Banqua Sp z.o.o

Anti-Money Laundering (AML)

Disclaimer:

This AML policy document is prepared for the " Banqua Sp z.o.o" considering broader AML compliance requirements, and the information provided. The responsibility to ensure policy confidentiality, periodic review, update, and approval of this document rests with the Board/Management of the company. This AML policy should not be considered as the AML procedure document and should not be used for any other company or business, whether in EU or any other jurisdiction. The AML policy should not be taken as an opinion on any AML/CFT or KYC-related specific issue/ matter that requires the involvement and opinion of a subject matter expert. MLRO under the supervision of the Board and Senior Management shall ensure that all applicable AML Regulations and requirements are identified and complied with in letter and spirit. AML/CFT or KYC-related issues/ matters faced by the company shall be looked after by the management and the MLRO of the company and if required the AML subject matter expert shall be contacted by the company, for opinion and advisory.

Contents-

1 Objective

Banqua Sp z.o.o, (referred to as “Company”) being registered in the register of Virtual Currencies as a cryptocurrency business is involved in wallet, custody, money transfer service, trading and investing in cryptocurrencies. The company does not deal in fiat currencies.

The company intends to do the crypto business in EU in a transparent manner and in compliance with applicable anti-money laundering (AML) Act, laws, regulations, and related requirements including EU AML Directive, to combat the money laundering or financing of terrorism.

Virtual currencies provide a powerful new tool for criminals, terrorist financiers and other sanctions evaders to move and store illicit funds, out of the reach of law enforcement and other authorities. Virtual currency systems traded on the Internet, are generally characterized by non-face-to-face customer relationships and may permit anonymous funding (cash funding or third-party funding through virtual exchangers that do not properly identify the funding source). They may also permit anonymous transfers, if the sender and recipient are not adequately identified, therefore, to avoid these risks the Board and Management of the Banqua Sp z.o.o, is committed to ensuring that appropriate and required anti-money laundering (AML) measures, systems and controls are developed and implemented, at all levels in the company.

Companies doing the cryptocurrency business activities are subject to obligations under the AML Act if they provide the following services:

- exchange services between virtual currencies and FIATs (bureaux de change, exchanges);
- exchange services between virtual currencies (bureaux de change, exchanges);
- brokering services between virtual currencies and FIATs or between virtual currencies (as above);
- account maintenance services for virtual currencies (i.e. wallets).

The company aims to establish the governing principles and implement processes and controls, to protect the company and its systems from being used by the criminals or money launderers. AML policy provides broader guidelines, to ensure that the Board of Directors, Senior Management, and employees, of the company identify, understand and comply with the applicable AML compliance requirements.

The company aims to prohibit and avoid establishing customer relationships with sanctioned Individuals, proscribed persons, money launderers, terrorists, criminals and related groups or

people. The company does not establish business relationships or provide services to the clients, customers or persons belonging to countries including Iran, North Korea, Russia, Democratic Republic of Congo and other countries that are banned by the state or regulatory authorities of the jurisdiction or appearing in the current sanction list.

2 Some Important Terms as per FATF

As per Financial Action Tash Force (FATF), **virtual currency** is a digital representation of value that can be digitally traded and functions as:

(1) a medium of exchange; and/or

(2) a unit of account; and/or

(3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from fiat currency (a.k.a. “real currency,” “real money,” or “national currency”), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency i.e., it electronically transfers value that has legal tender status.

Digital currency can mean a digital representation of either virtual currency (non-fiat) or e-money (fiat) and thus is often used interchangeably with the term “virtual currency”. In this paper to avoid confusion, only the terms “virtual currency” or “e-money” are used.

Convertible (or open) virtual currency has an equivalent value in real currency and can be exchanged back-and-forth for real currency. Examples include: Bitcoin; e-Gold (defunct); Liberty Reserve (defunct); Second Life Linden Dollars; and WebMoney.

Non-convertible (or closed) virtual currency is intended to be specific to a particular virtual domain or world, and under the rules governing its use, cannot be exchanged for fiat currency. Examples include: Project Entropia Dollars; Q Coins; and World of Warcraft Gold.

Cryptocurrency refers to a math-based, decentralized convertible virtual currency that is protected by cryptography. i.e., it incorporates principles of cryptography to implement a distributed, decentralized, secure information economy. Cryptocurrency relies on public and private keys to transfer value from one person (individual or entity) to another, and must be cryptographically signed each time it is transferred. The safety, integrity and balance of cryptocurrency ledgers is ensured by a network of mutually distrustful parties (in Bitcoin, referred to as miners) who protect the network in exchange for the opportunity to obtain a randomly distributed fee.

A **wallet provider** is an entity that provides a virtual currency wallet (i.e., a means (software application or another mechanism/medium) for holding, storing and transferring bitcoins or other virtual currency). A wallet holds the user's private keys, which allow the user to spend virtual currency allocated to the virtual currency address in the blockchain. A wallet provider facilitates participation in a virtual currency system by allowing users, exchangers, and merchants to more easily conduct virtual currency transactions.

The wallet provider maintains the customer's virtual currency balance and generally also provides storage and transaction security. For example, beyond providing bitcoin addresses, the wallet may offer encryption; multiple key (multi-key) signature protection, backup/cold storage; and mixers. All Bitcoin wallets can interoperate with each other. Wallets can be stored both online ("hot storage") or offline ("cold storage"). (Examples: Coinbase; Multibit; Bitcoin Wallet).

3 Scope and Confidentiality

This AML policy applies to all business operations and activities of the company, undertaken as part of the cryptocurrency business, including wallet, custody, money transfer service, trading and investing in cryptocurrencies through online portals, websites, marketplace or in any other acceptable form and manner.

This AML policy is a confidential document and shall not be replicated or used for any other company without consultation of relevant local AML/CFT regulatory experts or legal advisors.

4 Preparation and Approval

The preparation and implementation of AML policy is the responsibility of Board/Management/Owner of the Banqua Sp z.o.o. The policy needs to be reviewed periodically

to make necessary changes prescribed by regulators and should be approved by the Board of Directors and Management of the company.

5 Target Audience

This AML policy document is prepared for the management and employees of the Banqua Sp z.o.o who are expected to be vigilant in performing their day-to-day cryptocurrency business activities and operations. All employees of the company are required to ensure that business relationships with criminals including money launderers are not established and services are not provided to them in any manner.

6 Policy Ownership

This AML policy is owned by the Board/ Management of the Banqua Sp z.o.o. Money Laundering Reporting Officer (MLRO) of the company appointed by the Board of the company, being the subject matter expert, is required to periodically review, update (if necessary) this policy document and take approval of the Board and Senior Management of the company.

7 Money Laundering and Terrorist Financing

Money laundering is the processing of criminal proceeds to disguise its illegal origin. Money laundering process enables the criminals to enjoy profits and funds without jeopardizing their source.

When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention.

Criminal activity is usually undertaken to generate revenue or provide a benefit to those undertaking the activity. Significant criminal activity is undertaken by organized groups and laundering is the process of disguising the illegal origins and ownership of the criminal property to enable the criminals to use and enjoy it without jeopardizing themselves or attracting unwelcome attention, such as from law enforcement.

Stages of Money Laundering:

Stages of Money Laundering Money launderers engage in the following activities to launder funds:

Placement; is the first stage, where the illegal funds are placed in the financial system, either directly or indirectly.

Layering; is the second stage, where a series of accounts are used to transfer funds/assets from one account to another account. Very complex layers of transactions are created, to disguise the trail and origin of funds.

Integration; is the third stage, where the illegal funds are utilized to purchase different assets or the funds are invested in a legitimate enterprise, to convert the black money into white.

Terrorist financing is the provision or collection of funds with the intention that they should be used to carry out acts that support terrorists or terrorist organizations or to commit acts of terrorism. Terrorist financing includes the financing or aiding, abetting, and facilitating of terrorist acts, and of terrorists and terrorist organizations. It is a collection of funds, by any means, directly or indirectly, intending to be used, in full or in part, to carry out terrorist activities.

The motivation behind terrorist financing is generally ideological as opposed to profit-seeking, which is generally the motivation for most crimes associated with ML. Terrorism may be financed through illegal activity or the use of legitimately derived and owned funds.

Criminals may use the financial system or channels, to perform the terrorist financing activities, therefore, organizations are required to ensure that such activities are prohibited, through robust system of controls.

8 Compliance Program

A Compliance Program is intended to ensure compliance with AML/KYC requirements laid down in AML Act, Regulations, Directives and other applicable regulatory requirements. A Compliance Program forms the basis of customer due diligence, client identification, know-your-client requirements, reporting, and record-keeping, requirements.

The structure of the compliance department will primarily consist of the Marco Mariani and Allan Byron which are the two members of the compliance team. The headcount is dynamic at the moment, as it depends on the size and need of the company.

The Board and Management ensure that the appropriate Compliance Program which also covers the AML regulatory requirements is developed and approved. Following are a few of the key elements of a Compliance Program that relate to the AML measures and initiatives:

- appointing a dedicated Compliance Officer or Money Laundering Reporting Officer (MLRO), who is responsible for implementing the overall compliance program in the organization;
- developing and applying written and up to date compliance policies and procedures approved by Board of Directors;
- conducting a risk assessment, to assess and document the risk of a money laundering offence or a terrorist financing offence (ML/TF) occurring in the course of business;
- developing and maintaining a written, ongoing compliance training program for the employees and other authorized persons;
- instituting and documenting a plan for the ongoing compliance training program and delivering the training; and
- a plan for a periodic review of the Compliance Program to test its effectiveness.
- The firm will engage an independent compliance consultant or will utilize its internal audit department to test the effectiveness of the Compliance Program, which includes testing the KYC provider, and transaction control, to review existing parameters.

9 Role of Board of Directors / Senior Management

The primary responsibility to develop and implement the strong AML compliance culture is of the Board of Directors of the Banqua Sp z.o.o. The Board is required to set the tone from the top, so that Management is enabled to take appropriate measures and implement AML processes and controls, to comply with applicable AML regulatory requirements.

The Board of Directors and Senior Management of the Banqua Sp z.o.o are responsible to:

- Ensure that Compliance Program is developed, including allied policies;
- Ensure that Compliance program and policies are implemented at all levels in the company;
- Ensure that AML processes and controls are designed and implemented at all levels, to identify, verify and screen the customers of the company before establishing business relationship with them;
- Ensure that a dedicated Compliance Officer/ MLRO is hired, supported and provided with sufficient authority and resources, to perform AML related responsibilities;

- Ensure that company does not deal with criminals including money launderers, terrorists, tax evaders, persons involved in insider dealings, etc.
- Ensure that trading, investment, buy or sell, wallet arrangements or any other cryptocurrencies business activity is not done with any criminal, a person appearing in negative lists, banned jurisdictions, or related individuals;
- Periodically review and discuss the AML issues being presented by the MLRO to the Board and Senior Management;
- Issue appropriate instructions and guidelines to the management including MLRO, in light of applicable AML laws and regulations, to ensure that criminals including money launderers and terrorists are not entertained and ML/TF risks are managed on a timely manner;
- Ensure that appropriate disciplinary actions are initiated in case of violation of AML regulatory and policy requirements;
- Ensure arrangements of periodic AML training for the employees of the company. Training arrangement is made with the service provider "Scorechain" as an annual course for the monitoring of risky transactions and AML parameters.

10 Customer Due Diligence (CDD) and Know Your Customer (KYC)

Being in the business of cryptocurrency the Board and Management ensures that all the customers/clients/persons with whom the business relationships are developed or business activities are performed, are identified, and verified before such business activities and relationships. The company has an arrangement with the third-party KYC service providers, which performs the due diligence and KYC of the clients/customers/persons on behalf of the Banqua Sp z.o.o. ***For details of the Customer Due Diligence and Know Your Customer (KYC), please refer the Know Your Customer (KYC) policy of the company.***

11 Money Laundering Reporting Officer (MLRO) and His Role

A dedicated Money Laundering Reporting Officer **(Mr. Marco Mariani "MLRO")** of the Banqua Sp z.o.o is appointed who works with Board, Management and employees, to ensure that applicable AML/CFT regulatory requirements are complied with. MLRO heads the AML function and leads the AML team. MLRO works as the second line of defense and guides the business and operations team, about the AML/CFT and KYC requirements prescribed by a regulatory authority.

One of the key responsibilities of the MLRO is to ensure that all the clients, customers, or persons are identified, screened and verified before onboarding, providing any business services, making any investment or entering into any buy/ sell transactions. MLRO shall ensure that third-party KYC service providers confirm the application of appropriate KYC processes for each of the client, customer, person on a timely basis.

It is the core responsibility of the MLRO to regularly check and ensure that transactions and activities are not executed with criminals, blacklisted persons, banned countries/jurisdictions, or any other individual negatively declared by the regulator from time to time.

MLRO shall ensure that compliance with AML policy must be:

- reviewed, updated and should be in a form that is accessible to its intended audience; and
- approved by the Board and Senior Management of the company.

MLRO shall ensure that process of transaction monitoring and periodic reviews are implemented and performed, to ensure that management and employees comply with applicable AML laws and regulations and AML issues/ breaches are identified and mitigated on a timely manner.

High Risk Accounts / Customers / Clients:

MLRO shall ensure that all high-risk category customers that are identified before onboarding or after onboarding are identified and marked as “High-risk” in the AML system of the company. All high-risk category accounts/customers/clients shall be monitored and enhanced due diligence shall be performed. The company uses the third-party services to perform the KYC and due diligence, therefore MLRO shall ensure that the third-party service provider shares relevant information with the Banqua Sp z.o.o for all those customers/clients/persons, that are identified as high-risk.

High-risk category includes but are not limited to the persons or close family associates are identified as politically exposed persons (PEPs), and persons or their family members belonging to high-risk jurisdictions or countries, and persons with unclear source of income/funds.

Other High-Risk category accounts/ customers/ clients include:

- Housewives
- Sole-proprietors with an unclear source of income
- Foreign Non-Resident Persons
- Student Accounts

- Declared defaulters

MLRO shall ensure that before opening their accounts, approval of Board or Senior Management of the company is taken.

Accounts Not To Be Opened:

Board of the company and MLRO shall ensure that account opening team/ employees of the Banqua Sp z.o.o, do not open accounts of following:

- Persons/ customers/clients with an anonymous or fictitious name(s) or accounts;
- Customers who are nationals of, or are resident in jurisdictions having country-level embargoes/sanctions;
- Customers belonging to high-risk jurisdictions and countries;
- Persons with criminal history or background;
- Persons with the unclear source of income/ wealth or doubtful income sources;
- Proscribed persons;
- Persons dealing in illegal business activities;

Blocking of Accounts / Assets:

The MLRO and Management of the company shall ensure that assets are blocked of the customers who are found suspicious or involved in ML/TF activities. Such customers may be identified through the periodic AML monitoring performed by the MLRO, AML alert investigation, or identified by the AML/KYC service provider.

On identification of such a person/ customer, the accounts and services provided to such customer shall be immediately blocked by the company and it shall be ensured that the customer does not utilize the portal/ website or any platform of the company to perform transactions or activities. Asset blocking will be first by blocking the login of the customer's app, then communicating via email to circle's reference AML email, after reporting to OFCA. MLRO shall timely inform to the management and Circle about such a customer with the status of blocking of account and assets. After review and approval of Senior Management the OFAC shall be notified of the blocked accounts on timely basis. Confidentiality of the information shall be ensured by Management and MLRO while investigating and reporting in this regard.

Although screening against sanctions lists, Politically Exposed Person ("PEP") and adverse media lists, the MLRO shall escalate matches to Circle (i.e., not to Office of Foreign Assets Control ("OFAC") or other regulatory bodies).

The Management and MLRO shall ensure that any positive match against, sanctions, PEP and adverse media list shall be notified to the Circle via email in circle AML Referral Email within 24 hours.

PEP metrics are managed by checkin.com with their metrics in the KYC process for screening each person. The processes will be aligned with Banqua Sp z.o.o's policy and decision making is still held by the firm.

12 Transaction Thresholds and Monitoring

Management and the MLRO of the Banqua Sp z.o.o, shall ensure that the clients, customers, or persons with whom the company does cryptocurrency business are assessed from the risks point of view. MLRO shall ensure that risk profile of the customers, clients or persons, are created based on the KYC being performed before onboarding and establishing business relationship. Source of income should be legitimate and based on it, the risk profile shall be developed for each customer, client or person. Based on the risk profile, the transaction thresholds shall be created as a tool to monitor the activities of the clients, customers or persons with whom the company deals, invests or trade with.

MLRO shall ensure that transactions and activities of all the clients, customers or persons with whom Banqua Sp z.o.o has established business relationships, are regularly monitored considering the relevant risk profile and transaction threshold. Any breach of the threshold or mismatch of risk profile shall be appropriately investigated and concluded by the MLRO and the management of the Banqua Sp z.o.o.

The company may use the third-party provided services and tools to perform the transaction monitoring. The MLRO and management of the company shall ensure that the third-party service provider has the history of doing business with good reputation in the AML/KYC domain and it has appropriate compliance culture and controls that are necessary to perform the KYC on behalf of its clients. The Board and management including MLRO of the Banqua Sp z.o.o ensure that the third-party service provider complies with the legal and regulatory requirements related to confidentiality of the client's or customer's information.

Transaction monitoring metrics will be provided by our third-party vendor, Scorechain.com. Our analysts filter transactions by certain categories such as:

1. high value transactions
2. small amount sending/receiving from/to multiple senders/recipients

Depending on the company's set up, anything related to fraud will be handled by fraud/ payments and for KYC/ AML will be handled by different levels of analysts.

The company shall record all the transactions and shall separately identify the transactions, whose value exceeds threshold limits prescribed under the applicable AML Act and regulations. MLRO is required to regularly check the prescribed limit under the current AML Act and regulations and report to the relevant authority, (if required).

MLRO shall ensure that only those customers who pass the KYC due diligence process (as per KYC policy) may use account in the app. In case the suspicious transactions or activities are noticed over 5k USD then investigation shall be performed for those accounts and customers. Transactions shall be prevented to/from sanctions blockchain addresses. MLRO and AML service provider shall take control measures such as using sanction wallet screening tools to ensure that transactions are prevented from happening. Transactions are monitored by the MLRO on periodic basis to identify any suspicious activities or transactions in the accounts of the customers. Transaction monitoring may also be initiated based on the alert generated or reported by the service provider.

13 Risk Assessment

The management of Banqua Sp z.o.o shall ensure that risk assessment is performed before and after establishing business relationships. MLRO shall ensure that risk assessment activities are conducted appropriately.

Risk is the likelihood of a negative occurrence or event happening and its consequences. In simple terms, risk is a combination of the chance that something may happen and the degree of damage or loss that may result. To perform the risk assessment, the money laundering and terrorist financing (ML/TF) risks that are identified should be assessed for the inherent and residual assessment perspective.

Inherent risk is the risk of an event or circumstance that exists before the implementation of controls or mitigation measures.

Residual risk is the amount of risk that remains after the application of controls or mitigation measures.

When assessing ML/TF risks, it is important to distinguish between inherent risk and residual risk. The risk-based approach (RBA) focuses on the inherent risks to which the Banqua Sp z.o.o. is

exposed. All the ML/TF risks are required to be identified and assessed from the occurrence and likelihood perspective, on both inherent and residual basis. The risk score is calculated which is the product of the occurrence and likelihood of the risk. Based on the risk scores the classification of ML/TF risks are made as Low, Medium and High. High-level ML/TF risks are critical, therefore, management and MLRO shall take immediate actions to ensure that critical ML/TF risks do not occur. Appropriate mitigation risk measures shall be taken through the application of robust AML controls.

Being in the cryptocurrency business, the Banqua Sp z.o.o shall perform the ML/TF risk assessment periodically, to identify the potential and existing ML/TF risks that arise due to business activities or the activities of the customers, clients, persons and internal processes of the company.

As part of AML compliance, the company must conduct ML/TF risk assessment based on risk-based approach and it must understand:

- the types of money laundering and terrorist financing risks that cryptocurrency business may encounter as a result of its business activities and clients; and
- what is a risk-based approach (RBA) and how companies dealing in cryptocurrencies can use this approach.

Using an RBA enables to:

- conduct a **risk assessment** of cryptocurrency business, operating activities and customers/clients taking into consideration certain elements, including:
    - products, services and delivery channels offered and used by the Banqua Sp z.o.o;
    - the geographic location of Banqua Sp z.o.o cryptocurrency business activities;
    - new cryptocurrency business-related developments and technologies;
    - Banqua Sp z.o.o relationship with all types of clients; and
    - any other relevant factor.
- **mitigate the ML/TF risks,** through the implementation of AML processes and controls, including the ongoing monitoring of business relationships and transactions for:
    - keeping client identification information and, if required, beneficial ownership and business relationship information up to date following the assessed level of risk
    - reassessing the level of risk associated with transactions and activities; and

- applying enhanced due diligence (EDD) measures to those transactions and business relationships identified as high-risk.

ML/TF Risk Indicators:

Below are some ML/TF risk indicators surrounding the cryptocurrency business and related activities that may be used by the Banqua Sp z.o.o during the periodic ML/TF risk assessment exercise:

- The transactional activity far exceeds the projected activity at beginning of the relationship;
- The transactional activity (level or volume) is inconsistent with the client or person or counterparty's apparent financial standing, their usual pattern of activities or occupational information;
- The transactional activity is inconsistent with what is expected from a declared business;
- The volume of transactional activity exceeds the norm for the geographical area;
- Client or person or counterparty appears to be living beyond their means;
- Large and/or rapid movement of funds not commensurate with the client's financial profile;
- Rounded sum transactions atypical of what would be expected from the client or person or counterparty;
- Size or type of transactions is atypical of what is expected from the client or person or counterparty.
- Conducting transactions when the client's address or employment address is outside the local service area without a reasonable explanation.
- There is a sudden change in the client's financial profile, pattern of activity or transactions.
- Client or person or counterparty uses notes, monetary instruments, or products and/or services that are unusual for such a client.

Virtual Currency - ML/TF Risk Indicators:

Below are some of the Virtual Currency (VC) ML/TF risk indicators, that may be referred by the MLRO and the management during the periodic ML/TF risk assessment and transaction investigations:

- The client or person or counterparty makes statements about involvement in criminal activities.
- The client transfers Bitcoin in large volumes in exchange for privacy coins.

- The client is unwilling or unable to provide information about the source of privacy coins they once held or currently have.
- VC addresses match addresses on recognized watch lists such as the list of the Office of Foreign Assets Control (OFAC) or law enforcement information.
- Many clients register with the exchange within a short period using a shared address, mobile device, phone number, IP address and other common identity indicators.
- The client's VC wallet or address is linked to fraudulent activity in media reports and/or cyber security bulletins.
- A platform receives unusual or persistent requests from other exchanges/vendors/service providers in respect of a client's deposited funds or VC.
- Publicity is created around the initial coin offering (ICO) (advertisements, celebrity endorsements, social media ads), also known as pump and dump ICOs.
- The developers are anonymous or information provided about the ICO cannot be verified.
- There is no access to the smart contract, to the code or to technical information about the token's creation.
- There is no possibility to sell the investment or to exit the project to recover the invested funds.
- A series of complicated transfers of funds or VC to multiple addresses or wallets that seems to be an attempt to hide the source and/or intended use of the funds or VC.
- High volume and frequency of transfers between different types of VCs.
- Client provides an anonymous email address obtained through an encrypted email service.
- Funds or VC are added or withdrawn from a VC address or wallet with direct and indirect exposure links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (for example, ransomware) and/or theft reports.
- The VC flows through a large number of intermediate addresses in a very short period of time prior to being added to a client's wallet, or just after being withdrawn.
- The VC passes through mixers/tumblers and is transferred to multiple wallets, where the VC is exchanged for funds.
- The VC originated from an over-the-counter trade broker that advertises its services as privacy-oriented/anonymous.
- The source of funds used for the purchase of large amounts of VC is unknown.

- The email address used in the transaction is linked to advertisements for the sale of VC on peer-to-peer exchange platforms. These advertisements may suggest that the client is buying and selling VC on a commercial scale through a business as a non-registered money services business.
- The client frequently receives funds from multiple payment processors.
- The client makes frequent payments or transfers to companies, post office mailing services or uses money orders from agents of the Crown for the purchase of computer software or hardware.
- Evidence of untruthfulness on behalf of the client (e.g. providing false or misleading information).
- Client or person or counterparty exhibits nervous behaviour.
- Client or person or counterparty refuses to provide information when required, or is reluctant to provide information.
- Client or person or counterparty has a defensive stance to questioning.
- Client or person or counterparty presents confusing details about the transaction or knows few details about its purpose.
- Client or person or counterparty avoids contact with reporting entity employees.
- Client or person or counterparty refuses to identify a source for funds or provides information that is false, misleading, or substantially incorrect.
- Client or person or counterparty exhibits a lack of concern about higher-than-normal transaction costs or fees.
- Client or person or counterparty makes inquiries/statements indicating a desire to avoid reporting or tries to persuade the reporting entity not to file/maintain required reports.
- Insufficient explanation for the source of funds.
- An inability to properly identify the client or there are questions surrounding the client or person or counterparty's identity.
- The Client or person or counterparty refuses or tries to avoid providing information required, or provides information that is misleading, vague, or difficult to verify.
- The Client or person or counterparty refuses to provide information regarding the beneficial owners, or provides information that is false, conflicting, misleading or substantially incorrect.
- The identification document presented by the Client or person or counterparty cannot be authenticated.

- There are inconsistencies in the identification documents or different identifiers provided by the Client or person or counterparty, such as name, address, date of birth or phone number.
- Client or person or counterparty produces seemingly false information or identification that appears to be counterfeited, altered or inaccurate.
- Client or person or counterparty displays a pattern of name variations from one transaction to another or uses aliases.
- Client or person or counterparty alters the transaction after being asked for identity documents.
- The Client or person or counterparty provides only a non-civic address or disguises a post office box as a civic address to conceal their physical residence.
- Common identifiers (e.g. addresses, phone numbers, etc.) are used by multiple client or person or counterparties that do not appear to be related.
- Common identifiers (e.g. addresses, phone numbers, etc.) are used by multiple client or person or counterparties conducting similar transactions.
- Use of the same hotel address by one or more client or person or counterparts.
- Transactions involve client or person or counterparties identified by the media, law enforcement and/or intelligence agencies as being linked to criminal activities.
- Attempts to verify the information provided by a new or prospective client or person or counterparty are difficult.

14 Ongoing Monitoring

The MLRO and account opening/ onboarding team of the Banqua Sp z.o.o shall perform the ongoing transactions and activities monitoring of the clients/customers/persons with whom a business relationship is established. The monitoring shall be performed periodically based on the level of the company's assessment of ML/TF risks. Enhanced monitoring measures shall be taken for the high-risk category customers/clients/persons.

Following methods may be considered to conduct enhanced ongoing monitoring of the high-risk category customers/clients:

- reviewing cryptocurrency transactions based on an approved parameters of trading and investments approved by Board/management of Banqua Sp z.o.o;
- developing reports and reviewing these reports of high-risk transactions more frequently;

- flagging transactions or those activities that deviate from Banqua Sp z.o.o expectations and raise ML/TF risks or concerns;
- setting transaction limits or parameters on accounts or transactions that would trigger early warning signals and require a mandatory review; or
- reviewing transactions and activities more frequently against suspicious transaction indicators relevant to Banqua Sp z.o.o business relationships.

Following records shall be maintained as evidence of ongoing monitoring:

- processes in place to perform ongoing AML monitoring and the enhanced ongoing AML monitoring of high-risk customers/clients/persons; and
- processes in place and information obtained as a result of ongoing monitoring and enhanced ongoing monitoring of high-risk customers/clients/persons;

Ongoing monitoring may not be performed after the relationship with the respective customer is end or terminated.

15 Suspicious Transactions Reporting

The MLRO shall ensure that unusual or suspicious activities/ transactions are identified and reported on timely basis, to the Board and senior management and regulatory authorities.

MLRO of the company shall monitor the frequent high value cryptocurrency transactions, buying, selling, by the clients/customers/persons, and perform investigation to ensure that the illegal/ black money is not used for the transactions.

Alerts generated are investigated and the closure of alerts depend on factors such as nature of the alert generated, communication process with the customer to obtain required evidences etc.

Banqua Sp z.o.o will target to resolve the alert within 2-3 hours of the time the alert is generated. The MLRO will be in charge of analyzing and disposing of the potential flags.

To investigate the suspicious transactions the business relationship team of the company shall contact the respective clients/customers/persons to make appropriate inquiries about the source of income/funds used for transactions, possible change in business activities and risk profile of particular clients/customers/persons. Doubt may be created where a single customer/client/person or related persons frequently conduct cryptocurrency transactions in a

short period, especially the high-value crypto transactions or the transactions with no apparent business purpose or sense.

The company is required to send the suspicious transaction report to the regulator, in a prescribed manner as soon as practicable after the Board and management of the company including the MLRO have taken reasonable measures to establish that there are reasonable grounds to suspect that the transaction or attempted transaction is related to the commission of a money laundering offense or a terrorist activity financing offence. These measures include:

- screening for and identifying suspicious transactions;
- assessing the facts and context surrounding the suspicious transaction;
- linking ML/TF indicators to the assessment of the facts and context; and
- explaining company's grounds for suspicion in an STR, where it articulates how the facts, context and ML/TF indicators allowed to reach grounds for suspicion

Suspicious or abnormal activities and transactions shall be appropriately recorded by the company. All investigations and outcomes shall also be recorded by the company. Before, during and after the investigation, the management of the company shall ensure that confidentiality of the information related to the customer is ensured, and only authorized persons in the company perform the monitoring and investigations, such as MLRO and the authorized person from business team who are in contact with client/customer/person.

Suspicious Activity Reports (SARs) shall be prepared by MLRO for the review and feedback of the Board and senior management. SARs shall be reported to the regulator. Accounts, and business relationships with those clients/customers/persons shall be terminated who are found involved in suspicious activities or transactions.

Banqua Sp z.o.o shall consult with its legal department/ advisor in case activities/ transactions or scenarios require legal consultation from the legal experts.

16 Sanctions

Sanctions and Embargoes ("Sanctions") are tools used by governments, international organisations and supranational bodies to help maintain or restore global peace and security. Sanctions are intended to deter a range of activities including terrorist financing, proliferation financing, and abuses of fundamental human rights.

Sanctions may be imposed in various form in response to a particular circumstance and the most common types of sanctions imposed include:

(i) Economic sanctions – which typically include the withdrawal of customary trade and financial relations for foreign and security policy purposes, for example, the U.S. embargo of Cuba.

(ii) Diplomatic sanctions – defined as the reduction or removal of diplomatic ties which may include limitations or cancellations of high-level government visits or expelling or withdrawing diplomatic missions or staff.

(iii) Trade sanctions – these are restrictions that encompass arms embargoes, restrictions on the use of weapons and restrictions on dual-use items. Trade restrictions are intended to place controls on:

a. The import, export and movement of goods and technology;
b. The provision and supply of services; and
c. The involvement of citizens in these activities

(iv) Financial sanctions are restrictive measures imposed by a government that prohibit an entity from carrying on transactions with or providing financial services to a person or organization designated as a target. These measures can vary and may include the freezing of funds and economic resources to a sanctioned country, government, organization, individual or entity who may be local resident or abroad. Given the nature of services provided by the company, financial sanctions are typically the most common forms of sanctions and restrictive measures Board and Management of the company and MLRO need to monitor.

The Board. Management and MLRO of Banqua Sp z.o.o shall ensure that:

I. Business or activities are not carried out which includes making available funds or other assets, entering into trading or investments, providing financial or other related services, directly or indirectly, wholly or jointly, for the benefit of designated persons; or behaving in a certain way contrary to applicable financial sanctions.

II. written policies and procedures concerning sanctions compliance remain adequate and effective, and therefore such policies shall be reviewed by the Board of the company on at least an annual basis and re-approved and re-issued by the board of directors, at least annually;

III. MLRO and management shall ensure there is adequate and ongoing training of key staff on sanctions compliance as further set out in this Sanctions Policy.

Sanctions screening forms part of customer due diligence processes and procedures (“CDD”) as set out in KYC policy of the Banqua Sp z.o.o. All potential clients and related parties are required

to be subjected to an initial screening via the preferred third-party screening database, World-Check. World-Check is a leading global screening database that pioneered the provision of open-source intelligence for customer database entity screening. World-Check database coverage includes Global Sanctions lists, narrative sanctions (sanctions ownership information) names of politically exposed persons (“PEPs”), close associates and family members, state-owned entities and state invested enterprises.

Board, Management and MLRO of the Banqua Sp z.o.o shall periodically review the sanctions requirements and ensure that all reporting obligations related to Sanctions are identified and complied with on an ongoing basis.

Management and MLRO shall ensure that the blockchain sanctions monitoring is performed periodically, which is not linked to the amount but to the address of the sender or recipient. It shall be ensured transactions are not executed where the address of the sender or recipient relates to blockchain sanctions. (Through the collaboration of our service provider, si scorechain we can control the fund transfer service in blockchain, in which wallet and in which country).

17 Travel Rule

The Banqua Sp z.o.o, shall ensure that the travel rule related to Electronic Fund Transfer (EFT) and Virtual Currency (VC) are complied with to ensure that specific information is included with the information sent or received in an EFT or a VC transfer.

18 Record Keeping and Retention

MLRO shall maintain AML/CFT records including the new customers/clients/persons onboarded with their KYC details, suspicious transactions or activities identified. All the records shall be kept for a minimum period of 7 years in an appropriate manner. All high value sales transactions shall be recorded by the company including the KYC information of the persons/ customers to whom the sales are made, date of transaction/s.

Additionally, MLRO shall ensure that following minimum records are also maintained in an appropriate, safe and accessible manner:

a. Reports shared with the Regulatory authority

b. AML/KYC records received from third-party service providers or AML/KYC performed by the company itself

c. Details and evidence of enhanced due diligence (EDD) measures performed for High-risk category customers/clients/persons

d. Transaction alerts were generated and investigated during the period

e. Suspicious Transaction Reports and their filing with the relevant regulator

f. Large Cryptocurrency/ Virtual Currency Transaction Reports

g. Electronic Funds Transfer Reports

h. Records of transactions of prescribed limits

i. Records of electronic funds transfers

j. Virtual currency exchange transaction tickets

k. Foreign currency exchange transaction tickets

l. Records of account holders such as signature cards, Intended use of an account, applications, account operating agreements, debit and credit memos, deposit slips, account statements, etc.