ANTI – Financial Crime POLICY

September 2020

Table of Contents

1.Our Company

Wirebloom LTD ("Wirebloom" or the "Firm") is an authorized electronic money institution ("EMI") regulated by the Financial Conduct Authority (FCA) in the UK under license number 900810. We are a fully operational Fintech company providing financial services through our proprietary technological banking platform. Our clients connect to our environment and can access a wide array of payments, banking and remittances services.

Purpose of this policy

This anti-financial crime, or AFC policy sets out the anti-financial crime rules at Wirebloom and will be used to develop and implement appropriate AFC procedures and controls across the Firm.

Wirebloom has no tolerance for financial crime in its business operation and has used industry guidance in the creation of this policy. Wirebloom also recognises current AFC legislation in the UK and has considered the following when implementing this policy;

- Proceeds of Crime Act 2002 - POCA
- Money Laundering and Terrorist Financing Regulations 2019 - MLR
- Terrorism Act 2006 - TA
- Office of Financial Sanctions Implementation - OFSI
- Criminal Finances Act 2017 - CFA
- Financial Action Task Force - FATF
- Joint Money Laundering Steering Group - JMLSG
- FCA Financial Crime Guide - FCA FCG

The main AFC risks at Wirebloom are;

- Money Laundering.
- Terrorist Financing.
- Fraud.
- Bribery & Corruption
- Sanctions Evasion.

Breaches of the above legislation may be considered a criminal offence and result in fines, censure, reputational damage and loss of business confidence. Criminal charges against individuals for breaches or non-compliance could lead to custodial sentences in prison and/or fines.

This policy applies to all employees of Wirebloom, including consultants, contractors, and agency staff, all of whom are collectively referred to as 'staff' in this document.

Senior management of Wirebloom will provide direction to, and oversight of, the AFC strategy as well as apply a risk-based approach across the business.

The firm's AFC Policy has been designed to align with current UK regulatory and legel obligations concerning the prevention of financial crime. Non-compliance or breaches of the policy may expose the Firm to censure, regulatory investigation, penalties and criminal charges. Therefore, Wirebloom expects strict adherence to this policy and its anti-financial crime objectives, failure to do so may be considered gross misconduct and a disciplinary offence.

As a FCA authorised Electronic Money Institution ("EMI"), the Firm has regulatory and legal obligations to help prevent financial crime being present in its daily operations.

As a financial services firm operating in the UK, Wirebloom is required to implement systems and controls that will protect customers and itself from the threat of financial crime. Having robust and appropriate controls, which seek to disrupt financial criminals also helps promote the UK financial system as safe for customers and enhance the UK financial market's reputation as a major global financial centre, which is a key FCA objective.

Wirebloom acknowledges that the threat from financial crime is present in its business model. Financial criminals are becoming more creative and successful at exploiting weaknesses in the AFC frameworks implemented by financial services firms. The controls set out in this policy will seek to disrupt financial crime occurring at Wirebloom, whilst acknowledging financial crime may never be fully eradicated. The Firm's main objectives are to protect its customers and its business model.

Money Laundering Reporting Officer

Wirebloom has appointed Alan Hadley as its Money Laundering Reporting Officer, or MLRO. Alan's main duties will be to ensure Wirebloom is kept up to date on all financial crime matters that may impact the firm, draft appropriate anti-financial crime policies and monitor the effectiveness of Wirebloom's anti-financial crime systems and controls. Alan must also develop training procedures for all staff concerning financial crime at the Firm, how to identify it and how to help prevent it.

Alan is also the Nominated Officer and is also responsible for receiving suspicious activity reports filed by Wirebloom staff and reporting to the FCA, National Crime Agency, OFSI and other law enforcement agencies when necessary.

The MLRO has overall responsibility for the establishment and maintenance of Wirebloom's AFC systems and controls and will report to the Wirebloom Board.

In the absence of the MLRO, the designated Nominated Officers are;

Anna Zaveriuha or Elizabeth Ajani

Wirebloom's appointed MLRO reports directly to the Board of Directors. The main activities of the MLRO comprise, but are not limited to, the following:

- oversight of all aspects of the company's AFC controls.
- focal point for all activities within the company relating to AFC.
- establishing the basis on which a risk-based approach to the prevention of financial crime is put into practice.

- supporting and co-ordinating senior management focus on mitigating financial crime risk in individual business areas; and
- ensuring that the Company's wider responsibility for AFC is addressed centrally through appropriate training activities.

The MLRO is also required to produce reports for Board meetings including, but not limited to, the following items:

- Confirmation that adequate customer due diligence information is being collected and that ongoing monitoring is taking place.
- Summary data relating to complex or unusual transactions.
- Number of internal consents / Suspicious Activity Reports (**SARs**) received from staff members.
- Number of SARs made to the National Crime Agency (**NCA**).
- Information on status of staff training within the company.
- Confirmation that all business records have been properly stored and are retained according to regulatory requirements.
- Changes in the regulatory and legal environment which do or might impact the business.
- Changes in the risk matrix affecting the business; and
- Contacts with the regulator.

1.1 What is Money Laundering?

It is important to understand what money laundering is, how we identify it, why we must help prevent it, and how we use the Firm's systems and controls to achieve this in our day to day duties.

Money Laundering is the process of disguising the origin of the proceeds of crime. Generally, money laundering occurs in three stages:

Placement: Involves introducing cash into the financial system.

Layering: Carrying out complex financial transactions to disguise the illegal source of the cash

Integration: Funds introduced into the economy and used to acquire legitimate assets or fund other criminal activities or legitimate business.

1.3. Offences

There are three broad groups of offences related to money laundering that firms need to avoid committing. These are:

- knowingly assisting (in several specified ways) in concealing, or entering into arrangements for the acquisition, use, and/or possession of, criminal property.
- failing to report knowledge, suspicion, or where there are reasonable grounds for knowing or suspecting, that another person is engaged in money laundering; and
- tipping off or prejudicing an investigation.

If convicted of any of the above offences, individuals can face up to 14 years imprisonment on the UK and an unlimited fine.

1.4. Terrorist Financing

There can be considerable similarities between the movement of terrorist property and the laundering of criminal property: some terrorist groups are known to have well established links with organised criminal activity. However, there are two major differences between terrorist property and criminal property. More generally:

- often only small amounts are required to commit individual terrorist acts, thus increasing the difficulty of tracking the terrorist property.
- terrorists can be funded from legitimately obtained income, including charitable donations, and it is extremely difficult to identify the stage at which legitimate funds become terrorist property.

2. Know Your Business (KYB) Policy

2.1. Purpose

This KYB policy applies to all new and existing customer relationships and to all products and services offered by Wirebloom. KYB is an ongoing, underwriting ‐ based process to gather relevant information about customers and their business and financial activities in order to:

- Facilitate the timely identification of customer activity that is inconsistent with established facts and information. Wirebloom is committed to deterring the use of its products and services for illegal purposes. The KYB policy and supporting procedures are a key component in the program to prevent and detect all forms of financial crime;
- Meet legal and regulatory obligations; and
- Gather enough information to assist in determining appropriate products and services to meet our customers' financial needs.
- Confirming Customer Identity

When establishing a relationship with a customer Wirebloom will confirm the identity of a person or the existence of an entity within acceptable timeframes using acceptable identification methods. When a product or service is being established, inquiries will be made to determine whether it will be used by or for the benefit of a third party. Where required, particulars of the third party and their relationship with the customer will be obtained prior to establishing the relationship.

- Collecting and Recording Customer Information

Wirebloom will collect and record all pertinent information regarding current and prospective customers including beneficial owners, intermediaries and other interested parties and will establish the purpose and intended nature of each relationship. Where applicable, Wirebloom will record the type, volume and frequency of expected account activity and we will make enquiries into the source of incoming funds or assets. The extent of such measures will be determined on a risk ‐ sensitive basis depending on the type of customer, business relationship, product and transactions.

- Verifying Customer Information

Wirebloom will take reasonable and appropriate measures to verify the key information provided by prospective customers to reliable independent sources. Wirebloom will perform additional verification activities for relationships that represent a higher level of risk.

Wirebloom will refuse to enter or continue relationships or conduct transactions with any person or entity that insists on anonymity or provides false, inconsistent or conflicting information where the inconsistency or conflict cannot be resolved after reasonable inquiry.

- Monitoring and Updating Customer Information

Wirebloom will monitor customer activity to identify and report transactions that may be indicative of illegal or improper activity. Wirebloom will keep information regarding the customer and their business and financial activities as accurate, complete and up to date as necessary to fulfil the purpose for which it was collected. When changes in a customer's financial behaviour become apparent, we will take steps to determine the underlying reasons.

2.2. Management Responsibilities

The accountability for confirming identity and recording, verifying and updating customer information resides with management of the business unit where the relationship, product or service is maintained. In special circumstances management may rely on another party, either internal or external to Wirebloom, to perform parts of the Know Your Business process on their behalf. In these cases, the basis for such reliance should be documented, including those processes that provide management with reasonable assurance that these responsibilities have been reliably performed. Where reliance is placed on a party external to Wirebloom, arrangements should be subject to written agreements that clearly define responsibilities for collecting and verifying customer information. The records of the business unit maintaining the relationship should contain all the information required under this policy.

3. Risk-Based Approach

Wirebloom adopts a risk-based approach to managing the risks presented by the business, in line with the current JMLSG guidance.

Wirebloom maintains a standardized risk rating model to conduct risk assessments related to the exposure to money laundering across all client relationships. Wirebloom's AFCrisk profile is determined after identifying and documenting the risk inherent to the business The Wirebloom Board of Directors approves this model on an annual basis and will make changes to its AFC procedures based on new rules and regulations.

The risk-based approach will be proportionate and appropriate to the Firm's business model and align to its regulatory and legal obligations to mitigate against financial crime.

Wirebloom will identify the financial crime risks presented by:

- Industry type
- Number of years in business
- Legal entity
- Complexity type
- Shareholding Structure
- Beneficial owners
- Products
- Geographical areas of operation.
- Value of Transactions
- Political exposed

Consequently, Wirebloom will:

- Design and implement controls to manage and mitigate those risks.
- Monitor and seek to improve the operation of these controls.
- Record what has been done.

The risk-based approach will recognise that financial crime risks vary according to customers, jurisdictions, products and method of delivery.

Wirebloom will implement procedures aligned to its risk assessment and this policy. The procedures will include, but will not be restricted to:

- identification and verification of customer identity
- monitoring of transactions
- review of customers' data according to the risk level presented by the customer and the business
- appropriate training of all staff
- producing appropriate management information
- reporting upward
- effective liaison with all parts of the business
- maintaining up to date knowledge of regulation and legislation.

Wirebloom recognises that risks change over time and will continually and regularly update its risk management procedures.

5. Training

All employees will be made aware, through the annual compulsory training programme, of:

- The risks of financial crime, the relevant legislation, and their obligations under that legislation.
- The identity and responsibilities of Wirebloom's nominated officer (MLRO)
- Wirebloom's procedures in how to recognise and deal with potential financial crime transactions or activity.

Staff training on anti-financial crime measures will be carried out annually for all staff, and details will be recorded.

The MLRO is responsible for oversight of Wirebloom's compliance with its requirements in respect of staff training and has overall responsibility for the establishment and maintenance of effective training arrangements.

Training covers, as a minimum, the following subjects focusing on the relevance to, and implications for, the company:

- the risks of financial crime, the relevant legislation, and obligations under that legislation
- the identity and responsibilities of Wirebloom's nominated officer and MLRO
- the firm's procedures on how to recognise and deal with potential financial crime transactions or activity

6. Sanctions and PEPs Screening

Wirebloom uses an external service provider to screen beneficial owners and directors against recognised Sanctions Lists and Politically Exposed Persons (**PEPs**) lists. Individuals will be screened on on-going basis as well as on initial sign up. Wirebloom will not onboard any clients on the Sanctions List.

6.1. Sanctions Lists

Wirebloom will take all required steps to ensure that all customers with whom a business relationship is established are screened against relevant notices published by:

- the Office of Foreign Assets Control (**OFAC**)
- Her Majesty's Treasury Department – UK (**HMT**)
- European Union sanctions (**EU**)
- United Nations sanctions (**UN**)

Information leading to "fuzzy matches" will be investigated further, for example where the match was related to a name which can be deemed as popular, and this will be compared

against the other information that is collected at point of registration. The full evaluation of the customers data will provide a result.

Any confirmed matches to sanctions lists will be declined or closed, and the necessary reports will be made to the Office of Financial Sanctions Implementation, or OFSI.

6.2. Political Exposed Persons (PEPS)

A politically exposed person is an individual who has been appointed by a community institution, an international body or a state, to a high-profile position within the last 12 months.

These include:

- Heads of state and government
- National and regional members of government and parliaments.
- Heads of military, judiciary, law enforcement and boards of central banks
- Top ranking and senior officials of political parties and board members of state-owned enterprises
- Senior officials of the military, judiciary, and law enforcement agencies
- Senior officials of state agencies and bodies
- High ranking civil servants, senior members of religious groups, and ambassadors, consul, high commissioners
- Senior management and boards of directors of state-owned businesses and organizations
- Mayors and members of local county, city and district assemblies
- Senior officials and functionaries of international or supranational organizations
- Close business associates and immediate family members of such individuals are also considered PEPs within the same category.

Wirebloom will screen clients against the above PEP's list before onboarding. It will continually screen against this list throughout the business relationship. Any confirmed matches of a political exposed person will be declined and terminated.

7. Client Journey

Wirebloom will only onboard entities in the United Kingdom and European Union. Any requests outside of these regions will be declined.

Customer journey can be described as follows:

1. Customer signs up online for a Wirebloom account.
2. Customers are expected to use the Wirebloom account for the following purposes:
    I. Operational support
    II. Settlement from acquirers
    III. Payment of Invoices
    IV. Remit payments to vendor for services provided
    V. Other operational expenses
    VI. Sending funds to their own bank account using the account number assigned to each account
3. Funds in the Wirebloom account can be transferred to the client's bank account or to another Wirebloom account.

7. 1. Account Funding

The Wirebloom account can be funded in the following ways:

- Incoming payments from other companies in the group, partners, vendors, payment service providers, receipt of bank loan.
- P2P: An incoming money transfer from another Wirebloom's account.

7.2. Withdrawing

Funds can be moved out of the account in the following ways:

- Transfers to a bank account: operations executed by Wirebloom on behalf of and under instruction from the client.
- P2P: An outgoing money transfer to another Wirebloom account.

8. Registration

The first requirement of 'knowing your business' for anti-financial crime purposes is to be satisfied that a prospective client is who they claim to be.

Wirebloom will carry out appropriate KYB procedures for all clients. The objective of the KYB process is to ensure Wirebloom holds appropriate information to be able to satisfactorily know who Wirebloom is dealing with.

Wirebloom will utilize business identification procedures to validate its clients. Documenting and maintaining these identification procedures enhances Wirebloom's ability to prevent

financial crime activities. If Wirebloom fails to verify a client within an acceptable time period, all services will be suspended for that client and any accounts opened will be terminated. In addition, the account and services attached to that client will be under stricter scrutiny until the suspension and/or closure is carried out.

The Account opening form collects the following compulsory information:

- Business Legal Name
- Name of Directors
- Name of individuals who own or control more than 25% of its capital or profit, or voting rights
- Trading name
- Trading Address
- Telephone
- Email
- Anticipated use of funds
- Point of contact's details
- Jurisdiction of Incoming and outgoing funds
- Detailed description of business and use of the account
- Expected frequency of transactions
- Any other relevant information regarding the business operation relating to the use of our platform.

At this stage, Wirebloom will screen Directors and Beneficial Owners against Sanctions and PEP lists.

In addition, the system will automatically detect if the details entered are already assigned to another account holder. Wirebloom will only permit one account per customer and so the

details provided will be checked against the existing customer database to confirm that they do not already hold an account, and they were not previously unsuccessful.

9. Full Due Diligence (FDD)

Wirebloom adopts a verification service that enables It to fully retrieve vital company information from commercial registers worldwide. In real time, essential information including business registration number, company name, address, status, key management personnel, and date of incorporation, through government registers and public records are identified. Complete an AML check of the business through PEP, sanction and criminal watch list sources is also carried out and documented.

This process also includes the identification of the Ultimate Beneficial Owners (UBO) enabling Wirebloom to determine natural persons who have an ownership or a management stake in the company.

9.1. Sole traders

The following information will be gathered:

- Full name
- Residential address (if different to the business address)
- Date of Birth
- Business trading name
- Business address
- Purpose and nature of the business relationship

The client's identity will be verified through the submission of at least one of the following documents:

- Passport
- Driving license including photograph
- National ID card

In addition, a proof of the business address will be verified by production of a copy of one of the following:

- Driving license including photograph (if not used above)

- Bank statement (dated within the last 3 months)
- Utility bill (dated within the last 3 months)

The business address will be verified, in addition, by production of a copy of a valid bank statement relating to the business account and a utility bill dated within the last 3 months.

9.2. Partnerships and unincorporated businesses

The following information will be gathered in addition to the above:

- Full name of individual applying
- Business address
- Name of all partners or principals (identifying those who exercise control over the management of the partnership)
- Name of individuals who own or control more than 25% of its capital or profit or voting rights.
- Business trading name (if different)
- Purpose and nature of the business relationship

The customer's identity will be verified by production of a copy of one of the following, valid, documents:

- Partnership Deed
- Membership of a relevant professional or trade association

  And:
- Verify the identity of at least 2 partners or principals (as per the requirements set out above for '9.1. Sole Traders')

- Where a formal partnership agreement exists, a mandate from the partnership authorising the opening of an account and conferring authority on those who will operate it should be obtained.

  And:
- Verify the identity of all individuals who own or control more than 25% of its capital or profit, or voting rights

The business address will be verified, in addition, by production of a copy of a valid bank statement relating to the business account and a utility bill dated within the last 3 months.

9.3. Private companies

The following information will be gathered in addition to the above:

- Full name of company
- Registered number
- Registered office address in country of incorporation
- Business address (if different from registered address)
- Names of all directors (identifying those who exercise control over the management of the company)
- Names of all beneficial owners who own or control more than 25% of its shares or voting rights
- Business trading name (if different)
- Purpose and nature of the business relationship

The customer's identity will be verified by production of a copy of one of the following, valid, documents:

- Certificate of Incorporation (certified copy)
- Memorandum and Articles of Association
- Shareholder register
- Audited accounts (most recent)

  And:
- Verify the identity of at least 2 directors, including 1 controlling director (as per the requirements set out above for '9.1. Sole traders')
- Verify the identity of all beneficial owners and / or shareholders (as per the relevant ownership type)
-

In addition, a copy of a valid bank statement relating to the business account dated within the last 3 months will be requested.

9.4. Non-UK public sector bodies, government, state-owned companies and supernationals

The following information will be gathered:

- Full name of the entity
- Nature and legal status of the entity
- Registered office address
- Name of home state authority

- Business address (if different from registered address)
- Names of all directors (identifying those who exercise control over the management of the entity)
- Purpose and nature of the business relationship

Steps will be taken to understand the ownership of the entity and its relationship with the home state authority and further documentation will be obtained:

- Audited accounts (most recent)

And:

- Verify the identity of at least 2 directors, including 1 controlling director (as per the requirements set out above for '9.1. Sole Traders')

10. Enhanced Due Diligence (EDD)

Enhanced due diligence is required in circumstances giving rise to an overall higher risk.

When assessing the financial crime risks, the following factors will be considered:

- types of individuals involved in the management of the company (PEPs)
- countries or geographic areas (countries identified by credible sources as not having adequate AML/CTF approaches)
- transactions (discrepancies between submitted and detected information)
- delivery channels (businesses introduced by third parties)

Client's subject to EDD are required to provide documentary evidence regarding the legal origin of funds. Failure to provide such may result in a transaction being held.

As a result, senior management will take a decision to continue or terminate business relations with the respective client as well as to continue or terminate business relations with other clients who have the same beneficiaries or who conduct transactions on behalf of the same third persons.

11. Ongoing Due Diligence

Wirebloom performs a periodic re-underwriting of each client triggered by our rule - based system, This re-underwriting process can be triggered simply by the passage of time, by any of the key transaction monitoring events described above, by any change in management or ownership of the business or by any external information that might raise risk related red flags.

12. Transaction Monitoring

Our AFC compliance ensures that ongoing transaction monitoring is conducted to detect transactions which are unusual for the client's profile. All clients are initially accessed using our risk rating model, clients who fall outside of our acceptable scale will not be onboarded.
Every client has a tailored risk profile assigned to them when account is created for them on our portal. This risk profile is in line with the information collected at the time of opening.

Wirebloom performs a comprehensive process of transaction monitoring.
Our system functionalities include daily monitoring of transactions against rules to assist in the detection of suspicious activity.

Key transaction monitoring data points include but are not limited to velocity of transactions, failed transactions, growth and decline in average size of transactions as this may indicate an added risk which warrants additional due diligence.

Transactions which present high risks are placed on hold while being investigated. Further information will be sought from the clients where they must respond within a specific time frame. All investigated triggers are documented.

13. Suspicious Activity Reporting

When any member of staff either knows, suspects or has reasonable grounds for knowing or suspecting that a money laundering offence has been or is being committed they must make a suspicious activity report (**SAR**) to the MLRO.

Staff are not required to actively search for indications that money laundering offences are occurring. However, if they become aware of, or suspect that, such offences are occurring during their normal duties then they shall make a SAR to the MLRO.

Copies of Suspicious Activity Reports are kept for 6 years from the date of filing.

Failure to report a suspicion, known as a failure to disclose id a criminal office under POCA 2002.

13.1. Internal Reporting

All staff must report any activity that they see in the course of their duties and that they think may be suspicious to the MLRO; all such reports must be documented by the member of staff making the report. Wirebloom will provide all necessary training and guidance to ensure that staff are aware of

- Their obligations in this area
- Possible offences and penalties
- Any internal disciplinary sanctions that may apply for not reporting
- Procedures to be followed
- Documentation to be used to make reports
- Where to access further advice and guidance.

13.2. Suspicious Activity Reports – Internal Procedure

Wirebloom has made a SAR template (see Appendix 14.1.) available to staff, all reports must be made using this template to ensure consistency. All reports must be fully documented and must include at a minimum the following information:

- Name and contact details of person making the report
- The client's details
- The suspicious transaction details; date, amount and transaction reference.
- Details of any related transactions (as above)
- The reasons for the suspicions.
-

The fact that a report has been made and the content of the report must always remain confidential. A member of staff who forms or is aware of a suspicion of money laundering shall not discuss it with any outside party or any other member of staff unless directly involved in the matter causing suspicion.

No member of staff shall at any time disclose a money laundering suspicion to the person suspected. If circumstances arise that may cause difficulties with a client contact, the member of staff must seek and follow the instructions of the MLRO.

No copies or records of money laundering suspicion reports are to be made, except by the MLRO who will keep such records secure, and separate.

13.3. MLRO Acknowledgement and Evaluation

All members of staff, anywhere within Wirebloom, shall respond in full to all enquiries made by the MLRO for the purposes of evaluating a SAR. Information provided to the MLRO in response to such enquiries does not breach client confidentiality or professional privilege, and no member of staff shall withhold information on those grounds.

The MLRO will acknowledge every report made. This confirms to the member of staff who raised the matter that their legal obligation to report has been fulfilled. This response will:

- Acknowledge receipt of the report
- Remind the initiator of the report of their obligation to do nothing that might prejudice an investigation or tip off the client
- Provide feedback on the quality of the report and suggest areas of improvement for future reports.

The MLRO will then conduct his own evaluation of the information provided within the report and decide whether to make a disclosure to the NCA. The MLRO's review, evaluation and decision will be recorded.

Any internal enquiries made in relation to the report will be documented.

13.4. Tipping-Off

In some circumstances it may be necessary to obtain information from the customer before deciding whether to make a disclosure to the NCA. In these cases, the MLRO may request an appropriate person (such as a Fraud and Security, Marketing or Customer Services

Supervisor) to make discreet enquiries of a customer. In such circumstances care will be taken to ensure that the offence of 'tipping-off' will be avoided.

Under Section 7 of the Data Protection Act (DPA) a customer can request information regarding any of their personal information held or processed by an organisation – a Subject Access Request.

Section 29 of the DPA provides some exemption from responding to such a request when a SAR has been made, whether it has been reported to the NCA.

Where a Subject Access Request is received, and it is established that a SAR has been issued then the authority of the MLRO must be sought before any information relating to the SAR is released to the customer. The MLRO will keep a record of all such referrals.

13.5. External Reporting

The MLRO if absent, the designated nominated officer shall receive and evaluate internal suspicion reports and decide whether a formal disclosure is to be made to the authorities. If so deciding, the MLRO will make the formal disclosure on behalf of Wirebloom using the Suspicious Activity Report Form (see Appendix 14.2.).

Prior to making any such report the MLRO will undertake internal enquiries to satisfy themselves that, based on the information in the report and the result of their enquiries, they know or suspect, or have reasonable grounds to know or suspect, an offence of money laundering. External reports will not be made until all available information has been considered by the MLRO, unless this would render such reports untimely. Such information includes:

- The financial circumstances of a customer or any person on whose behalf the customer has been acting
- The features of all transactions that the firm has entered with or for the customer or any person on whose behalf the customer has been acting.

The decision whether there is knowledge, suspicion or reasonable grounds for knowledge or suspicion of a money laundering offence will rest with the MLRO or their delegated representative alone. Such a decision will not be subject to the consent of any other person within Wirebloom.

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

13.6. National Crime Agency (NCA)

The disclosure regime for money laundering and terrorist financing is run by the United Kingdom Financial Intelligence Unit (**UKFIU**), within the NCA.

A SAR is the name given to the making of a disclosure to the NCA under either the Proceeds of Crime Act (**POCA**) or the Terrorism Act. The NCA has issued a preferred form which can be found online (www.nationalcrimeagency.gov.uk). This securely encrypted system provided by the NCA allows firms to:

- register the firm and relevant contact persons
- submit a SAR at any time of day
- receive e-mail confirmations of each SAR submitted

SARs can still be submitted in hard copy, although they should be typed and on the preferred form. Firms will not receive acknowledgement of any SARs sent this way.

The national reception point for disclosure of suspicions is the UKFIU within the NCA. The UKFIU address is PO Box 8000, London, SE11 5EN.

The Financial Intelligence Helpdesk can be contacted on 020 7238 8282. Firms can contact NCA on this number for:

- help in submitting a SAR or with the SARs online system
- help on consent issues
- assessing the risk of tipping off so you know whether disclosing information about a particular SAR would prejudice an investigation

The NCA is required to treat any SARs confidentially. Where information from a SAR is disclosed for the purposes of law enforcement, care is taken to ensure that the identity of the reporter and their firm is not disclosed to other persons.

13.7. Seek 'Consent'

Where a report is received prior to a transaction or activity taking place then the MLRO will make the appropriate report to the NCA and seek consent to proceed with that transaction or activity.

The NCA has up to seven (7) days to confirm whether the transaction, for which a consent has been requested, can proceed – until the NCA gives consent, the transaction cannot proceed – it is frozen. In these circumstances, the staff member must be very careful that they do not 'tip off' the customer about the reason for the delay in processing the transaction.

Where the NCA gives notice that consent to a transaction is refused, a further thirty-one (31) day period (the "Moratorium") commences on the day that notice is given. The thirty-one (31) days include Saturdays, Sundays and public holidays. It is an offence to undertake the transaction during this period as the participant would not have the appropriate consent. The Moratorium period enables the NCA to further their investigation into the reported matter using the powers within the POCA in relation to the criminal property (e.g. imposing a restraint order). If the Moratorium period expires and no such action has been taken, the reporter is free to proceed with the act(s) detailed in the initial disclosure.

It is Wirebloom policy that all requests for consent must be processed through the MLRO – it is expressly forbidden for employees to make a 'consent' request direct to the NCA.

14. Record-Keeping

Wirebloom will retain the following records:

- Copies of, or references to, the evidence obtained of a customer's identity for six years after the end of the customer relationship.
- Details of customer transactions for five years from the date of the relevant transaction.
- Records of all AML/CTF training delivered
- Details of actions taken in respect of internal and external suspicion reports.
- Details of information considered by the MLRO or his nominee in respect of an internal report where no external report is made.

Wirebloom will ensure that the above requirements are adhered to, and that the documents are able to be produced on request.

Wirebloom will also ensure an audit trail is evident, this ensures that financial data records can be traced back to its source. Wirebloom will keep copies of the evidence of identification presented. Business records which includes transactions, records of disclosures, letters received from any law enforcement agencies for at least 6 years from the date when the relationship with the customer terminates.

15. Data Protection

In addition to meeting your record keeping requirements, Wirebloom also protects its client data. These include shredding forms or notes with customer and/or transaction information after the required retention period ends, locking customer records in a secure location.

16. Appendices

16.1. Internal Suspicious Activity Report Form

INTERNAL SUSPICIOUS ACTIVITY REPORT FORM

Care must be taken to ensure that this form is not seen by the client. Do not leave it in the client's file. This form must be sent to the MLRO as soon as possible.

To: Money Laundering Reporting Officer

From: _____ (Employee Name)

Date: _____

This SAR Is (Circle which Applies):

1. **A request for consent for a transaction which is not yet completed**
2. **A report on a transaction which has taken place which I consider suspicious**
3. **Report on other business-related activity which I consider suspicious**

I consider the following transaction suspicious and report this under the internal reporting procedure.

Date of Transaction: _____

Amount of Transaction: _____

Client Name: _____

Transaction Number: _____

Reason for suspicion: _____

16.2. Suspicious Activity Report Form- MLRO

SUSPICIOUS ACTIVITY REPORT FORM – MLRO

PRIVATE AND CONFIDENTIAL

SAR NUMBER: _____

Date of Transaction: _____

Amount of Transaction: _____

Client Name: _____

Transaction Number: _____

Reason for suspicion: _____

_____

_____

Internal SAR received from:

Date SAR received:

I can confirm that I have reviewed the internal SAR for this customer and all relevant information provided. Based on the information received and reviewed, the following action has been taken.

Referred to the National Crime Agency - Yes/ No

Decided not to submit a SAR for the following reason _____

_____

_____

Name of MLRO: _____

Date: _____

17. Terms and Acronyms

Terms	Definition
MLRO	Money Laundering Reporting Officer
AFC	Anti – Financial Crime
KYC	Know Your Customer
KYB	Know Your Business
EDD	Enhanced Due Diligence
CDD	Customer Due Diligence
SAR	Suspicious Activity Report
NCA	National Crime Agency
PEP	Politically Exposed Persons
FCA	Financial Conduct Authority
OFAC	Office of Foreign Assets Control
POCA	Proceeds of Crime Act 2002
JMLSG	Joint Money Laundering Steering Group
MLR	Money Laundering Regulations
EMI	Electronic Money Institution
NCIS	National Crime Intelligence Service
HMRC	HM Revenue & Customs
FATF	Financial Action Task Force
UBO	Ultimate Beneficial owner
CTF	Counter Terrorist Financing

