Anti-Money Laundering and Counter-Terrorist Financing Policy

Contents

1. Overview

This Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) policy will outline Bigness Coin's strategy and objectives for protecting Bigness Coin's products and services from being used for illicit purposes of money laundering, financing of terrorism, financial crime, and breach of national and international financial sanctions.

By implementing this policy, Senior Management of Bigness Coin are putting in place specific processes and procedures to provide detailed requirements and instructions for the employees of Bigness Coin. This is to ensure proper implementation of AML and CTF controls.

1.1 Applicability

Bigness Coin offers customers a range of bespoke products and services related to cryptocurrencies and blockchain technology, including cryptocurrency exchange, wallet, investment services and ICO. Bigness Coin products and services can be found on the Bigness Coin app.

This policy is applicable to all service operations of Bigness Coin, and the responsibilities thereof.

1.2 Regulation

Bigness Coin will act in accordance with the AML and CTF rules as defined in the following legislation and guidance documents:

- The 5th Anti-Money Laundering Directive (AMLD5) of the European Union.
- Directive (EU) 2018/843 of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (5th Anti-Money Laundering Directive or AMLD5).
- Regulation (EU) 2015/847 on information accompanying transfers of funds.
- Regulation (EU) 2018/1672 on controls on cash entering or leaving the Union.
- European Central Bank (ECB) guidelines on AML and CTF.
- EU Directive 2014/42/EU on the freezing and confiscation of instrumentalities and proceeds of crime.
- EU Regulation 2016/794 on Europol's support to Member States in counter-terrorism efforts.

1.3 Changes and Revisions

This document shall be subject to periodic reviews in accordance with changes in:

- Local and international legislation.
- Industry best-practice.
- Internal changes in the business that impact the products available and relevant revenue streams.

Senior Management must approve all changes before they are put into effect. Minor changes shall be reflected by incrementing the version number as 1.1, 1.2, 1.3, etc.

Where significant changes to the document are made, these shall be reflected in a new version number as 1.0, 2.0, 3.0, etc.

2. Money Laundering and Terrorist Financing

Money laundering is generally defined as the process by which the proceeds of crime, and the true ownership of funds, are changed or falsified so that they appear to come from a legitimate source. This process is often achieved by converting funds into other forms by the creation of multiple transaction layers.

A money laundering offence may be committed if a person:

- Conceals, disguises, or transfers criminal property.
- Enters or becomes involved in an arrangement which they know, or suspect facilitates the acquisition, retention, use or control of criminal property on behalf of another person.
- Acquires, uses, or has possession of criminal property.

All financial institutions are required to prevent and deter criminals from using their products and services for financial crime. Specifically, the laundering of the proceeds of crime or the funding of terrorism.

Therefore, it is important that Bigness Coin understands the methods of money laundering so that appropriate and proportionate controls can be applied internally.

2.1 Three Stages of Money Laundering

Money laundering is traditionally broken down into three separate steps which aim to conceal the origins of illicit funds and introduce them into legitimate financial systems.

However, it should be noted this is not a rule of money laundering and alternative methods can be applied.

2.1.1 The First Stage, Placement

This is the first point of contact between illicit funds and the financial system. This includes the movement of funds away from its original source and may use several individuals to conduct separate transactions of varying values and types. This breaks up the funds into smaller amounts below noticeable thresholds.

Examples of placement activity may include the following:

- False invoicing to match deposited cash.
- Smurfing, a process of lodging small amounts of money below AML reporting thresholds to bank accounts or credit cards.
- Trusts and offshore companies used to hide the identify of real owners.
- Excessive aborted or refunded transactions where funds are transferred to a third-party, after which the transaction is aborted and reversed, but funds are not returned.

2.1.2 The Second Stage, Layering

Once illicit funds have been placed in the financial system, criminals may move the funds around to separate the funds from their source and make it harder to establish the true origin of the funds.

This stage can take many different forms such as multiple bank transfers or making investments in other forms of capital.

Layering serves to make tracing transactions as hard as possible, and known methods are:

- Funds converted into monetary instruments or assets.
- Buying material items then selling at price points that do not make logical sense for the item being sold.

2.1.3 The Third Stage, Integration

In the final stage, the funds are used as if legitimately derived, with a seemingly legitimate origin. Here they can be used without detection or arousing suspicion. In the final stage, the overall aim of the laundering process is completed.

Finalising the integration process may include large payment settlements such as:

- The sale of property or transference of assets through shell companies.
- False loans.
- False import and export of goods.

2.2 Penalties and Offences

Failing to adhere to the regulatory obligations of AML comes with several penalties linked to relevant offences. These can be applied to both Bigness Coin employees at a personal level, as well as Bigness Coin as a financial institution. In addition, any breach of money laundering regulation could cause significant damage to the reputation of Bigness Coin and its employees.

Non-compliance with money laundering obligations by Bigness Coin employees is considered a serious offence. In the event of non-compliance by an employee, disciplinary actions will be taken by Bigness Coin which can include immediate dismissal. Therefore, it is important Bigness Coin understands not only the corporate responsibilities regarding the prevention of financial crime, but also the penalties if there was failure to fulfil them. Additionally, understanding the offences that can be committed has helped shape Bigness Coin's AML policies and procedures.

As outlined in the AMLD5, it would be a criminal offence to:

- Conceal, disguise, convert, transfer, or remove criminal property from the EU.
- Enter into an arrangement which you know, or suspect facilitates the acquisition, retention, use or control of criminal property.
- Acquire, use, or possess criminal property.
- These offences carry a maximum of fourteen years' imprisonment.

2.2.1 Failure to Report

It is an offence for any person who acquires knowledge, suspicion, or reasonable grounds to suspect money laundering not to report this as soon as it is reasonably practical after the information came to their attention.

Therefore, an offence can be committed if there is a failure to report any knowledge or suspicion of money laundering within Bigness Coin. This offence relates not only to information concerning Bigness Coin customers, but regarding any engagement where information passes through Bigness Coin.

It would also be a criminal offence to fail to report suspicion of money laundering in circumstances where:

- It is known or suspected, that there are reasonable grounds for suspecting, that another is engaged in money laundering.
- That knowledge or suspicion has come to light in the course of business in the financially regulated sector.
- The whereabouts of a suspect or any laundered property can be identified, or it is reasonable to believe that the information will or may assist in identifying the suspect or the whereabouts of the laundered property.

Failure to report in these circumstances is punishable upon conviction by a maximum of five years imprisonment, a fine or both. It may also give rise to the offence of money laundering which carries a penalty of fourteen years' imprisonment or an unlimited fine.

2.2.2 Tipping-off and Prejudicing an Investigation

Under money laundering legislation, it is also an offence to make a disclosure that is likely to prejudice an anti-money laundering investigation, where it is known or suspected that a disclosure to the authorities has been or will be made.

Employees of Bigness Coin could be at risk of committing a tipping-off offence if, after having made a report, being aware of a report, or intending to make a report, it is disclosed to the subject of suspicion that they are under investigation. This can happen accidentally, however ignorance is not a defence against the offence.

To defend against tipping-off, any customer under investigation that contacts Bigness Coin is to be passed onto the Money Laundering Reporting Officer (MLRO).

The offence of prejudicing an investigation can be committed if an employee takes any action that may prejudice an investigation or potential investigation into money laundering. This can be by destroying or concealing information or falsifying information related to the investigation.

The punishment upon conviction for Tipping Off or Prejudicing an investigation is a maximum of two years imprisonment, or a fine, or both.

2.3 Terrorist Financing

In addition to the offences set out in AMLD5, the EU regulatory framework includes specific provisions addressing the financing of terrorism, including the collection and use of funds for terrorist purposes.

Terrorist Financing can be defined as:

- Fund raising, which covers inviting other people to provide money or other property to support terrorism.
- Use and possession, which covers using money or other property for the purpose of terrorism.
- Funding arrangements, which covers a person knowingly entering into an arrangement whereby they provide funding for terrorists.

If an employee of Bigness Coin has reasonable cause to suspect that money or other property may be used for terrorist purposes and the suspicion is not properly reported to the MLRO, then the employee is at personal risk of committing an offence.

Regarding Bigness Coin as a business, an offence is committed if there is involvement in providing money or other property, to be used for the purposes of terrorism, even if the funds are clean in origin.

3. Risk Appetite

Bigness Coin considers financial crime to be unacceptable, unethical and has no appetite for business that puts Bigness Coin into proximity/or involvement with financial crime. Therefore, Bigness Coin will take timely, proper, and proportionate actions to minimise, manage and control the associated risks.

With that in mind, Bigness Coin has a commitment to financial crime prevention, and an approach tailored to promoting best practice techniques along with a high standard of efficient AML and CTF procedures.

To accomplish this task, Bigness Coin has a definitive risk appetite and a clear view on the types and amount of risk Bigness Coin is prepared to take regarding customers, products, services, and business opportunities. It allows for informed decisions to be made and provides clear boundaries when considering Bigness Coin's business development.

3.1 Principles

By implementing principals regarding how Bigness Coin operates its business, Bigness Coin can ensure preservation of reputation with its customers, service providers, partners, and industry in which it operates. These principals will help protect Bigness Coin and its customers from becoming a victim of fraudulent or unlawful activities.

When developing these principals, Bigness Coin shall comply and take guidance from the existing laws and regulations.

Therefore, in accordance with applicable laws and regulations, Bigness Coin shall:

- Deter the use of Bigness Coin's products and services for money laundering, terrorist financing and financial crime purposes.
- Maintain its internal compliance controls, including those related to the prevention of financial crime, AML and CTF.
- Ensure continuous development of internal controls in accordance with any changes in Bigness Coin's products, services, or business activities.
- Continuously identify and assess the risks involved with Bigness Coin's products, services, or business activities.
- Ensure ongoing monitoring of its customers' activities, including monitoring of customers' transactions and carrying out Customer Due Diligence (CDD) prior to entering into an agreement.
- Subject potential customers identified as high risk to Enhanced Due Diligence (EDD) before commencing any business relationship, except in case of confirmed PEPs where the business will not be accepted.
- Identify unusual and suspicious activity or breaches of financial sanctions and prepare relevant SARs.
- Establish controls to postpone or block activity/transactions/accounts where deemed suspicious.
- Ensure the preservation of, and appropriate restriction of access to, information about customers and their activities.
- Ensure the timely and compliant termination of customers which do not meet the compliance requirements of Bigness Coin.
- Protect its reputation by protecting itself and its employees from any unfounded allegations of being involved with criminal activity.
- Ensure that employees have full knowledge and a complete understanding of the AML and CTF obligations imposed on them by this policy and relevant legislation.

Regarding business operations, Bigness Coin does not:

- Tolerate money laundering or terrorist financing and will not knowingly conduct business with individuals believed to be engaged in any type of criminal behaviour.
- Deal with parties in breach of financial sanctions.
- Allow anonymous accounts, nor permit anonymous transfers of funds.
- Provide services to unknown third parties.
- Enter business relationships with customers who do not pass CDD checks.
- Do business with any customer(s) who pose an elevated money laundering or terrorist financing risk which cannot be mitigated by current systems and controls.
- Provide financial services for, or cooperate with:
    - Anonymous customers, companies, or individuals whose identity cannot be verified.
    - Individuals and companies subject to international and national sanctions.
    - Individuals identified as Politically Exposed Persons (PEP).
    - Shell banks/companies.
    - Financial institutions operating without a license.

3.2 Preferred Customer base

Bigness Coin's preferred customer base consists of merchants with a physical and online presence and covers:

- Wholesale.
- Retail.
- Low risk industries.

Bigness Coin has no expectations on customers transactions.

For clarity the following fall outside of Bigness Coin's risk appetite:

- Firms whose ownership involves multiple parenting structures.

As per the above, Bigness Coin will not engage with any customers that fall outside of its risk appetite, any current customers whose operations change to be outside of Bigness Coin's risk appetite are offboarded immediately.

4. Responsibilities and Obligations

Bigness Coin is fully aware of the risk that when providing financial services, Bigness Coin may be targeted by criminals to conduct financial crime, money laundering and terrorist financing. Senior Management are also aware of their responsibility in respect of these risks, including the risks related to Bigness Coin's compliance with regulatory and card scheme requirements.

This document is designed to ensure compliance with EU-wide legislation and regulations concerning anti-money laundering (AML) and counter-terrorism financing (CTF), applicable across all EU member states.

4.1 Senior Management

The Bigness Coin Senior Management consists of owners or employees who have the authority to make decisions that can change Bigness Coin's exposure to money laundering and terrorist financing risk.

Senior Management within their competence implement Bigness Coin's obligations in the prevention of financial crime, money laundering and terrorist financing. Senior Management also approve all policies and procedures for Bigness Coin and supervise the implementation of internal controls.

Senior Management must:

- Appoint an MLRO to implement and monitor Bigness Coin's AML and CTF controls.
- Review and approve the policies and procedures in relation to AML and CTF.
- Review the monthly and annual management information packs detailing Bigness Coin's performance and effectiveness in preventing financial crime.
- Implement any recommendations made by the MLRO.
- Review annually the performance of the MLRO to ensure the role is being adequately filled.
- Ensure that the MLRO has sufficient resources to fulfil their role and has adequate assignment of competent employees.
- Set a corporate culture demonstrating zero tolerance for financial crime.

In short, Senior Management are responsible for overall compliance, ensuring the adequacy of the controls and resources applied to the business. This includes the appointment of a suitable MLRO.

4.2 The Money Laundering Reporting Officer (MLRO)

The main objective of the MLRO is to ensure and control Bigness Coin's activities in the prevention of money laundering and terrorist financing in accordance with the requirements of EU laws and regulations, as well as the national laws of the member states.

The MLRO will act as a focal point within Bigness Coin for all activity relating to AML and CTF and is responsible for overseeing the implementation and operation of the processes as approved by Senior Management. The MLRO may also appoint a nominated officer to assist in the support of MLRO responsibilities, but the MLRO is always ultimately responsible.

The responsibilities of the MLRO and any nominated officer in the prevention of financial crime, AML and CTF are:

- Be the first point of contact for all employees regarding compliance concerns or financial crime prevention.
- The development and implementation of policies and procedures relating to activities of Bigness Coin and its employees in prevention of financial crime, money laundering and terrorist financing.
- Reporting to Senior Management via management information packs on the effectiveness of the current AML and CTF controls.
- Furthering the development of Bigness Coin's internal controls used to identify unusual or suspicious activity.

- Ensuring that the current implemented procedures for the investigation and reporting of suspicious activity is adequate.
- Determining the appropriate actions, investigation and/or termination of customer relationships in response to any SARs raised.
- Sending SARs to Europol or the competent national authorities of EU member states in the event of money laundering and terrorist financing suspicion.
- Cooperation with the European Central Bank (ECB) or the relevant national competent authorities regarding ongoing compliance or any SARs raised.
- Provide appropriate training and advice to Bigness Coin employees regarding AML and CTF obligations.
- Arrangement of internal risk assessments regarding Bigness Coin's products and services.
- Keeping up to date in changes in applicable regulations or Bigness Coin business activity.

Senior Management will ensure that the MLRO has a sufficient level of authority and independence within the company and that they have access to sufficient resources and information to carry out their responsibilities.

The MLRO will be subject to Bigness Coin's performance management process to ensure ongoing competence in the role of MLRO.

4.3 Compliance Monitoring Team

The Bigness Coin Compliance Monitoring Team's main objective is to conduct independent investigations of alerts and flags generated in the automatic screening systems applied to transaction monitoring and customer onboarding.

The Compliance Monitoring Team is also responsible for assisting the MLRO in developing, implementing, maintaining, and enhancing the policies, procedures, and controls applied to the prevention of financial crime.

The responsibilities and day-to-day obligations of the Compliance Monitoring Team are:

- Monitoring of AML and CTF controls to verify the performance and adequacy.
- Investigate real-time transaction monitoring flags and alerts.
- Submission of suspicion reports to the MLRO for review.
- Assess any flags of alerts pertaining to Know Your Business (KYB) information.
- Communication with customers regarding updated KYB checks as required.
- Communication with customers regarding EDD checks as required.
- Classify customers into the appropriate risk category in line with the documented risk category classification approach.

4.4 All Employees

Employees of Bigness Coin as a legal entity can be prosecuted and fined for non-compliance and violations of laws and regulations concerning prevention of money laundering and terrorist financing.

All employees have a role to play in achieving effective ongoing AML and CTF procedures and all employees are required to comply with Bigness Coin's policies and procedures. Non-compliance by employees may be considered as gross misconduct and could result in a disciplinary offence which could lead to dismissal. More seriously, the employee may even be subjected to criminal proceedings.

Therefore, employees are obliged to be aware of, and regularly improve, their professional knowledge concerning prevention of financial crime, money laundering and terrorist financing. In performing their functions, they are obliged to observe the requirements and internal regulations of Bigness Coin.

To ensure staff are appropriately prepared, Senior Management shall ensure the availability of necessary and adequate resources for all employees.

4.4.1 Employee Training

Bigness Coin understands the importance of ensuring that the appropriate training is delivered to all relevant employees. Where employees have not been trained, or where employees have been inadequately trained, Bigness Coin may be open to penalties and/or criminal charges.

Therefore, the MLRO arranges regular training of all employees concerning prevention of financial crime, money laundering and terrorist financing.

The training includes:

- Awareness and understanding of applicable laws, regulations, legislation, and employee obligations.
- This policy and other internal regulations regarding employee responsibilities and their effect on the business.
- How to recognise and deal with potential money laundering or terrorist financing activity.
- How to report suspicious activity.
- Details of the MLRO's identity and responsibilities.

The content of the training is updated as changes in regulation occur, and Bigness Coin provides full training to staff every twelve months. Additional training may be provided where an increased risk has been identified or where a significant change has taken place in the business.

During training, employees are informed about theoretical examples and practical recommendations regarding the identification of suspicious activity, as well as encouraged to promote a mutual exchange of experience. Additional training or refresher courses will be arranged if there is a need identified within any specific employee or department.

It is the MLRO's responsibility to arrange and maintain staff training. However, training may be carried out in person or virtually as appropriate and be performed by the MLRO or by a suitably qualified employee or external service provider.

A record is maintained of all staff training conducted, including the following information:

- A copy of training materials.
- Details of training provider (if provided externally).
- List of staff who have completed training, with dates, their signatures confirming the training took place, or any electronic training records.
- A retraining schedule.

5. Risk Methodology

Bigness Coin uses a risk-based approach when considering the controls applied to AML and CTF. All products and services are broken down and assessed against a series of risk-based categories.

5.1 Risk Categories

The following risk categories are considered.

5.1.1 Customer Risk

The customer risk relates to the risk that is posed by Bigness Coin's existing customer base. Certain types of customers that may pose a higher risk are of significant importance. Customer risk also covers any risks posed by Bigness Coin's products attracting potentially unwanted customers.

This risk category examines the potential flaws in any customer risk assessments that needs to take place before any agreement is put in place between Bigness Coin and the customer.

5.1.2 Product Risk

The features of Bigness Coin's products and services need to be considered as what is offered determines the exposure to specific risks which need to be addressed and mitigated as much as possible.

5.1.3 Transaction Risk

There is a risk that the products and services provided by Bigness Coin can be used to perform transactions whose volume, value and/or purpose are criminal in their intent, resulting in the increase of Bigness Coin's money laundering and terrorist financing risk.

5.1.4 Geographical Risk

Geographical risk relates to the risks posed by the jurisdictions Bigness Coin operates in and any customers who originate from there. An increase in geography causes an increase in the risk of exposure to global sanctions, as well as other global aspects of money laundering.

This risk also covers jurisdictions outside of Bigness Coin's operating area, which are areas potentially attracted to Bigness Coin's products and services.

5.1.5 Business Risk

Business risk relates to anything within Bigness Coin's operating structure that may increase the risk of money laundering. This can include employees participating in unlawful activity (knowingly or unknowingly) or being unaware of their employee responsibilities.

5.1.6 Distribution Risk

This applies to the distribution methods that Bigness Coin uses to obtain and service its customer base. As this is likely provided by an expanded organisational framework, distribution presents several risks that must be addressed and mitigated.

5.2 Business Wide Risk Assessment (BWRA)

Bigness Coin conducts annual Business Wide Risk Assessments (BWRA) to identify and assess the risks of money laundering and terrorist financing within its products and services. This assessment is documented and made part of Bigness Coin's compliance policies and procedures.

The BWRA is an assessment of Bigness Coin's activities within the approved policies and procedures and will be performed by the MLRO. The BWRA also influences changes in policy and procedure where required.

If the BWRA finds that Bigness Coin does not pay adequate attention to the provisions of the risk methodology, the AML and CTF controls, and/or other internal regulations concerning prevention of financial crime, Senior Management will be immediately notified and an action plan to rectify the inadequacies put in place.

Any action plan addressing the gaps identified will be devised by the MLRO and tracked to completion.

When considering the BWRA, risk items are identified with each having its risk impact to the business determined in two ways, either Inherent or Residual.

5.2.1 Inherent Risk

Inherent risk focuses on the natural risk that is present before any sort of control is implemented. An impact rating of High, Medium, or Low is achieved by considering the likelihood of any specific risk occurring and the severity of that risk if it were to occur. The combination of the ratings indicates an overall impact of the inherent risk and Bigness Coin then applies appropriate controls based on the determined impact.

For High Likelihood events, the impact will be calculated as follows:

- Likelihood High and Severity High, the item will be High Impact.
- Likelihood High and Severity Medium, the item will be High Impact.
- Likelihood High and Severity Low, the item will be Medium Impact.

For Medium Likelihood events, the impact will be calculated as follows:

- Likelihood Medium and Severity High, the item will be High Impact.
- Likelihood Medium and Severity Medium, the item will be Medium Impact.
- Likelihood Medium and Severity Low, the item will be Medium Impact.

For Low Likelihood events, the impact will be calculated as follows:

- Likelihood Low and Severity High, the item will be Medium Impact.
- Likelihood Low and Severity Medium, the item will be Low Impact.
- Likelihood Low and Severity Low, the item will be Low Impact.
- A risk matrix can also be used to visualise the impact scoring methodology:

	Severity		
Likelihood	Low	Medium	High
Low	Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	High

5.2.2 Residual Risk

An effective control will reduce the inherent risk impact and create a lower risk impact. The residual risk is the risk that is left after all controls have been put in place. Where an effective control has been implemented to directly address the inherent risk, then the residual risk impact is considered a level lower than the inherent risk.

For example, High Impact risks are dropped to Medium, and Medium dropped to Low. Low Impact risks, although they have a control applied, remain Low Impact as a minimum standard and are not to be considered impossible.

Any implemented control should directly address the inherent risk and be signed off by Senior Management.

5.3 Schedule

As a minimum, Bigness Coin will conduct a BWRA once a year. However, it may be necessary to conduct a BWRA because of a trigger event.

Trigger events can include, but are not limited to:

- When new products and services are introduced.
- When existing products and services change.
- When new customer demographics and geographies are considered.
- During changes in business structure.
- During regulatory changes.
- When a failing is identified in the way Bigness Coin manage/control risks.

A BWRA could be triggered by anything that may affect Bigness Coin's risk exposure.

The MLRO will co-ordinate the assessment and will summarise the results in the annual review where the findings will also be presented to Senior Management.

Priority will be given to areas where the risk is considered high, and controls will be tracked by the MLRO to ensure they are implemented.

6. Customer Due Diligence (CDD)

CDD is a legal requirement that involves the identification and verification of information about your customer. In accordance with financial regulations, Bigness Coin performs due diligence on all customers without exception.

Ongoing monitoring of all customer relationships will also be carried out as part of Bigness Coin money's CDD procedures. Bigness Coin will also apply EDD on customers where a higher risk of financial crime, money laundering or terrorist financing has been identified.

6.1 Know Your Business (KYB)

Bigness Coin does not allow anonymous accounts, nor permit anonymous transfers of funds. Therefore, when starting contractual relationships with any new customers, Bigness Coin employs a strict KYB procedure to identify and verify those it will potentially do business with.

Bigness Coin applies KYB CDD processes during the following scenarios:

- Before establishing a customer business relationship.
- During periodic reviews of customer data.
- During trigger events, related to the suspicion of financial crime being committed by a customer.

When establishing or maintaining any business relationship with a customer, Bigness Coin works to an approach based on the perceived risk level of any given customer. Bigness Coin applies internal classifications which determine level of risk for the onboarding of customers. These risk levels are Low, Medium, or High.

Bigness Coin views the inherent risk of its customer as Medium but by performing CDD and confirming their identity through KYB procedures it considerably lowers that risk. If the customer fails to pass the KYB procedures, is provisionally identified as a PEP, or is later a subject of a SAR, then the risk of that customer becomes High.

Only by going through the EDD procedures can that risk potentially be lowered.

All High risk relationships will be formally reviewed for acceptance and approved by the MLRO, except in case of confirmed PEPs where the business will not be accepted.

For clarity, any customer confirmed to be present on an international sanctions list will also not be accepted.

In line with EU regulations and AMLD5, Bigness Coin implements KYB procedures to ensure comprehensive understanding and verification of our business clients.

These procedures include:

- Business Entity Verification. All business clients must provide official registration documents, such as incorporation certificates and Articles of Association. This is crucial to establish the legal standing and ownership structure of the business.

- Verification of UBOs (Ultimate Beneficial Owners). Identification and verification of individuals who ultimately own or control the business entity are required. This includes verifying their identity and their shareholding or control percentage.

- Business Risk Profiling. Businesses are profiled based on industry, geographic location, and nature of business activities. High-risk industries or jurisdictions may require enhanced due diligence measures.

Monitoring and Review. Ongoing monitoring of business activities, including transaction analysis and regular review of business profiles, is conducted to ensure continued compliance with AML and CTF regulations.

6.1.1 Customer Identification Process

Verification and continuous assessment of customer information is an essential method of AML and CTF. All customers of Bigness Coin are identified and verified before any agreement is put in place. This allows Bigness Coin to understand the underlying level of risk and assign the appropriate risk category before engaging in any business activity.

Customer identification shall be carried out based on digital copies of government issued identity documents verified against third-party sources such as national registers, credit institutions, and government databases.

Bigness Coin uses third-party KYB software to verify the information and documentation provided by customers. Should the third-party KYB software be unavailable, there is a manual onboarding process.

Customers can contact Bigness Coin customer support if they encounter issues navigating the onboarding process, but all customers will be verified by third-party KYB software before being approved to use Bigness Coin products and services.

Bigness Coin applies the following Know Your Business (KYB) procedures to ensure the corporate customer meets the required regulatory and CDD standards.

The following details shall be reviewed:

- Corporate customer's incorporation details.
- Details of all directors and persons responsible for running the business (to ensure that they are fit and proper).
- Details of the services provided by the corporate customer.
- Details of the corporate customer's internal risk controls (if relevant to the services provided).

KYB CDD processes are applied during the following scenarios:

- Before establishing a corporate business relationship.
- During periodic reviews of corporate customer data.
- During trigger events, related to the suspicion of financial crime being committed by a corporate customer.

6.1.2 Incorporation Review

In order to confirm the full details of the corporate customer the following information needs to be obtained:

- Legal Name.
- Trading Name (if any).
- Registered Address.
- Trading Address.
- Website Details.
- Legal Status.
- National business registry number.

Legal details need to be verified with the national business registry, where the necessary incorporation documentation can be obtained.

6.1.3 Directors, UBOs, and/or Persons Responsible

Checks also need to be made with regards to director(s), ultimate beneficial owners (UBO), and/or persons responsible for the management of the corporate customer's business activities. Bigness Coin requires UBOs with a holding percentage of 20% or more to be reviewed.

Bigness Coin requires the following UBOs to undergo high risk review:

- Firms with more than 5 UBOs, each UBO must be verified regardless of holding percentage
- Firms with overseas ownership (outside of the EU).

Bigness Coin uses the same third-party software to verify the information and documentation provided by director(s), UBOs, and/or persons responsible.

The information required for verification is:

- Government issued photo identity document (e.g., Passport) containing:
  - Full name.
  - Date of birth.
  - Photo.
- Confirmation of their ownership or control within the corporate customer's business activities.
- Residential address confirmation.
- Where the firm operates out of a physical location this address must be confirmed.

Bigness Coin also require evidence that they are fit and proper persons. Checks need to be made regarding the

following:

- Honesty, integrity, and reputation, including ensuring that they have not been convicted of any criminal offence.
- Competence and capability, including ensuring they have the sufficient knowledge and awareness of the regulatory environment to carry out their duties.
- PEP, adverse media, and sanction checks.

6.1.4 Services Provided

Bigness Coin will investigate the corporate customer's commercial presence to understand the following:

- The precise products or services that are being offered.
- The geographical location of customers and operations.
- The source of funds.

This information will be analysed for any impact to regulatory requirements, and to ensure it fits within Bigness Coin's risk appetite.

6.1.5 Adverse Media Screening

Adverse Media Screening, also known as media monitoring or negative news screening, is undertaken as part of the KYB process. It is the process in which a customer, or prospective customer, is screened against negative information and publicly available data sources. This allows Bigness Coin to identify and prevent potential risk events before they arise.

This includes searches against social media and online news providers for all customers during the normal KYB process. All customers are screened for adverse media at point of application, but where a customer is flagged as Medium risk, this search will be done weekly to monitor for any changes in the customer's public information. Where possible adverse media screening includes checking customer reviews for relevant findings.

6.1.6 Politically Exposed Person (PEP)

Due to their position and influence, it is realised that many PEPs are in situations that can potentially be abused for the purpose of laundering illicit funds or other offences such as corruption or bribery. However, these recommendations should not be interpreted as all PEPs are involved in criminal activity.

PEPs are outside the risk appetite of Bigness Coin. However, for sake of clarity and in order to ensure PEPs are not onboarded, the definition of a PEP is outlined below.

PEPs are defined as individuals entrusted with prominent public functions, including:

- Members of the administrative, management or supervisory bodies of state-owned enterprises, government corporations, government business enterprises, government-linked companies, or public enterprises.
- Members of courts of auditors or of the boards of central banks.
- Members of supreme courts, of constitutional courts or of other high level judicial bodies.
- Members of European Parliament or national parliaments within the EU.
- Members of the governing bodies of political parties.
- Heads of State, heads of government, ministers and deputy or assistant ministers.
- High ranking military officials.

In some instances, a family member of a PEP may also be identified, which includes:

- The spouse or civil partner of a PEP.
- Children of a PEP and/or the spouses or civil partners of a PEP's children.
- Parents of a PEP.

PEP classification remains for a period of twelve months after the person ceases to hold the public function or longer if the PEP continues to pose a risk of money laundering and terrorist financing.

In accordance with regulatory obligations, all customers are reviewed using third-party KYB software to identify the presence of PEPs. Where information identified via KYB software suggests that a potential or existing customer could be a PEP, this should immediately be reported to the MLRO for investigation and confirmation.

In confirmed cases the potential customer will be notified of a failure to complete the application. For confirmed cases relating to existing customers, the customer will be notified, and the termination process enacted.

6.1.7 Sanctions

National governments or International Bodies such as the European Union, United Nations, or the relevant national authorities within the EU, the Office of Foreign Assets and Control (OFAC, US Treasury) and more, impose International Financial Sanctions. Engaging in business activities with sanctioned individuals and entities are prohibited and Bigness Coin has an obligation to freeze the assets of any confirmed sanction match and report any transactions to the authorities.

For clarity, Bigness Coin will not set up accounts for customers listed on any financial sanctions lists or carry out any transactions or business activity with them. This is because it is a criminal offence to make funds or financial services available to individuals or entities on sanctions lists.

Bigness Coin is required to screen its customers and employees, filter its transactions, and prevent activity with sanction targets immediately once identified. Bigness Coin does not whitelist any individuals, including their own employees. All customers and employees will undergo initial and ongoing sanction checks.

To minimize the customer risk, Bigness Coin applies screening checks before establishing any business relationship, and daily thereafter regarding whether the members of its customer base are included in relevant watch or sanction lists accessed by the third-party KYB software.

In the event of a sanctions flag for new customers, the account opening process will be put on hold pending further investigation. In case of a flag, the case will be referred to the MLRO to decide on the next course of action.

To determine if the flag is a false positive, the MLRO must do a review to confirm whether the customer is confirmed to be on a sanctions list. After completing the review, the MLRO will decide on whether to establish a relationship with the customer if the outcome of the investigation identifies the flag as false.

For a new flag on an existing customer, then the customer's account will be put on hold pending further review. The case will be escalated to the MLRO for immediate review. If the flag is found to be a false positive, then the account's hold will be released, and the customer contacted regarding service disruption.

Should it be confirmed positive, the case will be presented to the authorities, and Senior Management.

Where a potential associate is confirmed to be on a sanctions list the onboarding processes is stopped immediately. Bigness Coin will report the event to the authorities, and Senior Management immediately.

All confirmed sanction flags will be reported to:

Financial Analytical Office

Washingtonova 1621/11 Praha 1,

110 00 Prague 1,

Czech Republic

T: +420 257 044 501

E: legislativa@fau.mfcr.cz

6.2 Know Your Customer (KYC)

Bigness Coin implements comprehensive KYC procedures to comply with EU regulations and ensure the integrity of its customer base. The KYC process involves the following steps:

Customer Identification and Verification:

- **Required Information**:
- Full legal name
- Date of birth
- Nationality
- Permanent residential address
- Contact details (email and phone number)
- **Documentation**:

- A valid, government-issued photo ID (passport, national ID card, or driver's license)
- Proof of address (utility bill, bank statement, or official government correspondence not older than three months)
- Where applicable, additional documentation to confirm source of funds or wealth (e.g., salary slips, inheritance documentation, sale of assets)

Enhanced Due Diligence (EDD):

- Applied in situations where the customer poses a higher risk, such as non-residents, PEPs, or individuals from high-risk countries.
- Additional documentation may be required, such as financial statements, business documentation, or evidence of wealth.

Continuous Monitoring and Updates:

- Regular updates to customer information, particularly when there are changes in personal circumstances or significant financial activities.
- Use of third-party verification systems to continuously monitor for changes in status or new risk indicators.

Adverse Media and PEP Screening:

- Daily screening of customer information against adverse media and international sanctions lists.
- Immediate action, including the potential termination of the business relationship, if a customer is identified as a PEP or involved in suspicious activities.

6.3 Customer Risk Levels

Upon completed of the CDD process, customers will be categorised as either Low, Medium, or High.

Bigness Coin classifies a customer as Low risk where the customer has passed all CDD requirements and has been successfully onboarded without issue.

This would include:

- Successful photo ID, and address verification for UBOs.
- Provided jursidiction based documentation.
- Has not raised any PEP, sanction, or adverse media flags.
- Relationship to the business has been established.

Low risk customers are considered Bigness Coin's ideal customer base and fall under automated monitoring procedures which utilise the least amount of Bigness Coin's resources and attention.

Medium risk customers would include:

- A Director/UBO was provisionally flagged for PEP, sanction, or adverse media, but had since been identified as a false flag.
- The customer's activity is inconsistent with other customers but not considered suspicious.
- The customer's activity is inconsistent with expected activity as per the customer's declared turnover, but within an allowed variance.
- The customer has been included in previous investigations but not found to be sufficient enough to indicate suspicious activity.

Medium risk customers are manually monitored alongside automated monitoring. Manual monitoring will continue as long as the MLRO perceives there to be a higher risk than normal posed by the customer. If the customer activity is considered to be in line with expectations, then the risk rating can be lowered upon MLRO approval.

High risk customers are those with a significant failing when passed through the CDD procedures or those who are found to be participating in suspicious activity.

High risk customers are those who:

- Have been provisionally flagged for PEP, sanction, or adverse media, but an investigation has not been able to confirm the flag(s) as false.
- Provided KYB details that do not meet Bigness Coin's requirements or standards.
- Participates in activity unacceptable to Bigness Coin and is considered suspicious.
- Are currently part of an ongoing investigation relating to suspicious activity.
- Are considered a risk to Bigness Coin as determined by the MLRO for any justifiable reason in relation to the prevention of financial crime, money laundering and terrorist financing.
- Customers with UBOs who reside outside of the EU.
- Customers with more than 5 UBOs.
- Customers with a trading history of one year or less.

Bigness Coin does not provide products and services to customers deemed High risk. Potential customers identified as High risk are to undergo additional due diligence and investigation. If the risk level cannot be mitigated, then the customer will be notified of their failure to pass the onboarding process.

Any existing customer flagged as High risk will have their services halted until an investigation can confirm the accuracy of the flag and mitigate the risk. Where the risk can be lowered, the customer is categorised as Medium. Where the risk cannot be lowered, Bigness Coin will enact the termination procedure.

6.4 Enhanced Due Diligence (EDD)

Bigness Coin's CDD and KYB procedures are in place to protect Bigness Coin from its products and services being used for the facilitation of financial crime, money laundering and terrorist financing.

Bigness Coin applies EDD to all customers and calculates their suitability against key onboarding risk identifiers such as:

- A review of existing banking activity to determine the frequency/schedule of incoming and outgoing funds.
- A demographic review based on Geographical Risk to determine if funds are coming in from territories that fall outside Bigness Coin's regulated areas.
- Confirmation if the primary source of funds is from a high risk or unsustainable source

Regarding the expected use of products, Bigness Coin will consider:

- The value of the financial activity that the customer expects to make.
- The expected frequency of the payments made by the customer.

Bigness Coin also uses EDD as part of its investigation procedures to mitigate the risks of financial crime, money laundering and terrorist financing.

The EDD process will consider further information when adjusting the risk level of a customer, and in each case following requirements will be met:

- Additional documents validated via third-party software.
- Further definition regarding the nature and purpose of the account/services requested.
- Additional information obtained to establish the source of wealth funding the account.
- Manual monitoring to be established based on the outcome of the EDD investigation.
- Obtaining approval from Senior Management before establishing or continuing the business relationship.

6.4.1. Source of Funds

During EDD, it may be necessary for Bigness Coin to establish a customer's source of wealth used to fund their account. This is primarily used to establish that Bigness Coin is not being used as a layering mechanism for money laundering or other forms of financial crime.

Bigness Coin considers the following sources of wealth acceptable:

- Sale of investments/liquidation of the investment portfolio detailing:
  - Description of shares/units/deposits.
  - Name of seller.
  - Time period held.
  - Total sale/liquidation amount.
  - Date funds received.
  - Investment/savings certificates, contract notes, surrender statements or equivalent clearly showing date and amount of surrender/liquidation/maturity.
  - Bank statement clearly showing receipt of funds and name of investment company.
  - Letter detailing receipt of funds from a regulated accountant on letterheaded paper and accompanied by updated proof of accountant's regulated status.
- Sale of property detailing:
  - Sold property address.
  - Date of sale.
  - Total sale amount.
  - Letter from a licensed solicitor or regulated accountant, stating property address, date of sale, proceeds received, and name of purchaser.
  - Copy of sale contract as well as proof of receipt of funds (e.g. bank statement) clearly showing receipt of funds and name of purchaser.
- Company sale detailing:
  - Name and nature of the company.

- Date of sale.
- Total amount.
- Client's share.
- Copies of media coverage (if applicable).
- Letter detailing company sale signed by a licensed solicitor or regulated accountant on letter-headed paper and accompanied by updated proof of accountant's or solicitor's regulated status.
- Copy of contract of sale, plus bank statement showing proceeds received.
- Inheritance detailing:
- Name of deceased.
- Date of death.
- Relationship to client.
- Date received.
- Total amount.
- Solicitor's details.
- Evidence that the customer is the inheritor.
- Grant of Probate (with a copy of the Will) clearly showing the amount of inheritance.
- Signed letter from a licensed solicitor or estate trustees on letter-headed paper clearly indicating the amount of inheritance, accompanied by updated proof of solicitor's regulated status.
- The Will (if absolute amount is not clearly shown, other documentary evidence shall be required to support this).

- Divorce settlement detailing:
  - Date received.
  - Total amount received.
  - Name of divorced partner.
  - Copy of court order clearly indicating the amount of settlement.
  - Letter detailing divorce settlement as well as clearly indicating the amount of settlement and signed by a licensed solicitor on letter-headed paper accompanied by updated proof of solicitor's regulated status.
- Company profits detailing:
  - Name and address of company.
  - Nature of company.
  - Amount of annual profit.
  - Copy of latest audited company accounts.
  - Documentary evidence of the nature of business activity and turnover, e.g. a letter from a regulated accountant accompanied by updated proof of accountant's regulated status.

6.5 Periodic and Event Driven Reviews

In order to make sure the due diligence information held regarding customer verification is up to date, Bigness Coin reviews and updates KYB information every three years unless flagged as a Medium or High risk customer, where it will be done more frequently as part of more stringent ongoing monitoring requirements.

SARs raised against a customer may also trigger an update request for KYB information, as will events that change the details stored against the account such as name and address.

Periodic KYB renewals, will be done on the following schedule using third-party KYB software:

- Low Risk Customers are reviewed every three years.
- Medium Risk are reviewed annually.
- High Risk Customers are reviewed when discovered and if their risk category cannot be lowered through EDD then the relationship will be terminated.

The MLRO shall be involved in the process of periodic and event driven reviews with customers who are categorized as High risk, or in cases where an increased risk has been identified. Renewed PEP and sanction assessments will also be applied to all customers daily.

7. Monitoring

Bigness Coin implements monitoring procedures to detect any unusual or suspicious behaviour regarding its customers' financial activities. Bigness Coin is required to perform monitoring of all transactions undertaken within its products and services and performs automated monitoring in real time and manual analysis post transaction.

There is no clear definition as to what activity can be called suspicious, but the techniques Bigness Coin applies are used to monitor financial transactions and customer behaviour in search for patterns attempting to conceal the true intent of the funds.

These patterns can include various risk categories such as unusual activity patterns, significant volumes, high amounts, risky jurisdictions, and activity aimed at avoiding suspicion.

Bigness Coin applies a number of monitoring techniques such as:

- Automated monitoring, which are alerts raised based on specific scenarios designed to identify suspicious transactions. The responsibility of addressing the alerts lies with the Compliance Monitoring Team. These alerts are addressed immediately.
- Manual analysis, which is undertaken every working day against the previous day's (or multiple days in the event of a weekend or holiday) transaction activity. Customer behaviour is reviewed to identify new patterns or activity that may be suspicious or indicate updates required to the alert scenarios applied to automated monitoring. Any customers flagged as Medium risk or higher are to undergo individual manual analysis and review until their risk category can be lowered.
- Additional review or monitoring may be undertaken in the event of a trigger event or if any employee comes across an event that might raise suspicion.

If during any of the above processes an employee identifies a suspicious transaction, then the SAR procedure will be followed.

7.1 Suspicious Activity

The definition of suspicious activity as well as the types of suspicious transactions which may be used for financial crime, money laundering and terrorist financing are almost unlimited. However, Bigness Coin maintains adequate information and knows enough about its customers' expected activities to recognise that a transaction or a series of transactions is unusual or suspicious.

A suspicious transaction will often be one which is inconsistent with a customer's known or expected behaviour, or the expected behaviour of Bigness Coin customers as a whole.

Examples of what might constitute suspicious activity are listed below. The relevant list is not exhaustive, nor does it include all types of activity that may be considered, nevertheless it sets a base level framework Bigness Coin and its employees can use in recognising the main instances of suspicious activity.

The detection of any of the transactions contained in the below list prompts further investigation and clarification on the circumstances surrounding the particular transaction.

Examples of suspicious activity are:

- Transactions with no discernible purpose or appear unnecessarily complex.
- Transactions which are inconsistent with Bigness Coin customers' known activities.
- Transactions whose nature, size or frequency appear to be unusual with regards to customer expectations.
- Transactions are flagged for investigation and a customer is reluctant/unable to provide supporting information/documents requested by Bigness Coin within relation to the investigation of the flagged transaction.
- A customer requests to close their account following the request of supporting information/documents by Bigness Coin.

- Transactions are flagged for investigation and a customer provides falsified information/documents within relation to the investigation of the flagged transaction.

7.2 Transaction Monitoring System

In order to distinguish suspicious activity from legitimate activity, customer transactions are monitored by the Compliance Monitoring Team maintain fraud prevention via a fully automated, real-time monitoring.

Bigness Coin has implemented a set of various flags and triggers to identify unusual transaction behaviour. These rules and the logic behind these flags are regularly reviewed in order to ensure that they continue to identify all possible suspicious or unusual transactions that could take place.

Real-time transaction monitoring is applied in one of two processes:

- Prevention, where real time blocks are applied to suspicious transactions before they are processed.
- Detection, where real time flags after the event where transactions are considered unusual but do not meet a requirement to be prevented from occurring.

Bigness Coin's transaction monitoring system is also capable of quarantining any attempted transaction that appears suspicious in nature. Following the quarantining of any suspicious transaction, an investigation will take place.

Transaction monitoring is conducted on a risk-based approach. Depending on the risk posed by the specific transaction, the intensity of the checks as well as the measures taken for mitigating the risks may vary from:

- Requesting additional documentation/information to ascertain the nature of the transaction.
- To a possible block of the account or termination of the customer relationship.

Bigness Coin applies increased transaction monitoring for customers that are flagged as Medium risk. All transactions of such customers are manually reviewed by the Compliance Monitoring Team (and by MLRO if necessary). Customers flagged as High risk are unable to transact until their risk rating can be lowered.

The MLRO also has access to the results of transaction monitoring. Results are regularly reviewed by the MLRO who in turn provides Management Information reports to Senior Management as required.

Senior Management will consider the appropriateness and effectiveness of Bigness Coin's monitoring processes as part of its ongoing review of Bigness Coin's business risk assessments and associated policies, procedures, and controls.

Where Bigness Coin identifies weaknesses within its monitoring, it is ensured that the weaknesses are rectified in a timely manner.

7.3 Investigation

Transaction flags are investigated for legitimacy, and, in turn, it is decided if a SAR is required.

Since transaction monitoring is conducted on a risk-based approach, the MLRO and/or the Compliance Monitoring Team may request additional information depending on the nature of the transaction itself and overall transaction history of the customer.

The Compliance Monitoring Team can request the following supporting information/documents:

- Details of the nature of the transaction if it is not self-evident.
- Information and documents proving the customer's source of wealth and ownership over the method used to fund the Bigness Coin account.
- Renewed KYB documents to reverify the customer's identity.
- Documents supporting the transaction with the merchant, including documents certifying the actual provision of goods or services (contracts, invoices, quotations etc.).

All communications, reviews, decisions regarding flagged transactions and SARs are documented and monitored by the MLRO.

7.4 Dormant Account Procedure

Dormant accounts are accounts that:

- Are initially inactive accounts where an account has been created but an initial transaction has not been made in 3 months.
- Are semi active accounts which have transacted but have been identified by Bigness Coin as being continuously inactive for a period of three months.
- Are low activity accounts whose transaction volume and value falls significantly under expected amounts in a three-month period.

Dormant accounts are suspended and investigated by the MLRO, depending on the customer's response Bigness Coin will:

- If satisfied with the customer's response Bigness Coin will reactivate the account.
- Where unsatisfied Bigness Coin will increase the customer's risk rating to Medium and require the customer to undergo EDD before the account is reactivated.
- Where there is no response, or where the customer refuses to undergo EDD, then the customer is offboarded.

Bigness Coin carries out periodic reviews of all accounts to detect inactivity and are subsequently made dormant. The dormant account may be reactivated or closed via a written request from the customer, in such cases the customer must provide the following documentation and information for verification:

- Address.
- Contact details.
- Source of funds bank account details.
- Copies of any registration documentation given during CDD.

Customers who refuse to cooperate or who provide inadequate or false information are investigated by the MLRO or Nominated Officer, a SAR is raised depending on the outcome of the investigation. Where the customer requests the account to be closed then Bigness Coin offboards the customer. A customer that closes their account must pass Bigness Coin's CDD checks again before the account can be reopened.

Upon successful completion of CDD, the customer's account is reactivated.

All accounts that are nominated as dormant, or dormant accounts that have been reactivated, are subject to ongoing monitoring to avoid unauthorised transactions from the account. Dormant accounts are monitored to ensure that only the original customer is using the account. The accounts are also monitored to ensure that Bigness Coin employees do not engage in criminal activities using the dormant account.

8. Identifying and Reporting Suspicious Activity

Bigness Coin is aware of the harm that might be caused to Bigness Coin's reputation if there is an attempt to use Bigness Coin's products and services for financial crime including money laundering or terrorist financing transactions. Therefore, it is an essential part of Bigness Coin's AML and CTF procedure that employees raise any suspicious activity by following the defined SAR process.

When an employee has reason to determine suspicious activity, they will immediately make a written report or email to the MLRO. If the employee feels it is urgent, they will contact the MLRO first and follow up with a written report. Any suspicion must not be discussed with anyone other than the MLRO.

8.1 Suspicion

Suspicion is made beyond general speculation and must be based on available information. Although suspicion requires no firm evidence, it must be built upon a foundation of fact. Suspicion is therefore personal and subjective but still must be viewed as serious by the MLRO.

If an employee considers activity to be suspicious, they are not expected to know or to establish the exact nature of any underlying criminal offence, or that the activity is arising from a crime, money laundering or terrorist financing.

Suspicion may be something that occurs based on the following examples:

- Any customer or employee activity or instruction that is not logical from an economic, financial, or practical point of view.
- Any financial activity where the amount, duration or other specific feature is inconsistent with the subject's personal, professional, business or expected activity.

An activity or event may not appear to be suspicious at the time, but if suspicions are raised later, an obligation to report then arises.

8.2 Reporting Process

Businesses operating in financially regulated sectors, and their employees, are required by law to disclose information to the authorities in circumstances where they know or suspect, or have reasonable grounds for knowing or suspecting, that another person is engaged in financial crime, money laundering or terrorist financing.

As a financial service provider, Bigness Coin is obliged to have procedures in place to detect, report and disclose activities or financial transactions which do not fit with the normal course of business. Disclosures are made by submitting a SAR.

The MLRO will receive any reports or concerns relating to any suspected or actual financial crime and will record, investigate, and report this to the relevant authorities where necessary. The MLRO is responsible for all communications with the the relevant national competent authorities and any law enforcement agencies concerning the reporting of suspicious activity.

All SARs are stored securely and is strictly confidential, accessible only by the MLRO and a designated other of the MLRO's choosing. All notifications made will be handled with strict confidentiality.

All customer activity is subject to ongoing monitoring, therefore:

- When suspicious activity is identified, the employee immediately notifies the MLRO in writing and in person where possible.
- The MLRO immediately reviews the details of the suspicious activity and seeks further information where necessary to determine whether financial crime is suspected.
- The relevant customer's account is internally flagged, and where necessary blocked, whilst the compliance investigation is underway.
- Any employee who is contacted by the relevant customer must not speak to them and pass them on to the MLRO immediately.
- When a suspicion is confirmed the MLRO alerts the Europol as soon as possible.

- The MLRO investigates what additional information can be provided regarding the customer or transaction in question.
- If financial crime is not suspected, the reasons will be documented, identifying why no further action needs to be taken and, if appropriate, the customer's account will be unblocked.
- If financial crime is suspected, the customer relationship will be terminated.
- The MLRO incorporates any lessons learnt into future employee training, policies or processes as required.

9. Terminating Customer Relationships

In circumstances where a customer is deemed to be outside Bigness Coin's risk appetite, it may be necessary to terminate the business relationship. Given the sensitive nature of such an event, it is essential that an effective termination strategy is put in place.

The termination strategy will ensure that relationships with customers who are deemed not acceptable are terminated lawfully while also managing business risk, as well as avoiding potential reputational and legal impacts.

During customer termination, all funds are to be removed from the customer's Bigness Coin ewallet and returned to the original source. Once the customer's account has been reduced to zero balance and all products and services have been restricted, then the account is considered closed.

A customer may request to have their account terminated with no resistance from Bigness Coin. However, there are defined circumstances where it will be necessary to escalate issues to Senior Management regarding termination of customer relationship(s):

- A new/existing customer has been identified as being on a sanctions list.
- A new/existing customer has been identified as being a PEP.
- New legislation has been identified that may impact on Bigness Coin's risk appetite.
- An event has occurred in which an existing customer has been found to be linked to financial crime, money laundering or terrorist financing.

Bigness Coin will also choose to terminate customers if there has been a breach in customer terms and conditions such as:

- The use of Bigness Coin's products and services in connection with industries that are prohibited.
- The use of Bigness Coin's products and services for illegal purposes.
- Where Bigness Coin's products and services have been used by anyone other than the onboarded customer.

When terminating a relationship with a customer regarding the above events, the following procedure needs to be followed:

- The MLRO will escalate the matter to Senior Management for them to decide on whether a relationship needs to be terminated.
- The reason for terminating the relationship will be fully documented.
- If not in breach of any legal requirements, a notice period will be agreed to ensure that all pending financial services are completed and settled.
- The termination notification that is communicated to the customer provides a clear period of time for the customer to find an alternative financial services provider.
- At the end of which the notice period, the account will be closed, and funds returned to the last known funding source of the customer (unless prohibited by law from doing so).
- Bigness Coin will ensure removal of the customer details from any relevant database where it does not impact the need to retain information for AML and CTF purposes.
- Legal and regulatory issues encountered with the customer's termination are addressed systemically and, to avoid repetition of these problems with other customers, recorded and applied to the termination strategy or any other policy and/or procedure.

Should there be a conflict between the MLRO and Senior Management regarding the termination of a customer, the MLRO's judgment should take precedence when terminating a customer due to regulatory concerns or breach in compliance controls.

Details of any individuals who have been offboarded for breaching terms and conditions will be stored so as to identify them should they try and create a new account.

10. Onboarding form

Customer and Business Onboarding Form

To streamline the KYC and KYB processes, Bigness Coin has developed comprehensive onboarding forms, tailored to capture necessary information from both individual customers and business clients. The onboarding forms include but are not limited to the following fields:

1. **Personal Information:**
    - Full legal name, date of birth, nationality, and residential address.
    - Contact details including phone number and email address.
    - Identification number (passport, national ID, etc.).
2. **Business Information (for business clients):**
    - Legal name of the business, registration number, and date of incorporation.
    - Address of the registered office and principal place of business.
    - Details of the industry and nature of the business activities.
3. **UBO Information:**
    - Identification and verification details of UBOs, including their percentage of ownership and control within the business entity.
4. **Risk Assessment Details:**
    - Country of residence/business operation, anticipated transaction volumes, and types of services required.
5. **Consent and Acknowledgment:**
    - Confirmation that the information provided is accurate and complete.
    - Agreement to the terms and conditions, including consent for data processing and compliance with AML/CTF policies.