ANTI - FRAUD POLICY

KBJ PAY IS THE TRADING NAME OF KBJ SP Z.O.O., REGISTERED IN THE ENTREPRENEURS OF KRS KEPT BY THE DISTRICT COURT KRS: FOR THE CAPITAL CITY OF IN WARSAW, XII COMERCIAL DIVISION OF THE NATIONAL COURT UNDER KRS NUMBER 0000897043 REGISTRATION NUMBER 11650131

I. INTRODUCTION

KBJ Pay with its registered seat in Ł ul. Piekna 24/26A, 00-549 Warsaw, Republic of Poland (hereinafter: "the Company"), is legal entity incorporated by law of Republic of Poland and entered into Commercial Register under KRS Number: 0000897043 Registration number 11650131

The objective of this document is to implement risk controls that will aid in the detection and prevention of fraud. It is the intent of the Company to promote consistent organizational behavior and to uphold highest standards of moral and ethics while conducting business.

This Policy applies to all employees as well as shareholders, consultants, vendors, contractors, outside agencies doing business with employees of such agencies, and/or any other parties with a business relationship with the Company.

Management and all Company's employees are responsible for the detection and prevention of fraud, misappropriations, and other irregularities.

Fraud *is defined as the intentional, false representation or concealment of a material fact for the purpose of self-gain, profiteering or inducing another to perform fraudulent acts alone or in partnership. It is a breach of trust and gross violation of the all Company's values.*

Any irregularity that is detected or suspected must be reported immediately to the Company and internally to the Management Board, which coordinates all investigations for taking appropriate action.

The designated channel for communication is an e-mail: info@kbjpay.com

The Anti-Fraud Policy shall apply to any and all acts or omissions that constitute fraudulent or suspected fraudulent activities, including but not limited to those involving crypto assets, financial assets, monetary items such as cash, funds, stocks, proprietary information, intellectual property, materials of value, content, data, real or personal property, consumables, business transactions, agreements, contracts, bribes, gifts, favors, undue influence, or any other improper prioritization or conduct. This Policy encompasses fraudulent or suspected fraudulent conduct carried out for personal gain, whether individually or collectively, by employees, associates, or any other representatives of the Company.

Creating a comprehensive procedure for identifying and controlling fraud, elder abuse, and investment scams involves a multi-faceted approach. Based on information in place, an outline for general procedural the steps, measures of control, patterns to look out for, and tools that can be used:

1. **Policies and Procedures Establishment.**

Development and implementation of clear policies and procedures that outline expectations for identifying and addressing fraud, elder abuse, and investment scams.

2. **Conducting Training and Awareness Programs.**

Providing comprehensive training to employees, especially those in customer-facing roles, about the signs of fraud, elder abuse, and investment scams. Regularly updates employees on emerging fraud schemes and scams. Creating system of on-going trainings and ad hoc trainings, based on event-driven scenarios.

3. **Securing Customer Verification and Due Diligence.**

Implementation of robust customer verification processes to ensure the identities of clients and their intentions. Strict conduct thorough due diligence on new clients, especially those with suspicious or unconventional backgrounds.

4. **Robust Transaction Monitoring.**

Utilization of transaction monitoring systems to identify unusual or suspicious activities, such as large transactions, frequent withdrawals, using multiple cards on the one account or transfers to unfamiliar accounts.

Setting up thresholds and alerts for potentially fraudulent activities, based on assumptions and experience.

5. **Using system of Identifying Red Flags and Patterns.**

Providing trainings to employees to recognize red flags and patterns associated with fraud, elder abuse, and investment scams.

The most common includes:

5.1. Sudden changes in a client's behavior or financial habits.
5.2. Requests for secrecy or urgency in transactions.
5.3. Unexplained withdrawals or transfers.
5.4. Uncharacteristic involvement of third parties in financial transactions.
5.5. Pressure tactics or manipulation used against elderly clients.
5.6. Unsolicited offers promising high returns on investments with little or no risk.
5.7. Requests for personal or financial information via phone, email, or online.

For a more detailed summary of red flags in relation to cryptocurrencies, please see Appendix 1.

6. Securing proper Reporting and Escalation.

Establishment of clear procedures for employees to report suspected cases of fraud, elder abuse, or investment scams internally. System of incentives to encourage employees to escalate concerns to the appropriate authorities or senior management if necessary.

7. **Securing proper and time efficient Collaboration with Authorities.**

Partnerships with law enforcement agencies, regulatory bodies, and elder protection organizations to be established in order to share information and coordinate efforts to combat fraud and elder abuse.

8. **Common Use of Technology and Tools.**

Implementation of fraud detection and prevention software that utilizes artificial intelligence and machine learning algorithms to detect anomalies and patterns indicative of fraud. Data analytics tools to be used to identify trends and anomalies in financial transactions. Employment of customer relationship management (CRM) systems to track interactions with clients and flag any unusual behavior or requests.

9. **Regular Audits and Reviews.**

Regular audits and reviews of internal controls and procedures to identify weaknesses and areas for improvement. Reviews of past cases of fraud, elder abuse, and investment scams to identify commonalities and update prevention measures accordingly. These are to be done internally and externally.

10. **Maintaining Continuous Improvement.**

On-going monitoring and updating policies, procedures, and training programs to adapt to evolving threats and regulatory requirements.

The Company assumes that by following this procedure and incorporating appropriate measures of control, patterns identification, and utilizing the mentioned tools, organizations can enhance their ability to detect and prevent fraud, elder abuse, and investment scams effectively.

II. FRAUD SCHEMES.

Fraud schemes can take various forms and can be perpetrated through different methods. While the specific patterns may vary depending on the type of fraud, there are several common patterns and indicators that can help identify potential fraudulent activities.

Here are key patterns listed, which must be looked out for:

1. **Unusual Account Activity.**
- Sudden or unexplained changes in account balances, such as large deposits or withdrawals, may indicate fraudulent activity.
- Abrupt changes in transaction frequency or amounts that are inconsistent with the customer's typical behavior could be a red flag.

2. **Unauthorized Access.**

- Signs of unauthorized access to accounts, such as multiple failed login attempts or login from unfamiliar locations, may indicate attempted fraud.

3. **Identity Theft.**

- Requests to change account information or reset passwords without proper verification of identity may signal an attempt to commit identity theft.

4. **Social Engineering Tactics.**

- Social engineering tactics, such as phishing emails or phone calls impersonating legitimate organizations, are commonly used to trick individuals into revealing sensitive information or transferring funds.

5. **Account Takeover.**

- Unexplained changes in account ownership or authorized signatories without proper documentation could indicate an account takeover by fraudsters.

6. **Forgery or Falsification.**

- Instances of forged signatures, altered documents, or falsified information may be indicative of fraudulent activity.

7. **Wire Transfers to High-Risk Countries.**

- Large or frequent wire transfers to countries known for financial crime or money laundering activities may raise suspicions of fraud.

8. **Unsolicited Offers and Investment Scams.**

- Unsolicited offers promising unusually high returns with little or no risk, or pressure tactics to invest quickly, are common indicators of investment scams.

9. **Employee Collusion.**

- Collusion between employees and external parties to facilitate fraudulent transactions or cover up unauthorized activities may be detected through unusual patterns of communication or behavior.

10. **Mismatched Documentation.**

- Inconsistencies or discrepancies in documentation, such as address verification or identity proofing, may indicate attempts to deceive.

11. **Account Dormancy followed by Activity.**

- Accounts that have been dormant for an extended period suddenly becoming active with large transactions may indicate fraudulent activity.

12. **Phantom Employees or Vendors.**

- Payments to nonexistent employees or vendors, or inflated invoices for services not rendered, are common indicators of fraudulent schemes.

These are the most widely used patterns that may indicate fraudulent activity. It's essential to remain vigilant and continuously assess transactions and account activities for any anomalies or suspicious behavior. All employees must stay vigilant in order to secure operational activity of the Company.

III. ELDER ABUSE IN FINANCIAL SERVICES.

Elder abuse related to fraud involves exploiting older adults for financial gain through deceptive or manipulative means. Recognizing patterns associated with elder financial exploitation requires vigilance and awareness of common tactics used by perpetrators.

Here are most often used patterns that may indicate elder abuse related to fraud:

1. **Unsolicited Offers and Scams.**

Elderly individuals may receive unsolicited offers through phone calls, emails, or mail promising prizes, lottery winnings, or investment opportunities with high returns and low risk. Scammers may use persuasive tactics to pressure elders into providing personal information, such as Social Security numbers, bank account details, or credit card information.

2. **Deceptive Marketing and Sales Practices.**

False advertising or deceptive sales pitches targeting older adults with products or services that are overpriced, unnecessary, or of poor quality. Misleading claims about the effectiveness or benefits of products, treatments, or services, particularly related to health and wellness.

3. **Identity Theft and Financial Fraud.**

Unauthorized use of an elder's personal or financial information to open credit accounts, apply for loans, or make purchases without their consent. Forged signatures on checks, legal documents, or financial transactions, often carried out by caregivers, family members, or acquaintances.

4. **Power of Attorney Abuse.**

Improper or abusive use of a power of attorney granted by an elderly individual to manage their financial affairs, such as unauthorized withdrawals, transfers, or changes to legal documents.

Coercion or manipulation by individuals with power of attorney authority to gain control over the elder's assets or property.

5. **Investment Scams and Ponzi Schemes.**

Elderly individuals may be targeted by investment scams promising high returns with little or no risk, often involving fraudulent schemes such as Ponzi or pyramid schemes. Fraudsters may exploit the trust and vulnerability of older adults to convince them to invest in fraudulent ventures or financial products.

6. **Family Member or Caregiver Exploitation.**

Financial exploitation may occur when family members, caregivers, or trusted individuals abuse their position of trust to manipulate or control an elder's finances for their own benefit. This

could include withholding funds, stealing cash or valuables, or coercing the elder into making financial decisions against their best interests.

7. **Isolation and Control.**

Perpetrators of elder financial abuse may isolate the victim from family, friends, or other sources of support to maintain control over their finances and prevent detection of the fraud.

Recognizing these patterns and staying informed about common scams and fraud tactics can help protect older adults from financial exploitation. Company's employees must be very vigilant in reviewing accounts that are opened or subsequently used with transaction monitoring. However, due to the nature of the products offered, it can be very difficult to detect any of the above fraud patterns in relation to older people.

IV. INVESTMENT SCAMS.

Identifying investment scams requires a careful assessment of various factors and red flags that may indicate fraudulent activity.

Here are key indicators to help detect investment scams:

1. **Promises of High Returns with Low Risk.**

Investment opportunities that promise unusually high returns with little or no risk should raise suspicion. Legitimate investments typically involve some level of risk, and higher returns often correspond to higher risk.

2. **Guaranteed Returns or Consistent Profits.**

Scammers may guarantee consistent profits or returns on investments, regardless of market conditions or economic factors. In reality, investment returns can fluctuate, and there are no guarantees of profitability.

3. **Pressure to Invest Quickly.**

Fraudsters often use high-pressure sales tactics to create a sense of urgency and prompt individuals to invest hastily without conducting proper due diligence. They may claim limited availability or time-sensitive opportunities to pressure investors into making impulsive decisions.

4. **Unregistered Investments or Offshore Accounts.**

Investments that are not registered with relevant regulatory authorities or involve offshore accounts may be part of fraudulent schemes. Investors should verify the legitimacy of investment opportunities and ensure compliance with regulatory requirements.

5. **Lack of Documentation or Transparency.**

Legitimate investment opportunities typically provide detailed documentation, such as prospectuses, offering memoranda, or financial statements, to inform investors about the risks and terms of the investment. Lack of transparency or refusal to provide documentation should raise concerns.

6. **Complex or Unfamiliar Investment Products.**

Scammers may promote complex or obscure investment products that are difficult to understand or evaluate. Investors should be cautious of investments that lack transparency or involve unfamiliar concepts or structures.

7. **Unsolicited Offers or Cold Calls.**

Unsolicited offers or cold calls promoting investment opportunities should be treated with skepticism. Legitimate investment professionals typically do not engage in unsolicited sales tactics or pressure individuals to invest without proper consideration.

8. **Absence of Professional Credentials or Licensing.**

Investors should verify the credentials and licensing of individuals or firms offering investment advice or services. Professional designations, such as Certified Financial Planner (CFP), Chartered Financial Analyst (CFA), Chartered Accountants provide reassurance of expertise and adherence to ethical standards.

It's essential for investors to conduct thorough due diligence, seek advice from trusted financial professionals, and remain vigilant for potential signs of investment scams.

V. TOOLS AND TECHNOLOGIES.

To prevent fraud schemes, elder abuse, and investment scams, various tools and technologies can be utilized to enhance detection, prevention, and intervention efforts.

Here are commonly used tools in combating these types of financial crimes:

1. **Fraud Detection and Prevention Software:**
- Advanced fraud detection software employs algorithms and machine learning techniques to analyze transactional data and identify patterns indicative of fraudulent activity.
- These systems can flag suspicious transactions in real-time, helping financial institutions mitigate risks and prevent fraud.

2. **Identity Verification Solutions:**

- Identity verification tools use biometric authentication, document verification, and identity verification services to validate the identity of individuals conducting financial transactions.
- By verifying the identity of customers and detecting potentially fraudulent identities, these tools help prevent identity theft and unauthorized account access.

3. **Transaction Monitoring Systems:**

- Transaction monitoring systems continuously monitor financial transactions for unusual or suspicious activity, such as large transactions, multiple transfers to unfamiliar accounts, or deviations from normal spending patterns.
- These systems generate alerts for further investigation by compliance or security teams, enabling proactive fraud prevention measures.

4. **Customer Due Diligence (CDD) Solutions:**

- Customer due diligence solutions assist financial institutions in conducting thorough background checks and risk assessments on customers to identify potential fraud risks and comply with regulatory requirements.
- These solutions may include customer screening against sanctions lists, politically exposed persons (PEP) databases, and adverse media sources.

5. **Data Analytics and Predictive Modeling:**

- Data analytics tools analyze large volumes of financial data to identify trends, anomalies, and patterns indicative of fraudulent behavior.
- Predictive modeling techniques leverage historical data to forecast future fraud risks and optimize fraud prevention strategies.

6. **Cybersecurity Solutions:**

- Robust cybersecurity solutions, such as firewalls, intrusion detection systems, and endpoint protection software, safeguard against cyber threats and unauthorized access to sensitive financial information.
- Encryption technologies protect data in transit and at rest, reducing the risk of data breaches and identity theft.

7. **Education and Awareness Programs:**

- Educational initiatives raise awareness among consumers, employees, and vulnerable populations about common fraud schemes, elder abuse tactics, and investment scams.
- Training programs empower individuals to recognize warning signs, protect their financial assets, and report suspicious activities to relevant authorities.

8. **Regulatory Compliance Software:**

- Regulatory compliance software helps financial institutions adhere to anti-money laundering (AML), know your customer (KYC), and fraud prevention regulations by automating compliance processes, monitoring regulatory changes, and facilitating audit trails.

9. **Collaborative Platforms and Information Sharing Networks:**

- Collaborative platforms and information sharing networks enable financial institutions, law enforcement agencies, government authorities, and industry stakeholders to share

intelligence, collaborate on investigations, and coordinate efforts to combat financial crimes effectively.

10. **Elder Abuse Prevention Tools:**

- Dedicated elder abuse prevention tools, such as elder financial abuse detection software or caregiver monitoring systems, help identify signs of financial exploitation, neglect, or mistreatment among vulnerable elderly populations.
- These tools facilitate early intervention and support the protection of seniors' financial well-being.

VI. TYPICAL FRAUD ASSOCIATED WITH CRYPTO ASSETS.

Taking into consideration main activity of the Company, special section must be added which is related to frauds in crypto assets. Fraud in the crypto assets space encompasses a wide range of deceptive practices aimed at unlawfully obtaining funds or assets from individuals or entities involved in such transactions. Here are some common types of frauds related to crypto:

1. Phishing.

Phishing involves fraudulent attempts to obtain sensitive information such as passwords, private keys, or account credentials by impersonating legitimate entities through fake websites, emails, or messages. Scammers may trick users into disclosing their information, which can then be used to access their cryptocurrency wallets or accounts.

2. Ponzi Schemes.

Ponzi schemes promise investors high returns on their investments but pay returns using funds from new investors rather than legitimate profits. As the scheme grows, it becomes unsustainable, and early investors may receive payouts at the expense of later investors who lose their funds when the scheme collapses.

3. Pyramid Schemes.

Pyramid schemes operate similarly to Ponzi schemes but involve recruiting new participants into a hierarchical structure. Participants are promised returns for recruiting others into the scheme, and the payouts are funded by contributions from new recruits rather than legitimate profits.

4. Exit Scams.

Some cryptocurrency projects or platforms engage in exit scams, where they abruptly shut down operations and disappear with investors' funds. This often occurs after raising funds through ICOs or token sales without delivering the promised product or service.

5. Impersonation Scams.

Scammers impersonate reputable individuals, companies, or cryptocurrency projects on social media platforms or messaging channels to deceive users into sending them funds or divulging sensitive information. They may use fake profiles, misleading information, and persuasive tactics to trick victims into believing they are interacting with legitimate entities.

6. Malware and Hacking.

Malicious actors may use malware, ransomware, or hacking techniques to gain unauthorized access to cryptocurrency wallets, exchanges, or users' devices. They may steal private keys, seed phrases, or other credentials to siphon funds from victims' accounts or demand ransom payments in cryptocurrency.

7. Fake Wallets and Exchanges.

Scammers create fake cryptocurrency wallets or exchanges that mimic legitimate platforms to trick users into depositing funds. Once the funds are deposited, the scammers may disappear with the funds or use them for illicit purposes.

8. Fraudulent Trading Signals.

Scammers offer fraudulent cryptocurrency trading signals or investment advice promising guaranteed profits or insider tips. They may charge fees for access to these signals or encourage users to make trades based on false information, resulting in financial losses for victims.

VII. PROCEDURE RELATED TO POTENTIAL FRAUD DETECTION.

Detecting fraud is a serious matter that requires prompt and effective action to mitigate risks and ensure regulatory compliance. Here's a procedure of steps to follow when fraud has been detected:

1. **Initial Assessment:**

a) Verify the legitimacy of the detected irregularity or suspicious activity.
b) Determine the scope and potential impact of the fraud.

2. **Secure Evidence:**
   Preserve all relevant evidence related to the suspected fraudulent activity. This include, but not limited to, financial records, transaction logs, emails, and any other documentation.
3. **Initiate Internal Investigation:**

a) Conduct a thorough internal investigation to identify the root cause of the fraud, the individuals involved, and any systemic weaknesses in controls or processes that allowed the fraud to occur.
b) Interview relevant employees and review relevant documents and electronic data.
c) Engage external forensic experts if necessary to assist with the investigation.

4. **Implement Remedial Actions:**

a) Take immediate steps to prevent further losses and mitigate risks associated with the fraud.
b) Implement enhanced controls, procedures, and monitoring mechanisms to prevent similar incidents in the future.

5. **Notify Management and Board:**
   Inform senior management and the board of directors about the detected fraud, providing them with a detailed report of the situation.
6. **Consider Disciplinary Actions** (applicable to employees/ contractors):
   a) Determine appropriate disciplinary actions for individuals involved in the fraud, in accordance with company policies and applicable laws.
   b) This may include termination of employment, suspension, or other disciplinary measures.
7. **Review Compliance Obligations:**
   a) Assess any potential regulatory reporting requirements and ensure compliance with applicable laws and regulations.
   b) Report the fraud to regulatory authorities if required by relevant legislation.
8. **Notify Stakeholders:**
   Communicate with relevant stakeholders, such as customers, investors, and business partners, as appropriate, regarding the detected fraud and actions taken to address it.
9. **Review and Update Policies:**
   Review existing policies, procedures, and controls to identify areas for improvement and update them accordingly to strengthen the company's anti-fraud measures.
10. **Monitor and Review:**
    a) Establish ongoing monitoring and review processes to detect and prevent fraud in the future.
    b) Conduct periodic reviews and assessments of the effectiveness of anti-fraud measures.
11. **Document and Learn:**
    Document all findings, actions taken, and lessons learned from the incident to inform future fraud prevention efforts.
12. **Follow Up:**
    Continuously monitor and follow up on remedial actions to ensure effectiveness and address any residual risks or issues.

The above outlined steps may be tailored to the specific circumstances of the detected fraud and to seek guidance from legal counsel and other experts as needed throughout the process.

Additionally, if 3-rd party providers are involved in the process, collaboration with them must be secured on every stage of the proceeding, according to their fraud policies.

Person, who will conduct the internal investigation, will have:

1) free and unrestricted access to all Company’s records, systems and employees,

2) the authority to examine, copy, and/or remove all or any portion of the contents of files, without prior knowledge or consent of any individual who might use or have custody of any such items or facilities when it is within the scope of its investigation,
3) employees under investigation may be asked not to enter or to access any Company web pages, drives or links either personally or through colleagues or other means, until the investigations are complete.

Company reserves the right to question the employee's colleagues, friends, relatives, associates, outside service providers, etc., whom the Company or its investigating team suspects of their involvement. Above are applicable to the subcontractors.

VIII. CONFIDENTIALITY

The Company treats all received information confidentially.

Any employee who suspects dishonest or fraudulent activity will notify the Management Board (or designated person) immediately and should not attempt to personally conduct investigations or interview / interrogation related to any suspected fraudulent act.

Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. This is important in order to avoid damaging the reputations of persons suspected but subsequently found innocent of wrongful conduct and to protect the Company.

Attachments:

Appendix 1 - Fraud Response Procedure for Virtual Asset Service Providers (VASPs).

Appendix 2 - Red Flags for Crypto (VA).

Appendix 1

Fraud Response Procedure for Virtual Asset Service Providers (VASPs).

This document outlines the step-by-step procedure for Virtual Asset Service Providers (VASPs) to follow upon detecting or suspecting fraudulent activity. The procedure ensures compliance with regulatory requirements, minimizes risks, and maintains trust with stakeholders.

Please see the additional procedure guidelines related to Law Enforcement Queries in the AML Policy. This procedure is related to all applicable scenarios when fraudulent activity is detected internally.

I. Steps in the Fraud Response Process

1. Initial Detection and Reporting.

1.1 Identification of Suspicious Activity.

- Suspicious activity can be detected through:
  - Automated monitoring systems.
  - Employee observations or whistleblower reports.
  - Alerts from regulatory bodies or law enforcement.

1.2 Reporting Mechanism.

- The employee or system that detects the fraud must report it immediately through the designated channels:
- Internal reporting system - mailbox: info@kbjpay.com and mailbox of the direct supervisor and/or Management Board member.

1.3 Initial Assessment.

- The designated employee performs a preliminary review to:
  - Validate the report's credibility.
  - Determine the potential scope and impact.
  - Prioritize cases based on severity.

2. Securing Evidence.

2.1 Preservation of Data.

- All relevant data must be secured, including:
  - Documentation obtained from the User.
  - Transaction logs.
  - User communications.
  - System access records.

Above mentioned are done by creating a separate folder with ID number of the client on the sharedrive with printed to pdf all relevant data.

2.2 Access Control.

- The employee must restrict access to accounts, systems, or assets involved in the suspected fraud to prevent further losses or tampering. This action must be documented and added to the created folder.

2.3 Collaboration with Forensic Experts (if applicable).

- The employee decides, based on the factual information, on engagement of external forensic specialists for:
  - Advanced data recovery.
  - Blockchain analytics.
  - Cryptographic investigations.

All actions and findings must be documented and stored in the above mentioned folder.

3. Investigation.

3.1 The designated employee collaborates with various departments in order to obtain full information.

3.2 In Investigation Process designated employee:

- Analyzes transaction(s) pattern(s) and account(s) activity.
- Reviews KYC documentation and user(s) profile(s).
- Traces asset(s) movement(s) using blockchain analysis tools.

3.3 In area of Documentation designated employee must:

- Record all findings, including:
  - Nature of the fraud.
  - Methods used.
  - Individuals or systems involved.

4. Mitigation Measures.

4.1 Designated employee takes Immediate Actions which includes:

- Freeze of accounts associated with fraudulent activity.
- Revoke the system access for employees or third parties involved.
- Notify affected user (if applicable) about the incident and any protective measures.

4.2 Additional Containment actions to be taken:

- To Isolate the fraudulent activity to prevent its spread.
- Temporarily disable vulnerable systems or services, if required.

5. Notification and Reporting

5.1 Internal Notification done by the employee:

- Information to the Management Board or direct supervisor in writing (e-mail).

5.2 External Reporting done by the employee based on the decision of the Management Board.

- Notify regulatory authorities as required under AML/CTF laws.
- Provide reports to law enforcement agencies if the fraud involves criminal activity.

5.3 Customer Communication.

- Issue a formal communication to affected customers, detailing:
  - Nature of the incident.

- Steps taken to mitigate the impact.

6. Post-Incident Actions.

6.1 Review and Analysis is done by the supervisor or employee of the second line of defence.

- A root cause analysis (RCA) to identify gaps in controls should be conducted within two weeks from the information obtained by the designated employee.
- Evaluation of the effectiveness of amended fraud detection and response systems must be conducted.

6.2 Policy and Procedure Updates. The second line of defence employee:

- Updates internal policies and procedures based on lessons learned.
- Enhances monitoring systems to prevent similar incidents.

6.3 Training and Awareness. The MLRO or designated person:

- Conducts targeted training for employees to:
  - Identify new fraud patterns.
  - Reinforce reporting mechanisms.

Roles and Responsibilities

Employees

- Identify and report suspicious activity promptly.
- Cooperate fully with the designated employee who conducts the audit/ investigation.

Designated employee

- Lead investigations and coordinate with relevant departments.
- Ensure compliance with legal and regulatory obligations.

Management

- Support the investigation and allocate necessary resources.
- Approve updates to policies and systems.

Appendix 2

Red Flags for Crypto

The Financial Action Task Force (FATF) released a report highlighting red flag indicators of money laundering and terrorist financing specifically aimed at virtual assets.

These indicators are grouped into six categories:

- transactions
- transaction patterns
- anonymity
- senders or recipients
- source of funds or wealth, and
- geographical risks.

Transactions

Despite the nature of cryptocurrencies being very different to traditional fiat currency, the strategies employed by fraudulent users to launder money often resembles traditional methods. FATF highlighted several types of cryptocurrency transaction that could indicate money laundering may be taking place.

- Structuring transactions in small amounts or in amounts just under reporting thresholds.
- Making high-value transactions in a short period, or in staggered or regular patterns.
- Depositing funds suspected as stolen or fraudulent into crypto wallets.
- Transferring virtual assets to jurisdictions that have non-existent or weak AML/CFT regulation, or a jurisdiction that has no plausible relation to where the customer lives or conducts business.
- Withdrawing virtual funds without any in-between transactions, especially if the withdrawals incur fees, or converting the assets into multiple different assets that incur fees, especially if there is no logical business explanation.

Transaction patterns

Money laundering through Virtual Assets can often be identified through irregular, unusual, or uncommon transaction patterns, such as:

- New accounts opened with large initial deposits that are traded away shortly afterwards.
- New accounts funded with amounts that do not appear consistent with the user's profile.
- Transactions involving multiple assets or accounts with no logical business explanation.
- A number of crypto transactions which result in a loss of money due to account fees.

- Repeated exchanges of fiat money to cryptocurrency without logical business explanation, and small amounts from numerous virtual wallets that are instantly relocated or removed.

Anonymity

These red flag indicators draw from the vulnerabilities of the underlying technology surrounding virtual assets, more specifically the anonymous exchanges that occur between cryptocurrency consumers. Money laundering behaviour that takes advantage of the anonymous nature of cryptocurrencies may show the following characteristics:

- Moving assets from a public, transparent blockchain, such as Bitcoin, to a centralised cryptocurrency exchange and then on to a private or anonymous coin.
- Transactions by customers that involve multiple cryptocurrency type, in particular those that involve highly anonymous currencies that incur additional, unjustifiable fees.
- A significant volume of peer-to-peer transactions that involve mixing services without justification.
- Customers that operate as unregistered or unlicensed service providers for other users on peer-to-peer cryptocurrency sites, who may charge higher fees to their customers than traditional, licensed exchanges.
- The use of decentralised exchanges to transfer assets across borders.
- Funds entering cryptocurrency wallets from IP addresses associated with darknet or similar software, that allows for anonymity and encryption.
- Multiple, unrelated virtual wallets controlled from the same IP address.
- Sending funds to or receiving funds from service providers with weak or non-existent CDD/KYC processes.
- The use of virtual currency ATMs/kiosks in high-risk locations where increased criminal activity frequently takes place.

Senders or recipients

These red flag indicators focus on the behaviours from either the sender or recipient of illicit transactions.

This category can be further categorised as outlined below.

During account creation

- Creating multiple accounts under different names to circumvent restrictions.
- Transactions from non-trusted IP addresses, or IP addresses from sanctioned jurisdictions.
- Users whose internet domain registrations are in different jurisdictions to the one in which they reside, or a jurisdiction with weak controls.

During customer due diligence

- Incomplete or insufficient KYC information, or the customer declines to provide documents upon request or information regarding the source of funds.
- Customers supplying forged documents as part of the onboarding process.
- The sender/recipient lacking knowledge about the transaction, source of funds or client relationship.

Profile

- Customer credentials are shared by another account.
- Discrepancies between the customer's IP address and the IP from which transactions are initiated.
- Customer's details appear on public forums associated with illegal activity.
- A customer is known via public information to law enforcement for criminal activity.

Potential money mules or scam victims

- Senders seem unfamiliar with crypto technology.
- A customer is significantly older than the average user and is engaging in a large number of transactions.
- Potentially vulnerable customers dealing in high-risk transactions.
- A customer purchasing a large amount of assets which is inconsistent with their financial profile.

Other unusual behaviour

- A customer regularly changes their personal details.
- A customer tries to enter a platform from multiple different IP addresses in a short period of time.
- The language used in transaction message fields indicates illicit activity could be present.
- A customer repeatedly conducts transactions with certain individuals at a significant profit or loss.

Source of funds or wealth

- These are red flags that relate to the source of funds or wealth potentially being linked to criminal activity.
- Transactions originating from or sent to online gambling services.
- Transactions with accounts known to be linked to fraud, extortion, ransomware schemes, darknet marketplaces, illicit websites or sanctioned addresses.
- Significant deposits that are out of profile with an unknown source of funds.
- Large deposits into virtual wallets that are immediately withdrawn as fiat currency.
- A virtual wallet linked to multiple credit/debit cards that are known to frequently withdraw large amounts of fiat currency.
- The majority of a customer's wealth derived from crypto investments or initial coin offerings (legitimate or fraudulent).

- Funds received directly from mixing services or wallet tumblers.

Geographical risks

Criminals will often move funds across borders, typically to jurisdictions with weak or no AML/CFT regimes or cryptocurrency guidelines. Red flag indicators related to this activity include:

- Customer funds deriving from or that are sent to a different jurisdiction to the one in which the user is located.
- Customers using cryptocurrency services located in high-risk jurisdictions with limited or no AML regulations in place, and
- A customer relocating their workplace to a high-risk jurisdictions with limited or no AML regulations in place.