Financial Services and Money Laundering

You will comply with the provisions and requirements contained in the Financial Services and Markets Act 2000 and regulations made thereunder and the Proceeds of Crime Finances Act 2017 and the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 and the Companies instructions relating thereto.

ABS IT Services will carry out its due diligence in accordance with the following regulations:

- The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017
- The Criminal Finances Act 2017
- The Proceeds of Crime Act 2002 (as amended by the Crime and Courts Act 2013 and the Serious Crime Act 2015)
- The Money Laundering Regulations 2007
- The Terrorism Act 2000 (as amended by the Anti-Terrorism, Crime and Security Act 2001, the Terrorism Act 2006 and the Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007).

The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017

The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 came into force on the 26th June 2017 and replaces the Money Laundering Regulation 2007. With the introduction of the Proceeds of Crime Act 2002 and the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 it has broadened the definition of money laundering as well as widening the range of activities controlled by the statutory framework.

There are regulatory requirement overlaps in the various legislations, to avoid duplication of information and to circumvent confusion, this document to cover all requirements over a number of legislations and regulations.

All anti-money laundering and anti-bribery procedures follow the same 6 steps of prevention, which has been set out in the Criminal Finances Act 2017 section in more detail. The 6 principles ABS IT Services follows are:

1. Risk Assessment
2. Proportionality of Risk-Based Prevention Procedures
3. Top Level Commitment
4. Due Diligence
5. Communications and Training
6. Monitoring and Reviewing

The Proceeds of Crime Act 2002 and Money Laundering Regulations 2007

There has been a considerable amount of changes to the legislation regarding money laundering contained within the Proceeds of Crime Act 2002 (POCA) and Money Laundering Regulations 2007.

This policy applies to all employees of ABS IT Services and aims to maintain high standard of conduct and comply with all legal and regulatory requirements.

Please note that the prevention policy is covered under the Criminal Finances Act 2017 section.

What is Money Laundering?

The term Money Laundering is use for a number of offenses involving proceeds of crime or terrorist funds and comprises of the following acts:

- Concealing, disguising, converting, transferring or removing criminal property from the UK
- Entering into or becoming concerned in an arrangement in which someone knowingly (or suspects) facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person
- Acquiring, using or possessing criminal property as well as accepting stole items knowingly or knowingly taking advantage of or accepting items paid for by the proceeds of crime
- Becoming concerned in an arrangement facilitating concealment, removal from the jurisdiction, transfer to nominees or any other retention or control of terrorism property (section 18 of the Terrorist Act 2000)

Please note that the above are primary money laundering offenses and therefore are prohibited activities under the Proceeds of Crime Act 2002.

There are 2 third-party offences that should be noted:

1. Failure to disclose one of the prime offences
2. Tipping off: This is where someone informs a person(s) that are suspected of being involved in money laundering and as a result reduces the probability of being investigated or prejudicing an investigation.

Criminal Property is defined in the Proceeds of Crime Act 2002 as 'property' that is or presents the person's benefit from illegal action in whole or part and the person knows or suspects that it is the proceeds of a criminal act, therefore ALL property wherever located and includes:

- Money
- All forms of property, real or personal, heritable or moveable
- Things in action and other intangible property (drugs trafficking, people trafficking, prostitution, burglary, fraud, tax evasion)

There is a real possibility that any employee could be caught by the money laundering provisions if he or she knows, or suspects money laundering is or will occur and either becomes involved with it or does nothing about it.

ABS IT Services Responsibility is to undertake the following:

- Appoint a Money Laundering Reporting Officer (MLRO) to be a point of contact for employees to report/ disclose any money laundering activities.
- Implement a procedure to report suspicion of money laundering
- Gather client ID documentation
- Maintain records

Money Laundering Reporting Officer (MLRO)

ABS IT Services has nominated the Head of HR as the primary MLRO and in his/her absence has nominated the Managing Director as the secondary MLRO and their contacts are as follows:

Head of HR	Managing Director
25 Hercules Way **Farnborough** **Hampshire** **GU14 6UU**	34 Hercules Way Farnborough Hampshire GU14 6UU
Email: Kiran.Mahay@ABSbiz.co.uk	Email: Paul.Aujla@ABSbiz.co.uk
Tel: 01252 413 733	**Tel: 01252 413 737**

Reporting Your Suspicions

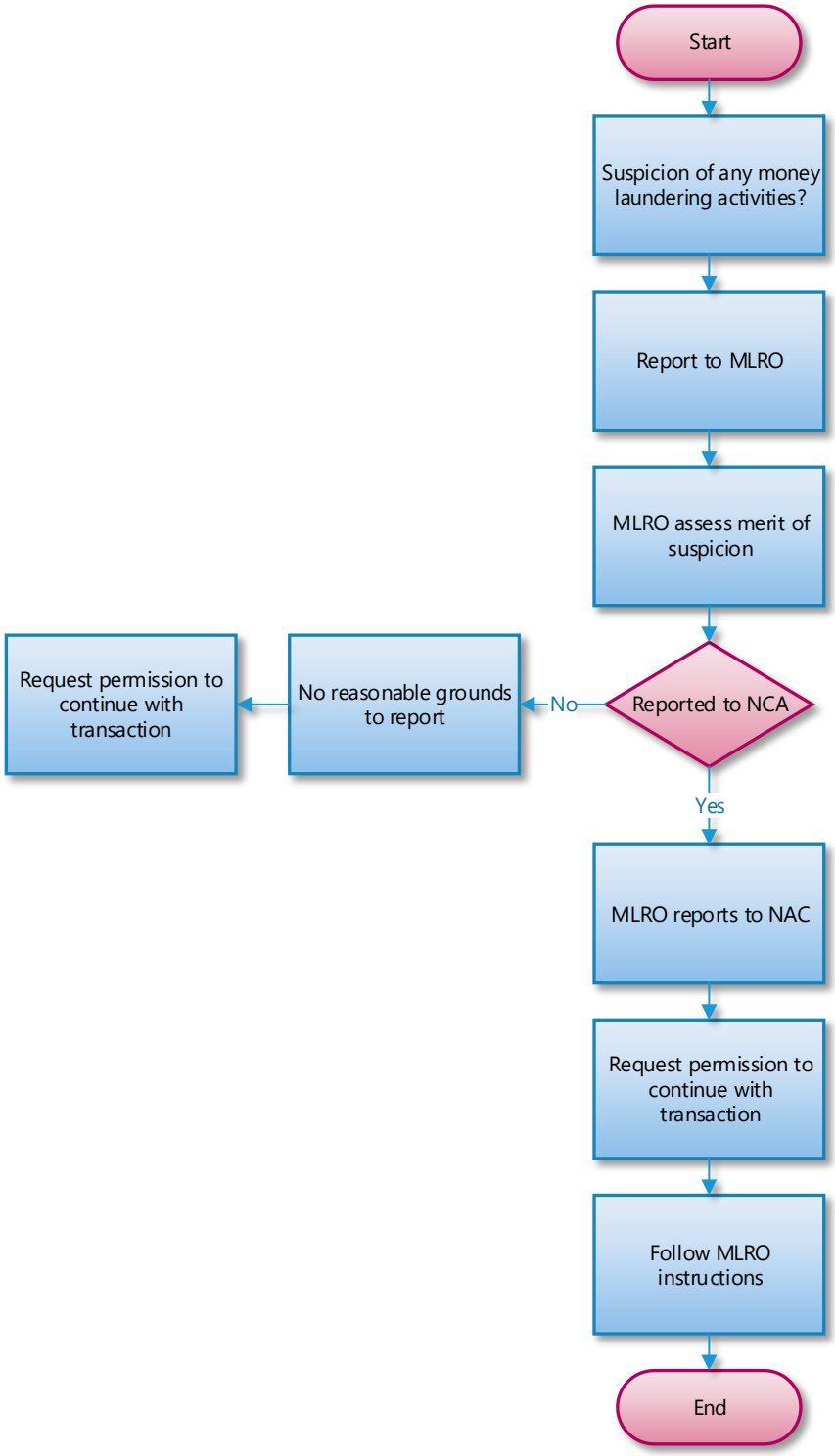
In a case where there is a suspicion of money laundering activity that is either taking place or has taken place, it is essential that you report this to the MLRO as soon as possible in writing as the preferred method, however a discussion can be had is required.

The report MUST include the following:

- Full details of the background
- Full details of the people involved which may include yourself if you believe you may have been involved: full name, DOB, address, company name, position, phone numbers, nationality, etc
- Full details of the nature of their involvement
- Type of money laundering activity involved
- Dates of activities as well as if any transactions have taken place, are going to take place or are imminent
- Where they took place
- How they were undertaken
- Details of the amount of money or assets involved

Providing as must information to the MLRO enables the MLRO to make an inform decision on whether there is a reasonable ground for suspicion and to prepare a report for submission to the National Crime Agency (NCA).

Under no circumstance should you voice your suspicion or any details to the person(s) suspected of the money laundering activities, otherwise you may be committing a criminal offence of 'Tipping Off'.


Start
Suspicion of any money laundering activities?
Report to MLRO
MLRO assess merit of suspicion
Reported to NCA
No
No reasonable grounds to report
Request permission to continue with transaction
Yes
MLRO reports to NAC
Request permission to continue with transaction
Follow MLRO instructions
End

Money Laundering Reporting Officers (MLRO) Responsibilities

When a report of money laundering has been submitted to the MLRO, they will carry out the following:

- Record the receipt of the report and acknowledge it.
- Assess the information submitted and advice the person concerned when a report can be expected
- Consider the report, make all necessary enquires and then decide whether to submit your findings to the National Crimes Agency (NCA). The following should be considered:
  - Is there criminal property?
  - Which offense is involved?
  - Is there a defence?
  - Whether to report and stop acting
  - Whether to acquire consent and keep acting
- Report the suspicious activity or transaction to the NAC by completing the Suspicious Activity Report (SAR)
- Where the MLRO suspects money laundering but has a reasonable excuse for nondisclosure or concludes there's no reasonable grounds to suspect money laundering, then they must note this in the report accordingly.
- Request consent from NAC for any transactions that have been reported and to make sure that no transactions are continued illegally

In addition to the above the MLRO should also

- Making external reports
- Be able to act on their own authority
- Have adequate resources allocated to anti-money laundering
- Oversee the organisations anti-money laundering systems and controls
- MLRO's annual reporting
- Ensure all employees are trained on money laundering and what to do if they suspect any fraudulent activities.
- Record keeping which must be kept for 5 years

All ABS IT Services employees are expected to comply with the anti-money laundering and anti-bribery procedures set out in this handbook. Any breach to these policies will be a dismissible offence and may also be a criminal offence which is subject to fines and imprisonment.

The Criminal Finances Act 2017

It is a criminal offence for companies, other corporate bodies and partnerships established under UK law or of other countries to fail in preventing a person, whether that's an employee, agent, adviser, intermediary, contractor or service providers in criminally facilitating tax evasion. If a person criminally facilitates the evasion of tax whilst acting for the relevant body, that body will be liable, unless proven reasonable prevention procedures were in place.

ABS IT Services policy on anti-facilitation of tax evasion is in line with the company statements, goals and objectives to conduct all our business transactions and communications in an honest and ethical manner by all persons or organisations who are acting on ABS IT services behalf.

Any form of tax evasion will not be tolerated by ABS IT Services and will be deemed as a dismissible offense. Employees or any associated organisation must not undertake any transactions or communication which causes ABS IT Services to commit a tax evasion offense or facilitates tax evasion offenses by 3rd party organisations/ associates.

The following will not be tolerated:

- Participation in any form of facilitating UK tax evasion or foreign tax evasion
- Aiding, abetting, counselling or receiving commission from a tax evasion offence
- Failure to report any requests or demands from any 3rd party person or organisation to facilitate fraudulent tax evasion by others
- Threaten or seek revenge against anyone who refuses to commit an offense or who has reported their concerns

Prevention

Within ABS IT Services there are very few opportunities for tax evasion, nevertheless our best line of defence against tax evasion or the facilitation of tax evasion are the employees as well as applying common sense e.g.

- Is business being conducted as normal between a person and the 3rd party organisation?
- Is the behaviour of the person or client or 3rd party organisation unusual?
- Are there are strange transactions being made or payments methods employed?

These can be indicators that something may not be as it seems.

Report any suspicions to the Head of HR or the Managing Director immediately.

The following 6 steps are in place to prevent any form of tax evasion:

Step 1: Risk Assessment

ABS IT Services will assess the nature and extent of its exposure to the risk from those who act for or on behalf of ABS IT Services engaging in activity to criminally facilitate tax evasion.

The risk assessment method is through vigilance, common sense and information gathering:

- Identify Risk Areas: ABS IT Services has very low risk of any Anti Money Laundering (AML) activities due to the nature of its business and size of the organisation. However, as a responsible organisation ABS IT Services will assess the following 3 elements within the scope of but not limited to employees, agents, advisers, intermediaries, contractors or service providers:
  - What is the nature of the work undertaken?
  - What is the overseas involvement?
  - Who are the clients?
- Opportunity: ABS IT services will consider if there are any opportunity for facilitating tax evasion by assessing the following:
  - How and when could employees, customers, suppliers or stakeholders have the opportunity to facilitate tax evasion?
    - ♦ This risk is very low due to security of buildings, sensitive rooms such as HR and accounting rooms where all records are kept and restricted access to software and systems. ABS IT Services also have CCTV in all its buildings and carries out BPSS checks on all its employees and SC checks for all employees that have access to sensitive customer or supplier data.
  - Is their work monitored?
    - ♦ All technical work is monitored thought management tools and all administrative work is accessed and signed off by a secondary person.
  - Is there a 4 eyes review policy?
    - ♦ ABS IT Services takes particular care with accounting records and each transaction is signed off by either the Managing Director or Head of HR as a security measure and tracking the

accounting department. With the technical teams, they work in 2 or more groups and each one is expected to know what each team member is doing.

- How likely is it that they will be caught?
  - ABS IT Services believes that all our employees, customers, suppliers and stakeholders understand that there is a high chance of any wrongdoing to be picked up and dealt with appropriately.
- How likely do they think they will be caught?
  - High as everyone understands that systems in place and why.
- How effective are the policies and procedures in deterring staff and associates?
  - ABS IT Services advocates its moral standing in the company handbook, various security and GDPR documents, meetings and discussions and iterates its intolerance of any such conduct that would bring ABS IT Services into disrepute.

- Motive: ABS IT Services understands the power of motive and the impact it can have on employees, customers, suppliers or stakeholders, which is why we have many policies to avoid temptation and have frequent company discussions on safety, awareness and repercussion's if policies are breached.
- Means: ABS IT Services has put in place policies and procedures to the best of its ability to prevent any scenarios where any employee can facilitate tax evasion by good and up-to-date record keeping, employing the 4 eye approach, second person signing off transactions other than the accountant, ensuring that all customers, suppliers and stakeholders understand our stance on bribery and AML standards ABS IT Services holds, thereby preventing any contact or communications of any such nature.

Step 2: Proportionality of Risk-Based Prevention Procedures

ABS IT Services has in place reasonable procedures that are proportionate to the risk associated with it committing tax evasion facilitation offences based on the nature, scale and complexity of its business.

Step 3: Top Level Commitment

At ABS IT Services the directors are the drivers behind anti-bribery and anti-money laundering directives and have strong views and moral standing which are communicated frequently to all and are committed to preventing any such misconducts from occurring within the organisation.

Step 4: Due Diligence

As part of ABS IT Services due diligence process the following will be carried out:

1. Evaluate: Check for any potential problems with prospective clients by obtaining documents that identifies the individual, the business and or the beneficial owner and location information:
   a. Full name of individual and or beneficial owner
   b. Official photo ID documents such as passport or driving licence
   c. Residential address by submission of bank statement, utility bills or telephone bill
   d. Business name and trading name
   e. Business registered address by submission of bank statement, utility bills or telephone bill
   f. Business details such as Type, incorporation date, company registration number, VAT number
   g. Confirmation of beneficial owner
   h. Purpose of business relationship
   i. Verify if client is included in any Politically Exposed Person (PEP) list, sanctions and other watchlists
   j. Detailed anti-money laundering policies and procedures

2. Vetting: Use of third-party providers to help perform due diligence such as banks, lawyers or auditors, however it remains ABS IT Services liability. In acknowledgement of this, ABS IT Services will take great care in selecting a trusted third-party provider.
3. Storage: The importance of securing the collected data is well understand by ABS IT Services and will be stored accordingly to the GDPR policies.
4. Gauge: It some circumstances there may be a need to conduct Enhanced Due Diligence, it is the responsibility of ABS IT Services to decide if this is necessary based on the following factors:
    a. Is the client on Politically Exposed Person (PEP) list, sanctions and other watchlists?
    b. High risk location of the person
    c. Occupation of the person
    d. Type of transactions
    e. Expected pattern of activity in terms of transaction types, value and frequency
    f. Expected method of payment
5. Records: Store all records for each customer in a digital form and be ready to provide the data if requested by the regulators.

Step 5: Communication and Training

All employees of ABS IT Services receive communication or training on the prevention policies and procedures set out above to reinforce their understanding.

The zero-tolerance approach on UK tax evasion and foreign tax evasion will be communicated to all clients, suppliers, contractors and stakeholders at the start of the business relationship.

Step 6: Monitoring and Reviewing

As part of the continued improvement process, ABS IT Services will monitor and review its prevention policies and procedures where necessary.

The Terrorism Act 2000

(as amended by the Anti-Terrorism, Crime and Security Act 2001, the Terrorism Act 2006 and the Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007)

The terrorist Act 2000 is a permanent anti-terrorism legislation that aims to combat a real global issue with terrorism and its financing. Although the name 'The Terrorism Act' suggests more terror related acts being legislated, the aim is actually to prevent the financing of terrorism and make people more vigilant about where the money goes once transferred, increasing awareness in the regulated sector and empowering employees to raise suspicion if they suspect wrongdoing.