AML Internal Policies and Process Manual

Contents

1. Glossary of terms

3rd AMLD	3rd Money Laundering Directive, EU
AML	Anti-Money Laundering
Beneficial Owner	The individual who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted.
Business Relationship	A business, professional or commercial relationship between a relevant person (i.e. someone to whom the MLR 2007 apply) and a customer, which is expected by the relevant person, at the time when the contact is established, to have an element of duration.
Consent	Permission given by NCA, for the carrying out of any action that would constitute a money laundering offence in the absence of that permission
Criminal Conduct	Conduct which constitutes an offence in any part of the United Kingdom, or would constitute an offence in any part of the United Kingdom if it occurred there.
Criminal Property	Any money or other assets which constitutes a person's benefit from crime.
Customer due diligence (CDD)	Identifying and verifying the identity of the customer and any beneficial owner of the customer, and obtaining information on the purpose of intended nature of the business relationship.
Enhanced due diligence (EDD)	Additional customer due diligence measure that must be applied: Where the customer is a Politically Exposed Person or In any other situation which by its nature can present a higher risk of money laundering or terrorist financing. Asked for additional information on the purpose of the transaction Asked for additional identification Asked for additional information on the

	receiver
FATF	Financial Action Task Force

Financial Sanctions Target List	A consolidated list of targets listed by the United Nations, European Union and United Kingdom under legislation relating to current financial sanctions regimes.
FCA	Financial Control Authority statutory regulator of most financial services providers in the UK
HMRC	Her Majesty's Revenue and Customs. Supervisory authority for all MSB.
Identification	Ascertaining the name of, and other relevant information about, a customer or beneficial owner.
Internal Report	A report made to the Nominated Officer or MLRO in a business.
JMLSG	Joint Money Laundering Steering Group: body representing UK Trade Associations in the Financial Services Industry and aiming to promote good antimony laundering practices and give relevant practical guidance.
Money Laundering	POCA 327, 328 and 329 (1) A person commits an offence if he— conceals criminal property; disguises criminal property; converts criminal property; transfers criminal property; removes criminal property from England and Wales or from Scotland or from Northern Ireland and Constitutes an attempt, conspiracy or indictment to commit such an offence or Constitutes aiding, abetting, counselling or procuring the commission of such an offence or Would constitute an offence specified above if done in the United Kingdom. [POCA, s. 340 (11)] A person also commits an offence of money laundering if he enters into or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property: By concealment

	By removal from the jurisdiction By transfer to nominees or In any other way. [Terrorism Act, s. 18]
MLR 2007	The Money Laundering Regulations 2007
MLRO	Money Laundering Reporting Officer. This term is used to describe the Nominated Officer appointed under regulations 20 (2) (d), MLR 2007 and s331, POCA.
Money Service Business (MSB)	An undertaking which by way of business operates a currency exchange office, transmits money (or any representations of monetary value) by any means or which cashes cheques which are made payable to customers.
Nominated Officer	A person in a firm or organisation nominated by the firm or organisation to receive disclosures under Regulation 7 and s. 330 of POCA from others within the firm or organisation who know or suspect that a person is engaged in money laundering. Similar provisions apply under the Terrorism Act.
Ongoing monitoring of a business relationship	Scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the relevant person's knowledge of the customer, his business and risk profile and Keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up to date.
POCA	Proceeds of Crime Act 2002.
Politically Exposed Person (PEP)	An individual who is or has, at any time in the preceding year, been entrusted with prominent public functions, or an immediate family member of such an individual, or a known close associate, of such persons.
Prejudicing an Investigation	The making of any disclosure or falsifying, concealing, or destroying, or being complicit in these, of any documents that are relevant to a money laundering investigation.
Regulated Sector	Persons and firms which are subject to

	Money Laundering Regulations.
Regulation EC 1781/2006	European Union Wire Transfer Regulations. Obliges payment service providers to send information on the payer with every transfer made on their behalf.
SAR	Suspicious activity report made to NCA.
Senior Management	The directors and senior managers (or equivalent), of a firm who are responsible, either individually or collectively, for management and supervision of the firm's business.
Simplified due diligence	An exception to the obligation to apply the customer due diligence measures for specified customers, e.g. financial institutions subject to the Money Laundering Directive or equivalent legislation and supervision. It is also available for some categories of products and transactions which may be provided by financial institutions.
NCA	National Crime Agency
Supervisory Authority	Bodies identified by MLR 2007 regulation 23 as being empowered to supervise the compliance of relevant businesses with the 2007 Regulations.
Terrorism Act (TA 2000)	Terrorism Act 2000, as amended by the Anti-terrorism, Crime and Security Act 2001.
Terrorist offences	The terrorist offences relate to fundraising, using or possessing terrorist funds, entering into funding arrangements, money laundering, disclosing information relating to the commission of an offence (similar to tipping off), or failing to make a disclosure in the regulated sector. (ss 19 and 21A TA 2000 (as amended)).
Terrorist Property	Money or other property which is likely to be used for the purposes of terrorism (including any resources of a prescribed organisation) or Proceeds of the commission of acts of terrorism or Proceeds of acts carried out for the purposes of terrorism. "Proceeds of an act" includes a reference to any property which wholly or partly, and directly or indirectly, represents the proceeds of the act (including payments

	or other rewards in connection with its commission). “Resources” includes any money or other property which is applied or made available, or is to be applied or made available, for use by the organisation. [Terrorism Act, s.14]
Tipping off	A tipping-off offence is committed if a person knows or suspects that a disclosure falling under POCA s 337 or 338 has been made, and he makes a disclosure which is likely to prejudice any investigation which may be conducted following the disclosure under s 337 or s 338. [POCA, s 333A].
Transaction	The provision of any advice by a business or individual to a client by way of business, or the handling of the client’s finances by way of business. A transaction could be simply operating across a client’s account.
Verification	Verifying the identity of a customer, by reference to reliable, independent source documents, data or information, or of a beneficial owner through carrying out risk-based and adequate measures.

2. Introduction

This manual is designed for the use by the employees of B2BinPay Limited (registered in England) as a guide for responsibilities and processes around AML. This manual is both for the management and the staff and needs to be reviewed regularly, not less than once a year.

It contains the information which all members of staff need to be aware of in order to prevent the business being used to launder the proceeds of crime or terrorist financing. All members of staff are at risk of committing a criminal offence if they assist in a criminal transaction by missing the warning signs.

Therefore, we focus on preventing of money laundering and terrorist financing risk by: 1. Identifying the potential risk 2. Assessing risk characteristics 3. Taking effective action to mitigate risk.

All staff operating with customer transactions must understand the approach and process to be aware of the risk associated with the nature of this business.

Furthermore, they must understand the possible consequences of being used to assist with money laundering and terrorist financing poses. These are risks to the individual and the company equally: 1. criminal and disciplinary sanctions 2. civil action against the firm as a whole and individual directors 3. damage to reputation leading to a loss of business.

We acknowledge that criminals might abuse our systems and try to launder money or finance terrorist activities. In order to protect our business from the involvement in such activities, we must take appropriate measures to manage and mitigate those risks. We must start by understanding who are our customers and what are the transaction patterns to be better placed to assess risks and spot criminal conduct. Therefore, we need to implement clear risk levels and implement reasonable and manageable controls to minimise money laundering and terrorist financing risk.

No matter how thorough our risk assessment or how appropriate our controls, some criminals may still succeed in exploiting us for criminal purposes. A well implemented, documented and constantly reviewed risk based monitoring combined with risk-based judgments on individual customers will empower us to justify our position on managing the risk to law enforcement, courts, HMRC and FCA.

3. Policy Statement

The Directors are committed to operating the business in a transparent and open manner consistent with their regulatory obligations. The directors and MLRO will always ensure that all suspicious activity is reported to the authorities.

As part of this commitment, B2BinPay Limited will adopt strict compliance of all applicable AML rules and regulations with specific emphasis on POCA, the 2007MLR, EU Payment Services Directive 2009, 3rd AMLD and Terrorism Act 2000.

B2BinPay Limited is aware that MSB have in the past been targets of organised crime seeking to launder the proceeds of illicit activity. B2BinPay Limited will always seek to disrupt this activity by cooperating fully with the authorities and reporting all suspicious activity to NCA.

All staff must take steps to ensure compliance with this policy and ensure that they fully understand the material contained in this manual.

It is the policy of B2BinPay Limited that staff must receive AML training on commencement of their duties. Staff will be given a copy of this manual and will be tested on its contents before starting any client facing duties. The MLRO holds copies of all training materials. Updated AML training is given annually. Records of all training including dates delivered and by whom are kept both centrally and on staff personnel files.

The MLRO of B2BinPay Limited is Sergejs Bergis. All issues relating to SAR must be referred to Sergejs in the first instance. The compliance director of B2BinPay Limited is also Sergejs Bergis.

A copy of this manual will be provided to all B2BinPay Limited directors, staff and agents.

4. Roles and Responsibilities

4.1 Senior Management

Senior Management has the overall responsibility for compliance at B2BinPay Limited. They are responsible for developing an internal culture of awareness of financial crimes at the company.

They should ensure that all involved departments are enough funded to guarantee the adequate attention to implement and follow through with these policies.

Senior management will be sent monthly reports by the compliance management on all Criminal Conduct and suspicious cases. They will also receive and consider the annual MLRO reports and will assist in implementing any recommended policies by the Ombudsman.

4.2 Compliance and Risk Management / MLRO

First point of contact for all compliance issues from staff, NCA and senior management. MLRO is responsible for receiving and managing internally all disclosures and making reports. Responsible for review circles of risk-assessment criteria and conducts risk assessments of compliance systems.

MLRO needs to manage the process of random audits of the system, filing and reporting (e.g. once a month report senior management on all Criminal Conduct and suspicious cases and annual report). Also MLRO is responsible for keeping the AML Internal Policy and Process Manual up to date with internal processes and risk areas.

MLRO responsibilities in the company include, but not limited to:

- Receiving disclosures from employees (also known as Suspicious Activity Report-SAR's).
- Deciding if disclosures should be passed on to the National Crime Agency (NCA).
- Reviewing all new laws and deciding how they impact on the operational process of the company
- Preparing a written procedures manual and making it available to all staff and other stakeholders
- Making sure appropriate due diligence is carried out on customers and business partners
- Receiving internal Suspicious Activity Reports (SARs) from staff
- Deciding which internal SAR's need to be reported on to NCA
- Recording all decisions relating to SARs appropriately
- Ensuring staff receive anti-financial crime training when they join and that they receive regular refresher training
- Monitoring business relationships and recording reviews and decisions taken
- Making decisionsabout continuing or terminating trading activity with particular customers
- Making sure that all business records are kept for at least five years from the date of the last customer transaction as per FCA regulations

4.3 AML Department

The AML Department is the cornerstone of the detection of risky customers and transactions. It needs to carefully implement an adequate risk-based approach. Therefore, it needs to feed the self-learning engines to adequately generate a risk profiling of each customer and transaction and assign a scoring. The engine shall be developed that easily the scoring can be changed to increase or decrease areas of risk potential. The team also will be responsible to generate reports and make random manual assessments.

Key responsibilities:

- Partnering with the customer facing teams to collect required legal documents and associated information to meet all regulatory and internal policies.
- Manage and facilitate customer due diligence.
- Undertake quality review of customers' CDD records.
- Serve as point of contact for CDD and reporting issues for designated customers.
- Reviewing and evaluating levels of EDD information risk and escalating as appropriate.
- Reviewing transactions for potential suspicious activity.
- Reviewing customer risk ratings for accuracy.
- Filing suspicious activity reports to MLRO. Ensuring suspicious activity reports are completed accurately and filed within the required timeframes.
- Retaining the appropriate records.

4.4 Customer Facing Staff (Customer Support)

The Customer Support Team is the customer facing entity within the company. Their responsibilities are on the one hand to deal with any complain form incomplete on-boarding, malfunctioning transactions and to monitor transactions in real time.

They will be trained from the MLRO to see transactions flowing through the system to evaluate and give a personal risk scoring.

The Customer Support Team will also be exposed to criminals as they will handle stopped KYC checks, stopped transactions or frozen funds. The MLRO and the management have to train their staff accordingly how to handle such case appropriately and how to report them.

Customer support responsibilities:

- Maintains customer records by updating account information.
- Handling complaints and queries (from customers and staff).
- Resolves product or service problems by clarifying the customer's complaint; determining the cause of the problem; selecting and explaining the best solution to solve the problem; expediting correction or adjustment; following up to ensure resolution.
- Identify and communicate trends and quickly notify leadership of potential issues.
- Sorting security issues.

5. Company Organisational Chart

The directors are responsible for implementation of the AML and Terrorist Act rules within the whole B2BinPay structure.

Insert an organisational chart below:

6. AML Reporting Chart

Internal reporting and communication follows the same reporting line shown in the organisation chart. All decisions are approved by Senior Management of the B2BinPay Limited. The Senior Management is responsible for the general implementation of the organisational structure that will handle Criminal Activity and to manage all the resources available. The Compliance Man-

ager is responsible for providing the training material and keeping the AML Internal Policy and Process Manual up to date. The Staff will report all suspicious activity to the Compliance Manager. The Compliance Manager will be responsible for handling all communication with global structure of B2BinPay. B2BinPay Limited reports all suspicious activity to the Regulators.

The Team of the Compliance Manager and the Technical Chief are also responsible for the implementation of the new finding of the reporting team in the self-learning detection engine.

7. Money Laundering

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origin of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. A process of money laundering will be described below.

7.1 What is Money Laundering?

Money Laundering is the process by which criminally obtained money or other assets (criminal property) are exchanged for 'clean' money or other assets with no obvious link to their criminal origins.

There is not one method of laundering money. Methods can range from the purchase of jewellery or a car to passing money through a complex international web of legitimate businesses and shell companies.

Where the initial proceeds of crime take the form of cash, criminals will often look for ways to allow such cash proceeds to enter the financial system, thereby concealing their origin – this is a classic form of money laundering.

MSB can present criminals with opportunities for money laundering. Strictly speaking, if a company involved in the administration of money services allows funds which are the proceeds of crime to be transferred to another person, such a company will have participated in money laundering activity. It should be noted, however, that such a company would not necessarily be committing a criminal offence - the reasons for this are explained below.

7.2 Stages of Money Laundering

Despite the variety of methods employed, the laundering process is generally accomplished in three main stages:

7.2.1 Placement

The placement stage represents the initial entry of the proceeds from crime into the financial system. Many crimes involve the creation of large amounts of cash. Having large amounts of cash about your person or in your possession at home can often link you to the crime by the Police. Therefore, criminals wish to hide this cash and the best way is to deposit the funds into an account of some sort.

However, entering a bank to deposit a lot of cash is suspicious in itself, especially as bank staff are now well trained to report any suspicious activity and questions will often be asked. Therefore, criminals may try to:

- Divide the cash into smaller amounts and make various deposits into one or more accounts at one or more banks.
- Open several accounts in different names at different institutions.
- Employ or persuade others to deposit funds for them.
- Purchase goods such as jewellery, art and other assets with a view to reselling them at a later date.
- Make deposits with the help of employees of the relevant financial institution.

Transferring this to B2BinPay Limited business:
We need to take care:

- of transactions form multiple accounts for the same receiver
- of transactions from one account to multiple receivers
- of transactions from one town from multiple accounts to the same destination
- of transactions coming from accounts created by auction houses, betting sites or e-wallets providers mainly used by gambling and betting sites

7.2.2 Layering

The layering stage is the most complex and often entails the international movement of the funds. The primary purpose of this stage is to separate the illicit money from source. During these stage money launderers is moving funds electronically from one country to another, then divide them into investments placed in advanced financial options or overseas markets, constantly moving them to elude detection. This is often done by creating complex layers of financial transactions designed to complicate the audit trail and provide anonymity. Often at this stage criminal would aim to transfer funds outside the UK away from the UK authority's jurisdiction.

Examples of such transactions include:

- Selling assets or switching to other forms of investment.
- Transferring money to accounts at other financial institutions.
- Wiring transfers abroad (often using shell companies).
- Depositing cash in overseas banking systems.

7.2.3 Integration

The provision of apparent legitimacy to criminally derived wealth. If the layering process succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as funds derived from legitimate sources (for example, an inheritance, loan payments, asset sales abroad).

It should be noted that the above is a simplified explanation of the money laundering process. In reality, modern financial systems allow criminals to attempt various methods and schemes, some of which are very complicated.

We need to take care of:

- using funds of a sales of assets like as house or jewellery
- using the funds for purchases of real estate, buying stakes in companies, or other large assets

7.3 The Money Laundering Laws

All organisations in the UK involved in the provision of financial services must comply with:

- The Proceeds of Crime Act (2002)
- The Money Laundering Regulations (2007)
- The Terrorism Act 2000

The proceeds of all criminal conduct including drug and terrorist related crime are covered, and an organisation which does not have procedures in place to combat Money Laundering could involve or lead to the commission of an offence by such an organisation.

The Joint Money Laundering Steering Group produces Money Laundering Guidance Notes for Banks and Building Societies and these are revised from time to time and can be found at www.jmlsg.org.uk. These put forward best practice ideas on how UK financial institutions should comply with relevant law.

7.3.1 What are the offences for financial institutions?

The above legislation creates a number of criminal offences relating to money laundering. As a company involved in the provision of financial services, both the company itself and our employees must be aware of these offences, as they could result in heavy penalties for the MLRO, the senior management and/or the employee.

These offences apply to all staff:

Section 327: it is an offence to conceal, disguise, convert, transfer or remove (from the UK) criminal property

Section 328: it is an offence to become concerned in an arrangement which a person knows or suspects facilitates the acquisition, retention, use or control of criminal property

Section 329: it is an offence to acquire, use or has possession of criminal property

These are the ‘main’ money laundering offences and where we refer to ‘Money Laundering’ in this section, what it means is the attempt, conspiracy to or commission of these offences.

"Criminal property" is property which:

- is or represents a person's benefit from criminal conduct; and
- the alleged offender knows or suspects constitutes or represents such a benefit.

"Criminal conduct" is conducting which:

- is an offence in any part of the UK; or
- is an offence in the jurisdiction where the conduct took place

- or where the conduct took place outside the jurisdiction, but would have if it occurred in the UK, attracted a maximum penalty of over 12 months imprisonment

These offences apply to the proceeds of all crimes and to any type of criminal conduct, regardless of amount.

If convicted of either of the offences listed above, a person can receive a maximum of 14 years' imprisonment and/or a fine.

7.3.2 The defences

- You did not know or suspect that the money or property in question was 'criminal property'. Deliberately shutting your eyes to an obviously suspect situation, will not constitute a defence. –
- You made an authorised disclosure i.e.:

* a disclosure to a constable (the police), B2BinPay MLRO or a Nominated Officer;
* and
* made in the form and manner prescribed in the regulations.

7.3.3 Failure to report money laundering

It is an offence for a financial institution or its employee not to report knowledge or suspicion of laundering activity as soon as reasonably possible, except where there is a reasonable excuse not to do so.

However, if a company or person involved in the provision of financial services fails to report money laundering in circumstances where this amounts to serious negligence, they could be deemed to be "assisting" the money launderers, in which case the stricter offence referred to above will have been committed.

If convicted of this offence, a person can receive a maximum of 5 years' imprisonment and/or a fine.

7.3.4 Tipping Off

Section 333A (1): disclosing a SAR. It is an offence for a person to make a disclosure which is likely to prejudice an investigation, when the person knows or suspects that an authorised disclosure has been made.

Section 333A (3): disclosing an investigation. It is an offence to disclose that an investigation into a money laundering offence is being contemplated or carried out if that disclosure is likely to prejudice that investigation. The key point is that you can commit this offence, even where you are unaware that a SAR was submitted.

If convicted of this offence, a person can receive a maximum of 5 years' imprisonment and/or a fine.

7.3.5 Reporting Suspicious Transactions

A report must be submitted to B2BinPay Limited MLRO whenever a transaction or event causes you to be suspicious. Potentially suspicious activity that may indicate money laundering Customers who provide insufficient or suspicious information:

- A customer uses unusual or suspicious identification documents that cannot be readily verified
- A customer uses different taxpayer identification numbers with variations of his or her name
- A business is reluctant, when establishing a new account, to provide complete information about the nature and purpose of its business, anticipated account activity, prior banking relationships, the names of its officers and directors, or information on its business location
- A customer's home or business telephone is disconnected
- The customer's background differs from that which would be expected on the basis of his or her business activities etc.

Funds Transfers:

- Many funds transfers are sent in large, round amounts
- Funds transfer activity occurs to or from a financial secrecy haven, or to or from a higher-risk geographic location without an apparent business reason or when the activity is inconsistent with the customer's business or history
- Funds transfer activity occurs to or from a financial institution located in a higher risk jurisdiction distant from the customer's operations
- Many small, incoming transfers of funds are received, or deposits are made using checks and money orders. Almost immediately, all or most of the transfers or deposits are wired to another city or country in a manner inconsistent with the customer's business or history
- Large, incoming funds transfers are received on behalf of a foreign client, with little or no explicit reason
- Funds transfer activity is unexplained, repetitive, or shows unusual patterns
- Payments or receipts with no apparent links to legitimate contracts, goods, or services are received
- Funds transfers are sent or received from the same person to or from different accounts
- Funds transfers contain limited content and lack related party information etc.

If a particular transaction or activity raises suspicions of money laundering or terrorist financing, B2BinPay Limited shouldn't proceed without getting consent from NCA.

B2BinPay Limited shouldn't proceed without getting consent from the NCA if a particular transaction or activity raises suspicions of money laundering or terrorist financing. The NCA will respond within 7 days of receiving the Suspicious Activity Report.

B2BinPay Limited can proceed with the transaction or activity if it doesn't receive a decision from the NCA within 7 working days from when they received the request. B2BinPay Limited won't be committing an offence because consent is automatically assumed in law if no decision has been received after 7 working days.

If B2BinPay does get a decision within 7 days but the NCA doesn't give B2BinPay Limited permission to proceed, they have a further 31 calendar days to take action. If after that further 31 days B2BinPay Limited have not heard anything from the NCA, B2BinPay Limited can proceed if it wants to. It won't be committing an offence.

A Suspicious Activity Report can be sent to NCA:

- electronically;
- by fax;
- by first class post or courier;
- submit a Suspicious Activity Report online using the NCA online system on their website.

Suspicion has been defined by the courts as being a degree of satisfaction beyond mere speculation, which is based on some foundation, but which does not necessarily amount to belief.

The International Compliance Association has described “suspicion” as being the third stage after “comfort” and “concern”.
B2BinPay Limited and employees could face prosecution if it is proven that nobody did make a report to our own MLRO, even though one had reasonable grounds for suspicion. Therefore, it is important that all employees and management are properly trained and remain vigilant of potential money laundering. The report should be made as soon as reasonably possible – this should normally be within the first 24 hours after discovery.

Punishment on conviction (for not reporting to our MLRO) is a maximum of 5 years’ imprisonment and / or a fine and there may be a case under an assistance offence, if serious negligence is proven, which carries a maximum penalty of 14 years in prison.

7.4 Terrorist Financing

In addition to money laundering offences, the Terrorism Act 2000 also creates a number of additional serious offences relating to the funding of terrorism, including participation in funding arrangements where there is at least reasonable cause to suspect that terrorism is involved.

In the context of the provision of financial services, it is also important to be aware that another offence under the Terrorism Act is Failure to report terrorist financing: It is an offence for a person not to report his belief or suspicion that another person is involved in the funding of terrorism, where that belief or suspicion is based on information which comes to his attention in the course of business.

There is also a “tipping off” offence, similar to that described above in relation to money laundering.

8. Customer On-boarding Process

8.1 KYC process

B2BinPay Limited and its staff are required to keep records of its customers. 2BinPay Limited has to oblige to all the rules in the different legislations it offers its services.

All customers of B2BinPay Limited will fall under the 3rd AMLD, MLR 2007 and Terrorism Act 2000. In these regulations B2BinPay Limited need to collect the identity of its customers and their addresses.

8.1.1 KYC process of individuals (Business to Customer model)

The next table shows the information we should get from the customer and applied CDD measures in regards of establishing relationship with individual.

Individual	CDD
1. Full name 2. Current residential address 3. Date of birth 4. Nationality 5. Identity document number 6. Nature and details of occupation / employment 7. Anticipated level and number of transactions 8. The purpose and reason for opening the account/transaction 9. Source of funds 10. Source of wealth	1. Obtain a government-issued identity document which contains the name, photograph and date of birth. 2. Obtain of a confirmation of residential address.

These Documents are accepted for the prove of identity:

- Passport
- National Identity Card
- Driving Licence
- Armed Forces ID
- Police Warrant Card
- NHS staff ID
- HMRC staff ID
- Immigration Application Card (IND)

For transaction from the UK there needs to be an additional upload of documents. There is a need to proof the address of the customer. In the enhanced DD, B2BinPay Limited needs two independent address proofs to be able to clear the customer KYC process. This applies for all jurisdictions.

There are the documents allowed for the proof of address:

- Driving licence* - only if it has not been used for identification verification
- Inland Revenue Tax notification
- Benefits agency
- Council Tax bill
- Letter from a university, college or language school
- Gas bill
- Electricity bill
- Water bill
- Landline telephone bill
- TV, satellite or cable bill
- Bank or building society statement
- Credit card statement
- Home or motor insurance certificate
- Vehicle registration document

Other situations for individuals

Individual	CDD
Non face-to face identification (where customer is not met personally)	While the documents obtained and seen may be similar to those required in normal 'individual circumstances' it is important to try and obtain some independent corroboration, which may include having them certified by other banks, lawyers, accountants, diplomatic missions, Commissioners of Oaths or Notary Public, or allowing uncertified documents provided the first payment to the account is carried out through an account in the customer's name with a bank from an equivalent jurisdiction.
Customers who cannot provide standard evidence (Such as customers: in lowincome groups; with legal, mental or physical inability to manage their affairs; people under care of others; dependent spouses or minors; students, refugees, migrant workers)	There are good reasons why such customers are unable to provide the documentation for verification, but they too are entitled to financial services and should not be excluded. In these cases, examples of alternate methods of verification that may be used include; 1. letter from relevant authorities, in case of recipients of government benefits/financial support such as unemployment benefit/old-age pension 2. letter from care home manager or employer 3. letter from educational institution 4. a letter or statement of reference from a person of good social standing such as a doctor, a teacher, a lawyer, an accountant, certifying his knowledge that the person is who he claims to be is the lowest level of verification that is acceptable.

8.1.2 KYC process of non-individuals (Business to Business model)

Non individual (corporates, partnerships, trusts, NGOs etc.)	CDD
1. Full legal name of customer 2. Full registered address ((i.e. incorporation, formation, or registration) in country of establishment, including country	Privately and government owned entities (corporates, partnerships, trusts, NGOs etc.) would typically require one of: 1. relevant company registry search, or 2. certified copy of certificate of incorporation/partnership deed/ business registration certificate (or equivalent), or 3. accredited business information service report, or other equivalent independent and reliable sources. As with individuals the guiding principle

	is that the documents used have been issued by the government, government body or agency or accredited/regulated industry body.
3. Registered number or other unique identifying number assigned by government to the entity (e.g. taxpayer identification number)	Using a risk-based approach there could be circumstances where the following could be used to satisfy CDD verification requirements: 1. certain regulated financial institutions can be verified by reference to the regulator's website 2. publicly quoted entities on a recognised exchange typically require evidence of listing on the exchange.
4. List of directors and their personal data	These could be obtained from the following documents: 1. Memorandum and Articles of Association 2. Resolution/Letter of appointment of director 3. Register of the Directors The personal data should be obtained as described in the table for individuals
5. List of authorised signatories and their personal data	1. Power of Attorney 2. Resolution for Authorised Signatory The personal data should be obtained as described in the table for individuals.
6. List of shareholders owning at least 25% of the shares/capital or voting rights and their personal data	1. Memorandum and Articles of Association 2. Register of the Shareholders 3. Share Certificates The personal data should be obtained as described in the table for individuals
7. List of beneficiaries owning at least 25% of the shares/capital or voting rights and their personal data	1. Declaration of Trust 2. Indemnity Agreement 3. Nominee Agreement The personal data should be obtained as described in the table for individuals.
8. Bank account details (bank name, bank country, account number, BIC, SWIFT)	1. Bank statement 2. Letter from the bank 3. Screenshot of the bank account (internet-banking)
9. Business involved in	1. Description of the business 2. Licence/permission if required

8.1.3 Beneficial owners
The Duty to Identify

Money launderers may seek to hide their identity behind nominees, or corporate or trust structures. Regulation 5 requires to identify any beneficial owner who is not the client, and take ade-

quate measures, on a risk-sensitive basis, to verify his identity, so that B2BinPay Limited knows who the beneficial owner is. That includes measures to understand the ownership and control structure of a company, trust or similar arrangement.

Definition of a Beneficial Owner

Beneficial owners are the individuals who enjoy the benefits of ownership even though title some form of property is in another name.

For a corporate body or partnership, a beneficial owner is any individual who:

- owns or controls over 25% of the shares or voting rights or in the case of a partnership, more than 25% of the capital or profits of the partnership; or
- exercises control over the management

For a trust, a beneficial owner includes:

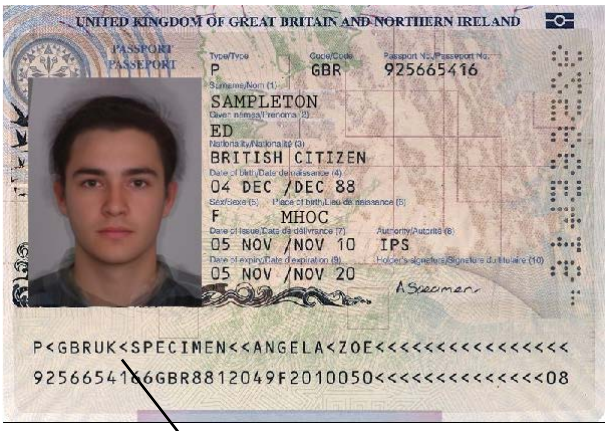
- individuals with interests in 25% or more of the capital of the trust property
- individuals who exercise control over the trust
- the class of individuals that the trust acts for (for example 'homeless persons in London', 'deaf and blind persons', 'children living in the village of Ambridge' or 'someone's children and grand-children')

For other legal entities, or arrangements that administer or distribute funds, a beneficial owner includes:

- individuals who benefit from 25% or more of the entity's property
- individuals who exercise control over 25% or more of the entity's property
- the class of individuals the entity acts for

8.1.4 External review

World-check (or any other ???) will be B2BinPay's external partner in the KYC procedure. Provider will verify all identity documents if they are a true document and not a fraudulent one. Therefore, World-check will prove the following criteria. They will send to B2BinPay OK/NOK respond to every document submitted. If the first one cannot be approved, B2BinPay Limited will ask for a second ID-document.



World-check has the databank connections to verify the name versus the central databases.

8.1.5 Customer Classification

Each Customer will be classified by our system depending on

a. PEP (Politically Exposed Person)
b. Amount send
c. Quantity of transaction within time period
d. Region
e. Sender/Receiver names matching
f. Payout-option chosen

The result of this scoring will trigger different Customer Due Diligence Processes. Each of these criteria has a weighting in the scoring. The weighting will be changing over time as the risk analysis will progress. As we have a risk-based approach, the more risk we see from one criteria the more relevant the criteria will become for the scoring.

Especially we need to take care of PEP. To identify whether the person is PEP this person will be searched against the PEP list integrated into the system. As an alternative method the search engines will be used (google, yandex, etc.)

The definition of a 'PEP' is set out below:

• is or has, at any time in the preceding year, been entrusted with prominent public functions

• is an immediate family member of such a person
• is a known associate of such a person
• is resident outside the UK
• is or has, at any time in the preceding year, been entrusted with a prominent public function by – a) a state other than the UK; b) the European Community; or c) an international body; or
• is an immediate family member or a known close associate of a person referred to in the paragraph immediately above.

Customers also will be checked against the Sanction Lists.

If a similar matching result is found, we do the following: - Apply EDD and add customer to our internal watch list in order to carry out ongoing monitoring.

If an exact matching result is found, we do the following: - Make a disclosure to the relevant authority (Asset Freezing Unit or NCA) and block the customer in our operational system until consent is given to proceed or refuse. In addition, we may cease the business relationship with the customer allowing 30 days' notice to comply with Terms & Conditions.

8.2 Risk Based Machine Learning Model

The core of our AML detection will be our AML Engine. For all stuff a better understand how flagging is being raised by the engine will help in the process of manual reviews are necessary.

8.2.1 Risk Classification:

Our system will classify 5 cases of risk:

- Low
- Intermediate
- Moderate
- High
- Severe

When the Moderate level is reached manually review by educated staff members is mandatory.

Risk Classification	Review Method	CDD and monitoring type	Re-review
Low	Automated	CDD, ongoing monitoring	By perforce (update expired documents, Customer informed about changes)
Intermediate	Automated	CDD, ongoing monitoring	Annually
Moderate	Manually	CDD, ongoing monitoring	Annually
High	Manually	EDD, enhanced ongoing monitoring	Every 6 months
Severe	Manually with approve of senior management (Board of Directors)	EDD, enhanced ongoing monitoring	Every 3-6 months

8.2.2 The behavioural cases:

For the risk scoring the following cases will be considered (the list is not exhaustive):

* User Account Behaviour (examples)

- N transactions from 1 user account to m Mobile Phones (can be time dependent)
- N transactions from n user accounts to 1 Mobile Phone (can be time dependent)
- Unusual Transaction behaviour (deviating from the average)

At beginning conservative limits being set to base the risk profiles. Through positive learning these sensitivities will be raised by machines.

* Transaction Corridor Behaviour Analysis:
- N transactions from n user accounts to m mobile phones in a particular corridor, when the usual transaction quantity is exceeded.
- Search for user account similarities

8.2.4 How can a corridor be defined?

Sender side:

IP Address
Bank or Credit Card Issuer Country
Users Nationality from the KYC Process.

Receiver side:

Country Code

Country Risk Assessment: Countries with a history of fraud and AML will be scored in a certain country risk scoring table.

Country	Risk Score
United Kingdom	Low
Foreign – FATF Member	Intermediate
Foreign – NCCT, INCSR, Corruptions Perception Index, other citation for weak AML	Moderate
Foreign – OFAC , Offshore Tax Haven	High

In-Depth Surveillance for High Risk Countries:

Due to higher risk profile transactions from these countries going to be flagged more often and reviewed manually with special care by staff.

Real Time Network Analysis will take place before every transaction. If connections are recognised which have been flagged before the transaction will be stopped.

Our system is using a Ranking Algorithm, which enables us to integrate an adaptive way to model the relevant risk factors.

Daily, weekly and monthly reports on AML cases to the MLRO will be used to update the ranking for the risk factors. Depending on the corridor the location data can be break down to the granularity of the region levels.

9. On-going monitoring

Regulation requires that company conducts ongoing monitoring of a business relationship on a risk-sensitive and appropriate basis. Ongoing monitoring is defined as:

- scrutiny of transactions undertaken throughout the course of the relationship, (including where necessary, the source of funds), to ensure that the transactions are consistent with the knowledge of the client, their business and the risk profile.

- keeping the documents, data or information obtained for the purpose of applying CDD up-to-date. B2BinPay Limited must also be aware of obligations to keep clients' personal data updated under the Data Protection Act.

Monitoring customer activity helps identify unusual activity. If unusual activities cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions that take place throughout a relationship helps B2BinPay Limited know its customers,
assist to assess risk and provides greater assurance that the company is not being used for the purposes of financial crime.

Monitoring is based on a considered identification of transaction characteristics, such as:

- the unusual nature of a transaction;
- the nature of a series of transactions;
- the geographic destination or origin of a payment; and
- the parties concerned.
- higher risk customer relationships require enhanced ongoing monitoring

10. RECORD KEEPING

10.1 CDD and transaction records

We will store records of all transactions for 5 years from the conclusion of the transaction on behalf of our customers or the end of the relationship. The records we must keep are: 1. copies of or references to the evidence of the customer's ID obtained under our CDD requirements; and 2. the supporting evidence and records in respect of the business relationships and transactions, which are subject of CDD or ongoing monitoring.

All records of CDD documentation are scanned and uploaded into our operational system linked in the customer unique reference number.

10.2 Internal and External SAR Records

As previously indicated, all internal reports will be kept on the SAR file as opposed to the customer file. The report will be kept for 5 years. In addition to this all SAR submitted including correspondence with and will be kept for unlimited period of time.

10.3 Training Records

The company maintains records of all AML training undertaken by staff, the date it was provided and the results of any tests if applicable. These records will be kept for 5 years following the end of employment with the company.

11. Customer Support

Customer Support, being the only directly with the client interacting staff of B2BinPay Limited, will have to be trained especially for the dealing with potential criminal customers. The customer support staff will have to do the training at least annually and read the AML Internal Policies and Process Manual. There will be questionnaires which they have to pass.

Criminals may get in contact with customer support because:
- Their identity check has not been approved
- They have been asked to do the extended due diligence
- They will not be able to set-up a transaction, receiver
- Their payment was refused
- Their assets were frozen

There are many more cases that lead to customer support requests. Requests may also be done by criminals. Therefore, it is very important for the Customer Support Staff to follow these procedures:

1. Every member of staff must be alert for the possibility that the firm's services could be used for money laundering purposes.
2. Alertness to the possibility of money laundering must be combined with an appropriate knowledge of clients' normal arrangements so that members of staff become aware of possible causes of suspicion.
3. A member of staff becoming aware of a possible suspicion shall gather relevant information that is routinely available to them and decide whether there are reasonable grounds to suspect money laundering.
4. A member of support staff who on consideration decides that there may be grounds for suspicion shall in normal circumstances raise the matter with the responsible MLRO. If after discussion they both agree that there are no grounds for suspicion, no further action should be taken.
5. 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.
6. No member of staff shall at any time disclose a money laundering suspicion to the person suspected, whether or not a client, or to any outside party. If circumstances arise that may cause difficulties with client contact, the member of staff must seek and follow the instructions of the MLRO.
7. No member of staff is obliged to discuss a suspicion of money laundering with the responsible Supervisors. They may, if in the circumstances they prefer, contact the MLRO directly.
8. If following the raising of a possible suspicion by a member of staff, or resulting from their own observations, the responsible MLRO decides that there are reasonable grounds to suspect money laundering, he or she must submit a suspicion report to the MLRO, in the format specified by the MLRO for that purpose.
9. An internal suspicion report does not breach client data protection rules, and no member of staff shall fail to make an internal report on those grounds.
10. If a suspicion report results from a matter raised by a member of support staff, the responsible MLRO must advise them in writing that a report has been submitted by reference to the matter discussed on the given date, without including the name of the person(s) suspected. This confirms to the member of staff who raised the matter that their legal obligation to report has been fulfilled.

11. In the circumstance where any member of staff forms a suspicion of money laundering but the responsible MLRO does not agree that there are reasonable grounds for suspicion, the member of staff forming the suspicion must fulfil their legal obligation by submitting a money laundering suspicion report to the MLRO, in the format specified by the MLRO for that purpose (form enclose to this manual). The responsible MLRO of B2BinPay Limited must recognise this legal requirement and assist the staff member in fulfilling it.

12. Whistleblowing

Whistleblowing is when an employee raised a concern about wrongdoing at work. Officially this is called "making a disclosure in the public interest". Employee can raise his concern at any time about an incident that happened in the past, is happening now, or he believes will happen in the near future.

Complaints that count as whistleblowing. Employee is protected by law if he reports any of the following:

- a criminal offence, eg fraud - someone's health and safety is in danger
- risk or actual damage to the environment
- a miscarriage of justice
- the company is breaking the law
- he believes someone is covering up wrongdoing

In the context of the B2BinPay, the term refers to B2BinPay staff raising concerns about issues which may affect customers, the public, other staff or the organisation.

There are a number of ways in which B2BinPay staff can raise concerns but it is generally considered best practice, where appropriate, to first raise a concern within the organisation (directly with a line manager, or staff member designated in the employer's policy for raising concerns). If serious concerns are not addressed satisfactorily then the issue could be escalated to the Chief Executive of the organisation. Issues around wider disclosure, to other bodies including the Serious Fraud Office and the Financial Conduct Authority.

The Serious Fraud Office is one of those prescribed bodies whom an employee can disclose information if the wrongdoing concerns serious or complex fraud, bribery or corruption in a UK company. In such circumstances, SFO would urge to contact them using their secure reporting form on web-site https://report.sfo.gov.uk/sfo-confidential---provide-information-in-confidence.aspx or using the following contact information:

Telephone number: 020 7239 7388 E-mail: confidential@sfo.gsi.gov.uk; Postal address: Serious Fraud Office, Elm House, 10-16 Elm Street, London, WC1X 0BJ.

FCA is a prescribed person under the Public Interest Disclosure Act 1998 (PIDA), which provides the statutory framework for protecting workers from detriment if they blow the whistle on their employer.

If employee wants to blow the whistle he can contact FCA on:

Telephone number: +44 (0)20 7066 9200 during office hours or leave a message on voicemail Email: whistle@fca.org.uk Postal address: Intelligence Department (Ref PIDA), Financial Conduct Authority, 25 The North Colonnade, London, E14 5HS.

A list of the prescribed persons and bodies who employee can make a disclosure to, can be found on the UK government web-site:
https://www.gov.uk/government/publications/blowing-the-whistle-list-ofprescribed-people-and-bodies--2.
There is also a brief description about the matters that can be reported to each prescribed person.

The Public Interest Disclosure Act 1998 (PIDA), which amended the Employment Rights Act 1996, provides protection for individuals who suffer a detriment by any act or any deliberate failure to act by their employer for raising a genuine concern.

Section 43B(1) of the Employment Rights Act 1996 (as amended by s.1 of the PIDA) sets out what constitutes a "qualifying disclosure" and is therefore protected under the Act. In particular, it is important to note that the Act's protections only apply to "information" which falls into one of the listed categories.

13. Company Training for AML

Annual Training (at least once a year) and up to date information for all staff is very important and required by regulator. Therefore, we have subscribed to the SWAT UK Complete Program.

http://www.swat.co.uk/Training/OnlineAntiMoneyLaunderingTrainingCourses/AMLSpecialistWebinars.aspx

Senior Management has already taken a second online course from High Speed Training on "Anti-Money Laundering (AML) and Financial Crime". This is to make sure all is covered and they are fully aware of the risks.

At the end of every online course there is a test each staff member has to take. The test has to be taken before commencement of their duties in their position. Currently duties that face risk of allying money laundering are Product Development, AML Engine Development Team, Customer Support and Senior Management.

In addition, though SWAT UK we have subscribed to the up-date newsletter which will enable B2BinPay Limited to stay up-to date with the changing requirements and findings. This will help the company further to keep all staff fully informed on regulatory requirements and then the new insights of AML prevention.

14. Annex 1. AML Suspicious activity report

The form is available for all staff:

Report submitted by:	Date of report:
Report received by (MLRO/Deputy)	Date acknowledged:

Client reference (optional):	

Name of entity with suspicious transaction:	
Name(s) of any associated individual(s):	

Description of suspicious activity:
Detail below what investigative work has been undertaken, if any:

Follow up action:	
Date report dealt with / resolved	
Date reported to the NCA	

MLRO Comments	

15 Annex 2. Annual Declaration of Staff

I confirm that:

* I have read, understood and will comply with the firm's written policies and procedures on antimony laundering.
* I have been trained on:
- the Money Laundering Regulations 2007, as amended;
- the money laundering aspects of the Proceeds of Crime Act 2002, as amended; - - the Terrorism Act 2000, as amended, and the related anti-terrorist financing legislation.
* I have received regular training on how to recognise and deal with suspicious transactions.
* I understand my duty to report knowledge or suspicion of money laundering or terrorist financing and will fulfil my obligations in this area.
* I am aware of the prohibition on making any disclosure that could amount to tipping off or prejudicing an investigation.

Signature_____

Name: Date completed

16. Annex 3. Senior Management and MLRO Quarterly Check List

1. Have the specimen policies and procedures been tailored to the firm's individual risks / needs?	Yes / No	
2. Are these policies and procedures still appropriate in the light of the current client base?	Yes/No/Updated	
3. Can you demonstrate that all staff completed the Introductory Money Laundering training?	Yes/No/N/A	
4. Where appropriate, can you demonstrate that all staff have either watched the annual AML update webinar or are familiar with the issues dealt with in the webinar?	Yes/No/N/A	
5. Where appropriate, can you demonstrate that specialist staff have attended the specialist AML training or are familiar with the issues dealt with in it?	Yes/No/N/A	
6. Can you demonstrate that all staff are aware of the issues raised in the monthly update newswire?	Yes/No/N/A	
7. Have all staff signed the annual declaration of money laundering awareness form?	Yes/No/N/A	

Client Check List		
8. A risk assessment for all clients	Yes / No	
9. Adequate know your client (KYC) information about the clients	Yes / No	

Review any suspicious activity reports received:

10. Review any suspicious activity reports received and confirm that they have all been reported to the NCA or a note made of why no such report was required	Yes/No/N/A	
11. Consider whether the pattern of reporting suggests that one or more staff are unaware of or ignoring their obligation to report suspicious activities to the MLRO.	Yes/No/N/A	

Action points (specify any follow up work required as a result of this review)				
No	Action point	Who is responsible ?	Deadline for completion	Completed/comments

17. Annex 4. Annual MLRO Report

Authorised/Licensed Firm's Name:	
Reporting Period:	
Financial Year End:	
Date of submission to Senior Management:	

Adequacy and effectiveness - AML/CFT
The report must assess the adequacy and effectiveness of the Firm's AML/CFT policies, procedures, systems and controls in preventing money laundering and terrorist financing.

The AML/CFT policies, procedures, systems and controls are:			
☐ Adequate	☐ Partially adequate	☐ Not adequate	☐ Not assessed yet
Comments: (How the adequacy assessment was conducted, areas of inadequacy…)			
The AML/CFT policies, procedures, systems and controls are:			
☐ Effective	☐ Partially effective	☐ Not effective	☐ Not assessed yet
Comments: (How the effectiveness was assessed, areas of ineffectiveness…)			

Suspicious Transaction Reports - AML/CFT
The report must include: the numbers and types of internal suspicious transaction reports made to the MLRO the number of these reports that have, and the number of these reports that have not, been passed on to the FIU the reasons why reports have or have not been passed on to the FIU

Internal STRs made to the MLRO	
☐ Yes	☐ No
Comments:	
If yes, the number & type(s) of Internal STRs made to the MLRO	
Comments: (detail the type of reports – refer to the FIU "Guide to ML/TF Suspicious Transaction Reporting")	
Internal STRs passed to the FIU	
☐ Yes	☐ No
Comments:	
If yes, the number of Internal STRs and reason(s) why the Internal STRs have been passed to the FIU **Was the Regulator informed in writing that the Firm has made a report to the FIU as per AML/CFT?**	
Comments:	
If no, the number of Internal STRs and the reason(s) why the Internal STRs have not been passed to the FIU	
Comments:	

Breach reports - AML/CFT
The report must include the numbers and types of breaches by the firm of the AML/CFT Law, these rules, or the Firm's AML/CFT policies, procedures, systems and controls

The number of breaches by the Firm of the AML/CFT Law, the AML/CFT Rules 2010, or the firm's AML/CFT policies, procedures, systems and controls			
Comments:			
The type of breaches by the Firm of the AML/CFT Law, the AML/CFT Rules 2010, or the Firm's AML/CFT policies, procedures, systems and controls			
☐ AML/CFT Law	☐ AML/CFTR	☐ Firm's AML/CFT policies,	☐ Other

		procedures, systems and controls	
Comments: (article/section/division, reasons, remediation action, prevention plan…)			

Improvements - AML/CFT
The report must include: areas where the Firm's AML/CFT policies, procedures, systems and controls should be improved, and proposals for making appropriate improvements

Area(s) of improvement				
☐ Policies	☐ Procedures	☐ Systems	☐ Controls	☐ no need for improvement
Comments: (how the areas of improvement were identified, what were they…)				
Proposal(s) for making appropriate improvements				
Comments: (type of improvement, action plan/timeframe, resources needed, senior management engagement…)				

Training - AML/CFT
The report must include: a summary of the AML/CFT training delivered to the firm's officers and employees areas where the Firm's AML/CFT training programme should be improved, and proposals for making appropriate improvements

The Firm has ensured that an appropriate training program has been delivered to its employees			
☐ Yes		☐ No	
Comments: (how did the firm determine whether the training was appropriate if no, why not, what is the remediation plan?)			
The Firm has delivered AML/CFT training program to:			
☐ the totality of the Firm's employees	☐ most of the Firm's employees	☐ to a few number of the Firm's employees	☐AML/CFT training program has not been delivered to the Firm's
Comments: (who received the training? who did not? why not? remediation program in place…)			

Summary of the AML/CFT programme	
Comments: (summary of the program, how did the program assist the Firm in discharging its obligations)	
Areas where the Firm's AML/CFT training programme should be improved	
☐ Yes	☐ No areas to improve
Comments: (if yes, what are they?)	
Proposals in place for making appropriate improvements	
☐ Yes	☐ No proposals
Comments: (if yes, what are they?)	

High Risk customers - AML/CFT
The report must include the number and types of customers of the firm that are cate-

gorised as high risk

Customers of the Firm categorised as high risk from a AML/CFT perspective			
☐ Yes		☐ No high risk customers	
Number of high risk customers:			
Comments: (further details…)			
If, yes, the type of customers of the Firm that are categorised as high risk from a AML/CFT perspective			
☐ Individuals	☐ Corporate	☐ Financial Institutions	☐ Other
Comments: (further details…)			
Assessment of the Firm's AML/CFT risk			
☐ High	☐ Medium	☐ Low	☐ AML/CFT risk not assessed yet
Comments:			
The Firm's approach to mitigate the AML/CFT risk that it faces			
Comments:			

Action Plans - AML/CFT
The report must include: progress in implementing any AML/CFT action plans

The action plan was subsequent to:			
☐ The AML Self-Assessment	☐ The Previous Annual MLRO report	☐ A Risk Assessment Visit undertaken by the regulator	☐ Other
Comments:			
Progress in the action plan implementation			
Item		**Progress made**	

Quality Assurance - AML/CFT
The report must include: the outcome of any relevant quality assurance or audit reviews in relation to the Firm's AML/CFT policies, procedures, systems and controls

Type of independent reviewer			
☐ Internal audit	☐ External audit	☐ Independent review by Compliance	☐ Other independent reviewer
Comments: (period, examiners, scope, methodology, MLRO & Senior management			

comments on the findings, action plan …)			
Outcome of independent reviews			
Finding		**Action Plan**	

Other matters	
Comments:	
Submitted By: [Name of MLRO, Authorised/Licensed Firm]	
Date:	
Signed:	

Senior Management consideration - AML/CFT
The Senior Management of a Firm must, within 4 months of the year end— consider each report made to it by the MLRO; and if the report identifies deficiencies in the Firm's compliance with the AML/CFT Law or these rules—approve an action plan to remedy the deficiencies in a timely way

Senior Management consideration of the report		
Yes		No
Senior Management's comment(s):		
Senior Management approval of an action plan to remedy the deficiencies in a timely way		
☐ Yes	☐ No	☐ Not applicable
Comments: (what are these action plans, what are the resources allocated for implementation, what are the deadlines set…)		

Agreed By: [Name/ Senior Management of Authorised/Licensed Firm]	
Title:	
Date:	
Signed:	

18. Annex 5. Current Lists integrated in our System where we take the names from:

- Bank of England Consolidated List
- UK HM Treasury List
- UK FCA
- Bureau of Industry and Security List
- DTC Debarred Parties
- European Union Consolidated List
- FBI Hijack Suspects
- FBI Most Wanted
- FBI Most Wanted Terrorists
- FBI Seeking Information
- FBI Top Ten Most Wanted
- Hong Kong Monetary Authority List
- Interpol Most Wanted
- Monetary Authority of Singapore List
- Non-proliferation Sanctions, U.S. Department of State, ISN
- OFAC Non-SDN Entity List
- OFAC Sanctions
- OFAC's Specially Designated Nationals & Blocked Persons Politically Exposed Persons
- Primary Money Laundering Concern
- Primary money laundering concern - Jurisdictions
- Terrorist Exclusion List
- United Nations Consolidated List
- World Bank Debarred Parties
- World Bank Ineligible Firms
- Reserve Bank of Australia
- OSFI Country
- OSFI Consolidate List
- OIG Exclusions
- Offshore Financial Centres
- Japan MOF Sanctions
- Japan Meti-WMD Proliferators
- Japan FSA
- Ireland Financial Regulator unauthorized firms
- HVD LDP
- Hong Kong Monetary Authority
- HM Treasury Investment Ban list
- Foreign Agents Registrations
- FATF – Financial Action Task Force
- Commodity Future Trading Commission Sanction
- Chefs of State and Foreign Cabinets Members
- Australia Department of Foreign affairs and trade
- EPLS