongoing monitoring process;
- A customer who has entered into a business relationship uses the relationship for a single transaction or for only a very short period without a reasonable explanation;
- A customer who does not exhibit any concern with the cost of transactions or fees;
- A customer who is known to have criminal, civil or regulatory proceedings against it for corruption, misuse of public funds, other financial crimes or regulatory non-compliance, or is known to associate with such persons, and etc.

2) Unusual activity indicative of trade-based money laundering:

- Discrepancies in the description of goods or commodity in the invoice or of the actual goods shipped;
- No apparent business relationship between the parties and transactions;
- Funds transferred into an account and moved to a high-risk country in the same amount;
- Companies operating in jurisdictions where their business purpose is not fully understood and there are difficulties in determining ownership;
- Lack of appropriate documentation to support transactions;

3) Unusual activity indicative of potential terrorist financing:
(a) Behavior indicators:

- The parties to the transaction (owner, beneficiary, etc.) being from countries known to support terrorist activities and organizations;
- Use of false corporations, including shell companies;
- Inclusion of the individual in the United Nations Sanctions list;
- Media reports that the account holder is linked to known terrorist organization or engaged in terrorist activities;
- Beneficial owner of the account is not properly identified;
- Use of nominees, trusts, family member or third-party accounts;
- Use of false identification;
- Abuse of nonprofit organizations;

(b) Indicators linked to financial transactions:

- The transaction is not economically justified considering the account holder's business or profession;
- A series of complicated transfers of funds from one person to another as a means to hide the source and intended use of the funds;
- Transactions that are inconsistent with the account's normal activity;
- Deposits were structured below the reporting requirements to avoid detection;
- No business rationale or economic justifications for the transactions;
- Use of multiple foreign bank accounts.

4) Unusual activity for virtual currency (VC), virtual assets (VA), virtual asset service providers (VASPs):

- Structuring transactions with VA (transactions of exchange or transfer), carried out in a similar way to structuring transactions with cash, by breaking into small amounts or into amounts that do not exceed the thresholds established for mandatory registration of transactions or for reporting;
- Making multiple high-value transactions or in short succession, such as within a 24-hour period; or in a staggered and regular pattern, with no further transactions recorded during a long period afterwards (which is particularly common in ransomware-related cases) or to a newly created or to a previously inactive account;
- Transferring VAs immediately to multiple VASPs, especially to VASPs registered or operated in another jurisdiction where there is no relation to where the customer lives or conducts business; or o there is non-existent or weak AML/CFT regulation;
- Depositing VAs at an exchange and then often immediately –
  (i) withdrawing the VAs without additional exchange activity to other VAs (which is an unnecessary step and incurs transaction fees);
  (ii) converting the VAs to multiple types of VAs, again incurring additional transaction fees, but without logical business explanation (e.g. portfolio diversification); or
  (iii) withdrawing the VAs from a VASP immediately to a private wallet (this effectively turns the exchange/VASP into an ML mixer);
- Accepting funds suspected as stolen or fraudulent –
  (i) depositing funds from VA addresses that have been identified as holding stolen funds, or VA addresses linked to the holders of stolen funds.

(a) Indicators related to Transaction Patterns

New user transactions

- Conducting a large initial deposit to open a new relationship with a VASP, while the amount funded is inconsistent with the customer profile;
- Conducting a large initial deposit to open a new relationship with a VASP and funding the entire deposit the first day it is opened, and that the customer starts to trade the total amount or a large portion of the amount on that same day or the day after, or if the customer withdraws the whole amount the day after (as most VAs have a transactional limit for deposits, laundering in large amounts could also be done through over-the-countertrading);
- A new user attempts to trade the entire balance of VAs, or withdraws the VAs and attempts to send the entire balance off the platform;

Transactions relative to all users

- Transactions involving the use of multiple VAs, or multiple accounts, with no logical business explanation;
- Frequent transfers in a certain period of time (e.g. a day, a week, a month, etc.) to the same VA account – or by more than one person; or from the same IP address

by one or more persons; or concerning large amounts;

- Incoming transactions from many unrelated wallets in relatively small amounts (accumulation of funds) with subsequent transfer to another wallet or full exchange for fiat currency. (Such transactions by a number of related accumulating accounts may initially use VAs instead of fiat currency);
- Conducting VA-fiat currency exchange at a potential loss (e.g. when the value of VA is fluctuating, or regardless of abnormally high commission fees as compared to industry standards, and especially when the transactions have no logical business explanation);
- Converting a large amount of fiat currency into VAs, or a large amount of one type of VA into other types of VAs, with no logical business explanation.

(b) Indicators related to anonymity:

- Transactions by a customer involving more than one type of VA, despite additional transaction fees, and especially those VAs that provide higher anonymity, such as anonymity-enhanced cryptocurrency (AEC) or privacy coins;
- Moving a VA that operates on a public, transparent blockchain, such as Bitcoin, to a centralised exchange and then immediately trading it for an AEC or privacy coin;
- Customers that operate as an unregistered/unlicensed VASP on peer-to-peer (P2P) exchange websites, particularly when there are concerns that the customers handle huge amounts of VA transfers on its customer's behalf, and charge higher fees to its customer than transmission services offered by other exchanges. Use of bank accounts to facilitate these P2P transactions;
- Abnormal transactional activity (level and volume) of VAs cashed out at exchanges from P2P platform associated wallets with no logical business explanation;
- VAs transferred to or from wallets that show previous patterns of activity associated with the use of VASPs that operate mixing or tumbling services or P2P platforms;
- Transactions making use of mixing and tumbling services, suggesting an intent to obscure the flow of illicit funds between known wallet addresses and darknet marketplaces;

(c) Indicators related to senders or recipients:

Irregularities observed during account creation

- Creating separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed by VASPs;
- Transactions initiated from non-trusted IP addresses, IP addresses from sanctioned jurisdictions, or IP addresses previously flagged as suspicious;
- Trying to open an account frequently within the same VASP from the same IP address;

Irregularities observed during CDD process

- Incomplete or insufficient KYC information, or a customer declines requests for KYC documents or inquiries regarding source of funds;
- Sender / recipient lacking knowledge or providing inaccurate information about the transaction, the source of funds, or the relationship with the counterparty;
- Customer has provided forged documents or has edited photographs and/or identification documents as part of the on-boarding process;

Customer Profile

- A customer provides identification or account credentials (e.g. a non-standard IP address, or flash cookies) shared by another account;
- Discrepancies arise between IP addresses associated with the customer's profile and the IP addresses from which transactions are being initiated;
- A customer's VA address appears on public forums associated with illegal activity;
- A customer is known via publicly available information to law enforcement due to

previous criminal association;

Profile of potential money mule or scam victims

- Sender does not appear to be familiar with VA technology or online custodial wallet solutions. Such persons could be money mules recruited by professional money launderers, or scam victims turned mules who are deceived into transferring illicit proceeds without knowledge of their origins;
- A customer significantly older than the average age of platform users opens an account and engages in large numbers of transactions, suggesting their potential role as a VA money mule or a victim of elder financial exploitation;
- A customer being a financially vulnerable person, who is often used by drug dealers to assist them in their trafficking business;
- Customer purchases large amounts of VA not substantiated by available wealth or consistent with his or her historical financial profile, which may indicate money laundering, a money mule, or a scam victim;

Other unusual behaviour

- A customer frequently changes his or her identification information, including email addresses, IP addresses, or financial information, which may also indicate account takeover against a customer;
- A customer tries to enter into one or more VASPs from different IP addresses frequently over the course of a day;
- Use of language in VA message fields indicative of the transactions being conducted in support of illicit activity or in the purchase of illicit goods, such as drugs or stolen credit card information;
- A customer repeatedly conducts transactions with a subset of individuals at significant profit or loss. (This could indicate potential account takeover and attempted extraction of victim balances via trade, or ML scheme to obfuscate funds flow with a VASP infrastructure).

(d) Indicators related to the source of wealth or funds:

- Transacting with VA addresses or bank cards that are connected to known fraud, extortion, or ransomware schemes, sanctioned addresses, darknet marketplaces, or other illicit websites;
- VA transactions originating from or destined to online gambling services;
- The use of one or multiple credit and/or debit cards that are linked to a VA wallet to withdraw large amounts of fiat currency (crypto-to-plastic), or funds for purchasing VAs are sourced from cash deposits into credit cards;
- Deposits into an account or a VA address are significantly higher than ordinary with an unknown source of funds, followed by conversion to fiat currency, which may indicate theft of funds;
- Lack of transparency or insufficient information on the origin and owners of the funds, such as those involving the use of shell companies or those funds placed in an Initial Coin Offering (ICO) where personal data of investors may not be available or incoming transactions from online payments system through credit/pre-paid cards followed by instant withdrawal;
- A customer's funds which are sourced directly from third-party mixing services or wallet tumblers;
- Bulk of a customer's source of wealth is derived from investments in VAs, ICOs, or fraudulent ICOs, etc;
- A customer's source of wealth is disproportionately drawn from VAs originating from other VASPs that lack AML/CFT controls.

(e) Indicators related to geographical risks:

- Customer's funds originate from, or are sent to, an exchange that is not registered in the jurisdiction where either the customer or exchange is located;

- Customer utilises a VA exchange or foreign-located MVTS in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for VA entities, including inadequate CDD or KYC measures;
- Customer sends funds to VASPs operating in jurisdictions that have no VA regulation, or have not implemented AML/CFT controls;
- Customer sets up offices in or moves offices to jurisdictions that have no regulation or have not implemented regulations governing VAs, or sets up new offices in jurisdictions where there is no clear business rationale to do so.

II. LISTS ON OPERATIONS SUBJECT TO FINANCIAL MONITORING AND GROUNDS FOR REPORTING SUSPICIOUS TRANSFERS

1) List of operations subject to financial monitoring:

- any suspicious transfers
- KZT 5M | outcoming transfer abroad to anonymous holder
- KZT 5M | incoming transfer from abroad from anonymous holder
- KZT 5M | outcoming transfer to customer with factual offshore address, registered offshore address
- KZT 5M | incoming transfer of customer with factual off-shore address, registered offshore address
- KZT 5M | outgoing & incoming transfer by customer with offshore account
- KZT 5M | outgoing & incoming transfer by customer with factual offshore address
- KZT 5M | outgoing & incoming transfer by customer with registering offshore address
- KZT 5M | outgoing & incoming transfer to person with offshore account
- KZT 5M | outgoing & incoming transfer to person with factual offshore address
- KZT 5M | outgoing & incoming transfer to person with registered offshore address
- KZT 7M | outgoing transfer free of charge
- KZT 10M | operations by legal entity within 3 months after officially registering
- KZT 100M | outgoing & incoming cross border transfer
- KZT 200M | transfer related to arrangement with property (transfer of rights from one person to another)

Customer Operations Identification Procedure with characteristics that correspond to typologies, schemes and methods of legalisation (laundering) of proceeds from crime and the financing of terrorism, approved by the Financial monitoring authority in accordance with the AML/CFT Law.

Duties Distribution between the C&E team (employees) on updating customer's (its representatives, beneficial owners) information (previously received) and (or) obtaining additional one.

2) Grounds for reporting suspicious transfers:

- any suspicious transfers
- KZT 5M | outcoming transfer abroad to anonymous holder
- KZT 5M | incoming transfer from abroad from anonymous holder
- KZT 5M | outcoming transfer to a customer with factual offshore address, registered
- offshore address
- KZT 5M | incoming transfer of customer with factual off-shore address, registered offshore address

- KZT 5M | outcoming & incoming transfer by customer with offshore account
- KZT 5M | outcoming & incoming transfer by customer with factual offshore address
- KZT 5M | outcoming & incoming transfer by customer with registering offshore address
- KZT 5M | outcoming & incoming transfer to person with offshore account
- KZT 5M | outcoming & incoming transfer to person with factual offshore address
- KZT 5M | outcoming & incoming transfer to person with registered offshore address
- KZT 7M | outcoming transfer free of charge
- KZT 10M | operations by legal entity within 3 months after officially registering
- KZT 100M | outcoming & incoming cross border transfer
- KZT 200M | transfer related to arrangement with property (transfer of rights from one person to another)

ANNEX 3. CUSTOMER DUE DILIGENCE PROTOCOL

Customer Due Diligence (CDD) Protocol

II. CDD GROUND		
INFORMATION FROM CUSTOMERS DOCS		**DOCUMENTS**
Customer's name		➢ **MUST HAVE:** • Certificate of Incorporation; • Articles of Associations; • Public register of the Company (if relevant); • License (if relevant); • Register of Directors; • Register of Shareholders; • WorldCheck; • AD Media; • Rent Agreement; or • Utility Bill (not less than 3 months); • Bank statement (if relevant) (not less than 3 months); • Bank statement of Shareholder(s) (not less than 3 months); • Invoices; • Contract with suppliers and/or customers. ➢ **DESIRABLE :** • Certificate of good standing; • Certificate of Incumbency; • Salaraly slips; • Financial statement; • Organisational chart; • Loan agreement; • Web-page; • Social Media pages (e.g. LinkedIn, Facebook).
Company's Registration Date		
Address (factual & registered)		
Company's Website/ Linkedin page of the company/Facebook page of the Company		
Customer's Business Activity		
***Regulated activity**		
Customer's Structure		
Customer Managers & TOP Managers, Legal/Physical Address, Virtual address Reputation		
Customer Shareholders | Beneficial Owners, Address, Virtual Address, Reputation		
Source of wealth :		
Source of Funds:		
Expected amount of transactions (operations)	**Per day: Per week: Per month: Per year:**	According to e-mail; +According to application form
Expected amount of sum of transactions of operations	**Per day: Per week: Per month: Per year:**	According to e-mail; +According to application form
Expected location of Customer's Customers, bank's location		According to e-mail; +According to application form

II. CDD OUTCOME	
Level of CDD	• **Standard** • **Enhanced**

AML TEAM'S RECOMMENDATION ON APPLICANT	**ONBOARD**	**Transaction Risk Level:** • **Medium Risk** • **High Risk** **Justification:** xx	**SUBJECT TO APPROVAL OF SEO**
	NOT TO ONBOARD	**Justification:** xx	

The Report is prepared by:
Name
MLRO

The Report is approved by:
Name
Compliance Officer

Should be recorded by the Sales Department and kept for 6 (six) years.

ANNEX 4. TRANSACTION DUE DILIGENCE PROTOCOL

Transaction Due Diligence (TDD) Protocol

I. GROUND FOR TDD		
Date of TDD	dd/mm/yyyy	
Date and Time of Initiation of Transaction	dd/mm/yyyy, --:--	
Transaction ID	xx	
Transaction Amount *(USD, EUR, or any other currency)*	0 USD	
Wallet's address (Sender)	xxxx	
Wallet's address (Recipient)	xxxx	
Transaction amount in KZT	0 (day of exchange currency rate dd/mm/yyyy)	
Provided documents on which Transaction is based	• **Invoice** • **Relevant Agreement**	
Leader/Coordinator of the Project - Operational Department	xx (Please, indicate who is the leader of the transaction)	
<u>Sender</u> **Name of Director** **Address**	**<u>xx</u>** xx	• **C&E Customer** • **Not C&E Customer**
Country where is the bank account of the sender is located[20*]	**xx**	
<u>Recipient</u> **Name of Director** **Address**	**<u>x</u>** **<u>x</u>** x x x x	• **C&E Customer** • **Not C&E Customer**

<table>
<tr><td colspan="2">Country where is the bank account of the recipient is located*</td><td colspan="2">xx</td></tr>
<tr><td colspan="4">II. TDD OUTCOME</td></tr>
<tr><td colspan="2">Level of TDD</td><td colspan="2">• Enhanced</td></tr>
<tr><td rowspan="2"><u>AML TEAM'S RECOMMENDATION ON TRANSACTION</u></td><td>PROCEED</td><td colspan="2"><u>Transaction Risk Level:</u>
• Medium Risk
• High Risk</td></tr>
<tr><td>NOT PROCEED</td><td colspan="2"><u>Justification:</u>
xx</td></tr>
<tr><td colspan="4">III. REQUIREMENTS IN REPORTING</td></tr>
<tr><td colspan="2">FIU Report</td><td colspan="2">• Required
• NOT Required</td></tr>
<tr><td colspan="2">Fintrac Report</td><td colspan="2">• Required
• NOT Required</td></tr>
<tr><td colspan="2">EDD on customer</td><td colspan="2">• Required
• NOT Required</td></tr>
</table>

<u>The Report is prepared by:</u>
Name
MLRO

<u>The Report is approved by:</u>
Name
Compliance Officer

Should be recorded by the Sales Department and kept for 6 (six) years.

ANNEX 5. SUPPLIER DUE DILIGENCE PROTOCOL

Supplier Due Diligence Protocol

Ground of SDD	Information obtained from Supplier's Documents/ Responsible employee	Documents
Date of SDD		
Supplier's Name, Address (factual & registered)		
Newly Incorporated Company		
Website check		
Customer's Business Activity		
Customer Managers & TOP Managers, Address, Reputation		
Leader/Coordinator of the Project - Business Development Department - Initiated by Responsible Officer for Supplier Dossier & Coordination		
Level of expertise and market reputation		
Bank's credit rating is		
The amount of Customer Money placed, as a proportion of its overall capital and deposits is		

The extent to which the Customer Money would be protected under a deposit guarantee protection scheme is		
High Risk Jurisdiction		
The level of risk in the investment and loan activities undertaken by it or members of its Group, where such information is available		
High Risk Partner		
Bank's use of agents and service providers		
The financial position of Bank's Group		
Compliance Officer Recommendation		
Risk Officer Recommendation		
Outsourcing Committee Decision		*The Responsible Officer should present its position to the Outsourcing Committee* *The Outsourcing Committee should make the decision of onboarding/ refusing Customer.*
Ongoing Screening	**Business Development Department**	*Responsible Officer should include the date when the Supplier is classified as …* ***Planned Ongoing Screening Date**: indicate the date after one year of onboarding.* ***Unplanned Ongoing Screening**: will be formed incase of Outsourcing Committee/Business Development*

		Department Officer/Risk Officer detected supplier are suspicious etc.

**This Protocol shall be recorded by the Business Development team and kept for 6 (six) years.*

ANNEX 6. EMPLOYEE DUE DILIGENCE PROTOCOL

Employee Due Diligence Protocol

Ground of EDD	Information obtained from Employee's Documents/ Responsible employee	Documents
Date of EDD		
Employee's Name, contact number		
Address (factual & registered)		
Passport/Identification check (with photo)		
Website check		
Education		
Medical records		
Criminal Record		
Position in C&E		
Location		
Type of contract		
NDA		
First day of work		
Leader/Coordinator of the Project - HR Department - Initiated by Responsible Officer for Employee Dossier & Coordination		

Security Department Recommendation		
Compliance Officer Recommendation		
Risk Officer Recommendation		
Compliance Committee Decision		

**This Report shall be recorded by the HR Department and kept for 6 (six) years.*

ANNEX 7. RISK ASSESSMENT QUESTIONNAIRE

RISK ASSESSMENT QUESTIONNAIRE

COMPANY DETAILS	
• **Company name:** • **Registered address:** • **City:** • **Zip code:** • **Country:** • **Telephone no:** • **Company registration no:** • **Date of incorporation:** • **Tax ID/VAT number:** • **Company Website:** • **Company Email:** • **Brief description of Company's primary activity:**	
Is the Company providing regulated services?	• Yes • No
EXPECTED TRANSFER ACTIVITY	
• **Main countries to which you will make transfers:** • **Main countries from which you will receive transfers:** • **Estimated number of outgoing transfers per month:** • **Estimated number of incoming transfers per month:** • **Average value of each transfer:** • **Maximum value of each transfer:**	
AUTHORISED SIGNATORY DETAILS	
• **First name:** • **Last name:** • **Address:** • **City/State:** • **Zip code:** • **Country:** • **Nationality:** • **Passport/ID no:** • **Passport Issue Date:** • **Passport Expiry Date:** • **Telephone no:** • **Fax no:** • **Signatory email address:**	

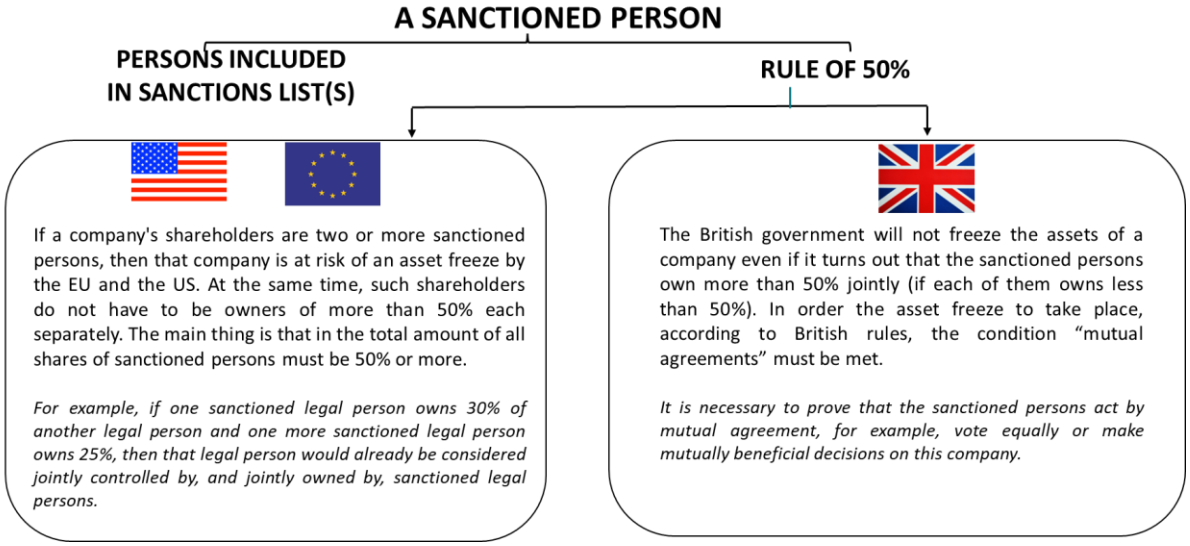
Is the Authorised signatory a politically exposed person?	• Yes • No
Is the Authorised signatory in the United Nations Security Council Consolidated List?	• Yes • No
DIRECTOR(S) OF THE COMPANY	
• **First name:** • **Last name:** • **Country:** • **Nationality:** • **Passport/ID no:** • **Passport Issue Date:** • **Passport Expiry Date:** • **Address:** • **Phone no:** • **Email address:**	
Is the Director a politically exposed person?	• Yes • No
Is the Director in the United Nations Security Council Consolidated List?	• Yes • No
Is/was senior managers (decision maker persons), UBO, founder - individual of the Customer or his\her close relatives PEP?	• Yes • No
Is/was senior managers (decision maker persons), UBO, founder - individual of the founder or his\her close relatives PEP?	• Yes • No
ULTIMATE BENEFICIARY DETAILS	
• **Share (%):** • **First name:** • **Last name:** • **Nationality:** • **Passport/ID no:** • **Passport Issue Date:** • **Passport Expiry Date:** • **Address:** • **Phone no:** • **Email address:**	
SOURCE OF INITIAL FUNDING	

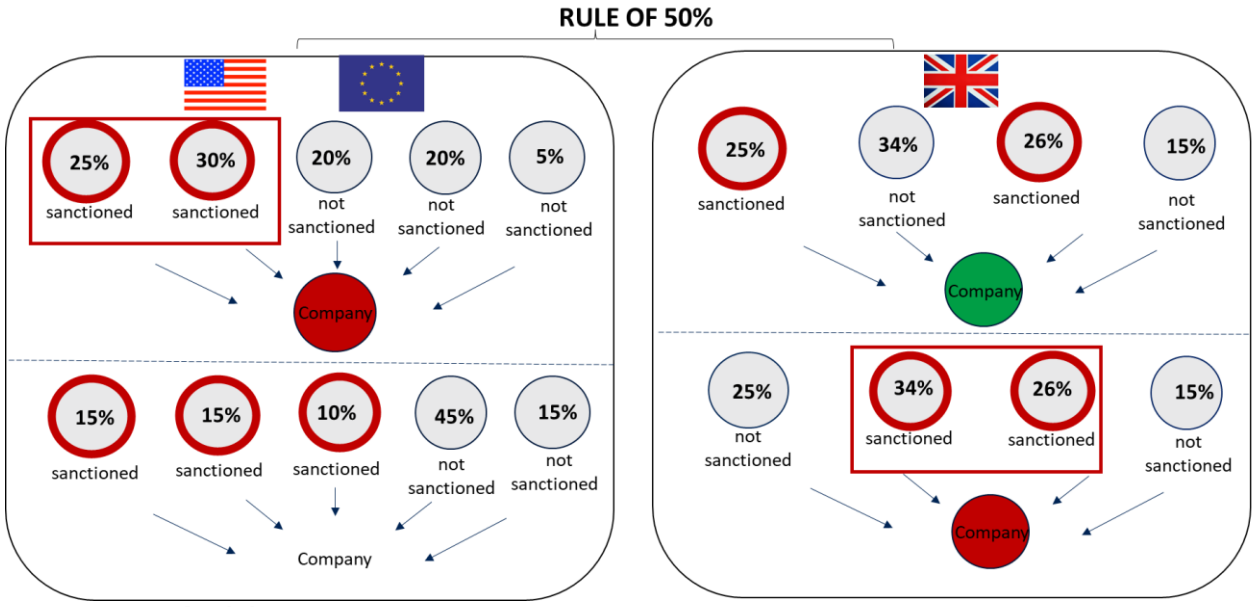
• **Value Of Initial Funding:** • **Currency of Initial Funding:** • **Originating Bank Name:** • **Originating Bank Address:** • **Account Name:** • **Account Number:** • **Signatory:**	
Describe precisely how these funds were generated:	
SANCTIONS COMPLIANCE	
Is/Are the company or connected/related parties, company's ultimate parent or subsidiary/subsidiaries incorporated; or have any offices, reside, or operate/have business activities in the following countries/jurisdictions associated with sanctions? **If yes, which country/countries?**	• Yes • No
Does your company have policies and procedures on sanctions compliance?	• Yes • No
Does your company procure, provide services, goods, collaborate with individuals or entities which are included in sanctions list(s)?	• Yes • No
Does your company procure, provide services, goods, collaborate with individuals or entities which are not in a sanctioned list but residents of countries associated with sanctions?	• Yes • No
DETAILS ABOUT YOUR PRIMARY CURRENT ACCOUNT	
Account currency:	
Enter an account name for your reference (optional):	
INTERMEDIARY	
Recommended by:	
CONCOMPANYATIONS	

I/we concompany that all information provided above is correct and true	• Yes • No
I/we shall notify the Collect & Exchange Ltd. immediately if any representation, undertaking or concompanyation contained herein, or any information provided, becomes, or is likely to become untrue or inaccurate in whole or in part, at any time, as it is stipulated in sections 8.16 and 8.17 of the General Terms of Services of Collect & Exchange Ltd	• Yes • No

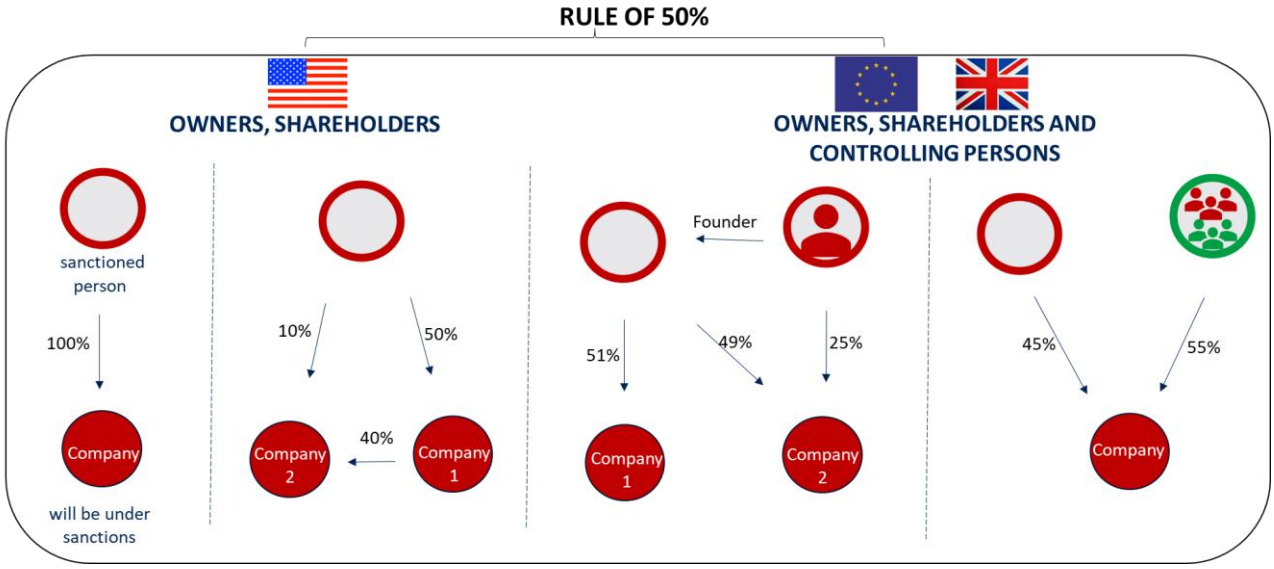
The AML team of Collect & Exchange Ltd. may require additional supporting documents or information. We want to ensure that our company will deliver the fastest and high-quality services to you in line with the Acting Law of the AIFC, relevant laws and regulations, as well as the best international standards.

ANNEX 8. RULE OF 50%





Scenario (a):


RULE OF 50%
OWNERS, SHAREHOLDERS
OWNERS, SHAREHOLDERS AND CONTROLLING PERSONS
sanctioned person
100%
Company
will be under sanctions
10%
50%
Company 2
40%
Company 1
Founder
51%
49%
25%
Company 1
Company 2
45%
55%
Company

Scenario (b):