ABM Global Compliance

Financial
Service
Regulatory Advisor

Web Training Course on
Anti Money Laundering & Combact Terrorist Financing

www.abmglobalcompliance.com

Content:

- Chapter 1: Introduction to Money laundering and Money Service Bus
  a) What is Money Laundering
  b) Stages of Money laundering
  c) Terrorist Financing
- Chapter 2: Legislations
  a) International Bodies for Legislations
  b) Local Legislations within the UK
  c) Sanctions
  d) Political Exposed Persons
- Chapter 3: Customer Due Diligence and Enhanced Due Diligence
  a) What is CDD
  b) What is SDD
  c) What is EDD
  d) Application of SDD and EDD
  e) Beneficial Ownership

ABM Global Compliance

Content:

- Chapter 4: Risk Based Approach
  a) Types of Risk
  b) Senior Management
  c) Legal Consequences
  d) Record Keeping
- Chapter 5: SAR and Regulatory Reporting
  a) What is SAR
  b) Procedures for making a report to the Nominated Officer
  c) Reporting And Notifications

ABM Global Compliance

Chapter 1: Introduction to Money laundering and Money Service Business

What is Money Laundering:

- Money laundering is generally defined as:
  - How criminals change money and other assets into clean money or assets that have no obvious link to their criminal origins.
  - 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.

- Most of the People when they are asked about What is Money laundering, they reply to it as
  - Conversion of Black Money in to White Money.
  - Converting Illegal money to Legal Money.
  - Laundering of dirty money.
  - Disguising the True origin of Money.

- The Main Aim of Money Launder is to enjoy the benefits of their Crimes, its important for Staff to Understand the Objective of Money Launderers. That can be:
  - Disguising the Proceeds of Crime.
  - Disguising the Ownership.
  - Disguising the Controls.

- How does Money Laundering takes place?
  - It may take in Various forms.
  - It can be in form of Cash, but it might be possible its deposited into Bank Account so that nature of funds can be change as funds in Bank but they are all proceeds of crime.
  - It can also be in form of Antiques, High Value Stones, Paintings, Expensive Cars, as well as Real Estate.

ABM Global Compliance

Chapter 1: Introduction to Money laundering and Money Service Business

Stages of Money laundering:

1) Placement: Cash generated from criminal activities like Drugs, Organized Crimes, Illegal Gambling, Prostitutions Most of these funds are in form of cash, Carrying a Cash or Holding it is Difficult as well as easily linked back to criminal Activities so they try to introduce this cash in to Financial System as soon as Possible. It is either converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions.

2) Splitting of Deposits: Launderers sometimes break the large amount of cash into Financial system by breaking it into small transactions and deposit it into multiple accounts belonging to different individual at different days, may be in different branches/different Banks or by corrupting the Bank Staff, it is also called Splitting or Smurfing or Structured Deposits after that all these funds are deposited into one bank account and consolidated there.

3) Mixing of Funds: Another Method used is mixing the illegal funds with legal cash business, generally by corrupting the Legal Cash Business and presenting the illegal cash as Part of Genuine Cash Business Income. Or Sometime setting up the similar genuine cash Business and using that to Launder the Illegal Funds.

4) Placing Funds with Money Service Business: Money Service Businesses are at risk of being used for Money laundering. If MSB have weak Controls/CDD Procedures then its possible that criminals might misuse their service to Launder the funds, it can also be done by Corrupting the Business Staff or by offering them the part of the proceeds of crime to facilitate the transportation or transferring of Funds.

ABM Global Compliance

Chapter 1: Introduction to Money laundering and Money Service Business

Stages of Money laundering:

5) Buying of Asset: Another Method of Placing funds is Asset Purchase mainly in Real Estate, Property and Motor Cars.

6) Layering: Once funds are Successfully placed in Financial System, Launderer do the multiple layers of Transactions to disguise and damage the source of property, the process can be from small transactions to complex one and the purpose is to make sure that any investigation or any funds source can be disguised, in terms of MSB, Transfer of funds from one country to another also falls in the Layering stage as funds are relatively out of the control of local Investigation Agencies. Layering also include making layers of transactions in the form of buying, selling of property, buying of another property thus making the audit trail difficult to trace.

7) Integration Stage: The last stage of Money Laundering in which the funds previously placed and layered are reintroduced into the economy as Clean money, although these funds appear to be the clean money but in actual they are proceeds of Crime. Funds that were laundered out side of Jurisdiction are brought back into home country as Foreign Remittance, Inheritance, profits, Loan or in lieu of services or cashing back of illegal funds invested in some sham scheme.

Scenarios where all three stages are not followed:

Their might also be the situation where there is no need for funds to be placed in Financial System, funds are already in Financial System, that may be in the case of Insider dealing when Mr.X obtain the Secret information about Company Alpha and he sell his stake before the news go public and hit the share price so all his proceeds he made by this piece of news are Proceeds of Crime laying in his Bank Account.

Chapter 1: Introduction to Money laundering and Money Service Business

Terrorist Financing:

Previously Proceeds of crime were the biggest source of Concern but during the last 2 decades the Terrorist Financing is one of the Biggest threats to Financial services.

Terrorist financing involves dealing with money or property that you've reasonable cause to suspect may be used for terrorism. The funds and property may be from legitimate sources or criminal sources. They may be in small amounts.

The Terrorism Act sets out the primary offences relating to terrorist funding. Regulated businesses like money service businesses must report a belief or suspicion of offences related to terrorist financing, such as:

- Fund-raising for the purposes of terrorism.
- Using or possessing money for the purposes of terrorism.
- Involvement in funding arrangements.
- Money laundering -facilitating the retention or control of money, which is destined for, or is the proceeds of terrorism.

Both Money Laundering and Terrorist Financing have certain features in Common like:

- The future use of funds is for Criminal Purpose.
- Disguise of source and use of funds in both cases.
- It might be possible that funds were obtained from legal source but their use may be for Terrorist Financing.

ABM Global Compliance

Chapter 2: Legislations

During the present time the ML and TF have been the global problem so all the nations of the world have setup some standard collectively to fight against these Situations/

We have International Bodies like:

- FATF (Financial Action Task Force)
- UNODC(United nation Office of Drugs and Crime)
- EU Commission (Issuing Directive since 1991-Current AML 5th Directive introduced in December 2019(AML 5th Directive)

Local Legislation with in the UK include:

- Money Laundering and Terrorist Financing (Amendment) Regulations2019 (The statutory instrument updates the UK's existing anti-money laundering legislation to take into account the Fifth Directive)
- Criminal Finances Act 2017
- The Terrorism Act 2000
- The Proceeds of Crime Act 2002
- Terrorist Asset-Freezing Act 2010
- Anti-terrorism, Crime and Security Act 2001
- Counter-terrorism Act 2008, Schedule 7

ABM Global Compliance

Chapter 2: Legislations

The Proceeds of Crime Act 2002:

POCA criminalises all forms of money laundering and creates other offences such as failing to report a suspicion of money laundering and ‘tipping off’*. The Proceeds of Crime Act 2002 requires you to submit a Suspicious Activity Report to the National Crime Agency if you know or suspect that a person is engaged in, or attempting, money laundering.

It is important not to inform a client where the details of a transaction have been reported to the National Crime Agency (NCA) or where a transaction may have to be delayed for the reason of waiting for consent. If you decide to end your working relationship with a client, then always ensure that you send them a Letter of Dis-engagement and be careful not to “tip off” if you are terminating the relationship for reasons that you feel it is not appropriate to work for them due to activities that you may suspect they are involved in. Always ensure that the reason you give cannot be construed as “tipping off”.

ABM Global Compliance

Chapter 2: Legislations

Terrorist Asset-Freezing Act 2010:

The Terrorist Asset-Freezing etc. Act 2010 gives HM Treasury power to freeze the assets of individuals and groups reasonably believed to be involved in terrorism, whether in UK or abroad, and to deprive them of access to financial resources.

The Terrorism Act 2000:

The Terrorism Act sets out the primary offences relating to terrorist funding. Regulated businesses like money service businesses must report a belief or suspicion of offences related to terrorist financing, such as:

- Fund-raising for the purposes of terrorism.
- Using or possessing money for the purposes of terrorism.
- Involvement in funding arrangements.
- Money laundering -facilitating the retention or control of money, which is destined for, or is the proceeds of, terrorism.

ABM Global Compliance

Chapter 2: Legislations

Counter-Terrorism Act 2008, Schedule 7:

The Treasury has powers under Schedule 7 to the Counter-Terrorism Act 2008 to require financial firms to takes specified actions in relation to a country of concern, or counter parties based in that country. Use of this power can be triggered if the risk of money laundering or terrorist financing activities is identified in a country.

Criminal Finances Act 2017:

The Criminal Finances Act 2017 make important amendments to the Proceeds of Crime Act, the Terrorism Act and the Anti-terrorism Crime and Security Act to expand the provisions for confiscating funds to deal with terrorist property and proceeds of tax evasion.

ABM Global Compliance

Chapter 2: Legislations

Sanctions:

The Restrictions put by international bodies on certain countries, individuals and Terrorist organizations, Human Smugglers to force them to change their behavior where diplomatically its not possible are called Sanctions. The sanctions can be in the form of trade barrier, travel restrictions, financial limitations like trade etc.

Sanctions may be issued against:

- Countries/jurisdictions (for example, US sanctions against Iran and Russia).
- Terrorist Organizations.
- Corrupt individuals (for example, especially designated nationals ‘SDNs’).
- Specific industry like Irani oil.
- Financial Institutions etc.

Main bodies that can impose Sanctions include:

- United Nations
- European Union
- United States Department of Treasury OFAC list
- UK FCO
- JMLSG
- OFAC
- UN
- HMT

ABM Global Compliance

Chapter 2: Legislations

Sanctions:

There are certain countries that have been under sanction list for some time like:

- Iran
- North Korea

Other countries that fall under sanction lists at certain times are:

- Libya
- Sudan
- Syria
- Myanmar

But the list is not final and it vary time to time.

All these bodies that put sanctions update the list Time to Time and most of the Money Service Software in the Market are integrated with these lists, and get updated whenever new list is available.

All individuals and legal entities who are with in or undertake activities with in the UK's territory must comply with the EU and UK financial sanctions that are in force. Most financial sanctions are made through EU law which has direct effect under UK law.

The Office of Financial Sanctions Implementation works closely with the EU Commission and other member states in implementing sanctions. Other financial sanctions are put in place by UK laws.

You should report any transactions carried out for persons subject to sanctions or if they try to use your services. You can report a suspected breach, sign up for free email alerts and obtain Information on the current consolidated list of asset freeze targets and persons subject to restrictive measures at:

https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation

ABM Global Compliance

Chapter 2: Legislations

Political Exposed Persons:

A politically exposed person is typically persons that are entrusted with prominent public functions, HELD IN THE UK or abroad:

- Heads of state, heads of government ,ministers and deputy or assistant ministers.
- Members of parliament or similar bodies.
- Members of the governing bodies of political parties.
- Members of supreme and constitutional courts and other high level judicial bodies.
- Members of courts of auditors or boards of central banks.
- Ambassadors, and high ranking officers in the armed forces.
- Members of the administrative, management or supervisory bodies of state owned enterprises.
- Directors ,deputy directors and member of the board, or equivalent of an international organization.

The definition includes family members such as spouse, partners, children (of the person and their spouse or partner) and parents and known close associates. Close associates are persons who have:

- Joint legal ownership ,with a politically exposed person of a legal entity or arrangement.
- Any other close business relationship with a politically exposed person.
- Sole beneficial ownership of a legal entity or arrangement setup for the benefit of a politically exposed person.

ABM Global Compliance

Chapter 2: Legislations

Political Exposed Persons:

The danger posed to a financial services business by PEPs is simply that the business may be exposed to property that has been generated by corruption.

The risk posed by PEPs can be reduced if we have a look at :

- Geography.
- Source Of Wealth.
- Source Of Funds.
- Relationship.

The main risk in relations to PEP can be the use of Corruption proceeds in transaction, Transparency International Corruption Index explain the amount and level of corruption in a specific country and it can be used as a base point to trace the funds as well as type of transaction.

ABM Global Compliance

Chapter 3: Customer Due Diligence and Enhanced Due Diligence

What is CDD:

CDD is basically a risk assessment over the Customer as per the recommendations by FATF.

- Identification of Customer.
- Verifying its Identity from reliable, independent source.
- Identification of Beneficial Owner ship.
- Verifying the identification of Beneficial Ownership.
- Obtaining the information on Intended nature and Purpose of Relationship.
- Conducting the ongoing monitoring of Business Relationship.
- Retain records of these checks and update them when there are changes.

Making sure that transactions are in line with the customer information we hold as per the risk profile of the customer

CDD is important in relation to providing the protection against the misuse of our services by any Criminals and its most important factor in strengthening the AML Controls of the company

So its important for Business to Have Risk based Approach in relation to customers and activities and all the CDD procedures should be followed.

You must apply customer due diligence measures:

- When you establish A business relationship.
- When you carry out an 'occasional transaction‘.
- When you suspect money laundering or terrorist financing.
- When you have doubts about A customer's identification information that you obtained previously.

ABM Global Compliance

Chapter 3: Customer Due Diligence and Enhanced Due Diligence

What is CDD:

If the customer doesn't comply with it, don’t:

- Carry out a transaction with or for the customer.
- Establish a business relationship or carry out an occasional transaction with the customer.

What is SDD:

As per the JMLSG, the Simplified Due Diligence should be perform when there is Low risk of AML and TF, if following the internal Risk Assessment, Business consider it risks to be Low then its allow to do the Simplified Due Diligence in relation to these transactions.

For Example:

If transaction falls under the Threshold and identification and verification of customer is already done the SDD is allowed, it will reduce the time of transaction, already established relationship of customer, reduce paperwork and less documents.

ABM Global Compliance

Chapter 3: Customer Due Diligence and Enhanced Due Diligence

What is EDD:

When there is High risk of Money Laundering or TF mainly due to type of clients, Jurisdiction of client, For example, Jurisdiction with weak AML Regulations or Countries Identified by FATF and EU with strategic deficiencies then the requirement is to go beyond the regular CDD and SDD procedures but perform the Enhanced Level of Due diligence.

Presence of Online frauds like Fake Documents provider can create additional Risks so a high degree of checks is required with all the Diligence

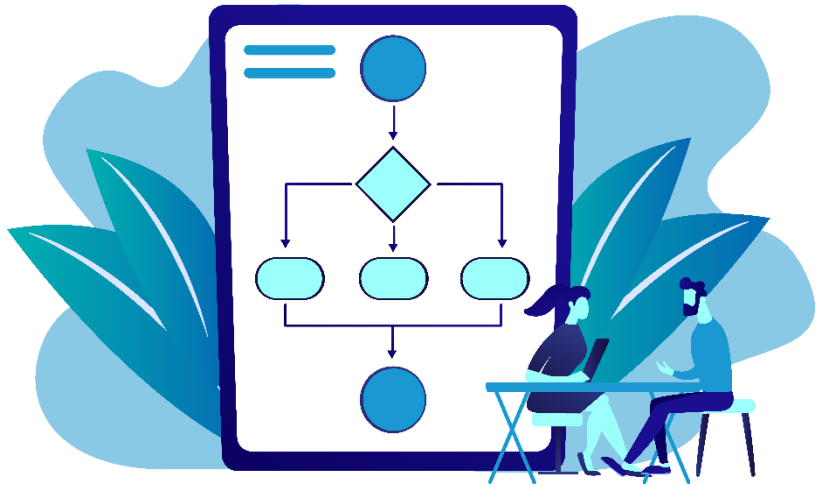
Additional checks may be appropriate for high-risk clients.

As an example, source of wealth descriptions that are not acceptable include: ‘savings’, ‘profits from investments’, ‘inheritance’, ‘business dealing’, ‘sale of business’ as they are insufficient proof that wealth is legitimate and not the product of criminal activity.

In other words it a sort of assurance that wealth is not generated by Criminal Activities.

EDD include in-depth questioning about the type of Funds and source of funds, Collection of supporting documents as well as risk of the transaction.

There is no Fix criteria set out for the EDD, all the procedures should be performed and every transaction should be checked at Individual merits.



ABM Global Compliance

Chapter 3: Customer Due Diligence and Enhanced Due Diligence

What is EDD:

You must have to perform EDD in cases when:

- Identified in your risk assessment that there is a high risk of money laundering or terrorist financing.
- Customer or other party is from a high risk third country identified by the EU.
- Person has given you false or stolen documents to identify themselves (immediately consider reporting this as suspicious activity).
- Customer is a politically exposed person, an immediate family member or a close associate of a politically exposed person.
- Transaction is complex, unusually large or with an unusual pattern and have no apparent legal or economic purpose.

The Risk Based approach states that we have to make decision as per our Risk

If risk is LOW based on the customer, transaction, behavior and all aspects for Example with in the EU Bank Transfer transaction by customer of Small Amount might consider as Low risk and Simplified Due Diligence will be required

On the other end if the customer is remitting to a High-Risk Jurisdiction identified by EU commission and FATF the transaction will fall under the Enhanced Due Diligence Procedures

The CDD and Know your customer help saves the genuine customers to being judged or considered as suspicious

ABM Global Compliance

Chapter 3: Customer Due Diligence and Enhanced Due Diligence

Example for Simplified and EDD Application:

A Customer is a Salary Individual providing the Pay slip to support his Source of Fund and wants to remit funds for family support and wants to remit to EU is falling under Simplified Due Diligence Criteria

On the Other end some one with huge amount of Cash reach a Licensed MSB and trying to send it to a High Risk Jurisdiction will fall under Enhanced Due Diligence.

Ongoing Monitoring of Business relations

HMRC MLR 2019 require the business to perform the Ongoing monitoring of Business relationship with the customer

It includes if there is any change in the Circumstances of the customer

- Customer job is changes
- Customer become PEP
- When customer carry out an 'occasional transaction'
- When business suspect money laundering or terrorist financing
- When business have doubts about a customer's identification information that you obtained previously.

ABM Global Compliance

Chapter 3: Customer Due Diligence and Enhanced Due Diligence

Beneficial Ownership:

As per the 5th Directive another Important areas was the identification of Ultimate Beneficial ownership.

Beneficial Owner is the natural person on whose behalf a transaction or activity is being conducted, or the natural person who exercises ultimate effective control over the management of a legal entity.

The Fourth Directive set out requirements for its members regarding ultimate beneficial ownership (UBO), including that companies must obtain and hold “adequate, accurate and current information” about their beneficial owners.

The Fifth Directive places greater emphasis on transparency around ultimate beneficial ownership as part of a targeted attempt to fight back against financial criminals who hide behind often complex and opaque corporate structures.

To comply with the Fifth Directive, organizations must secure access to reliable, accurate and complete UBO data as well as have the capability to unravel even the most complex corporate structures. This is important in order to identify UBOs to required thresholds before screening them for potential links to financial crime.

Following 5th AMLD- EU Parliament agreed to make a Beneficial Ownership Public Register so that FLUs can access the data and make efforts to curb the Money laundering

ABM Global Compliance

Chapter 3: Customer Due Diligence and Enhanced Due Diligence

Beneficial Ownership:

Acceptable forms of Documents Include:

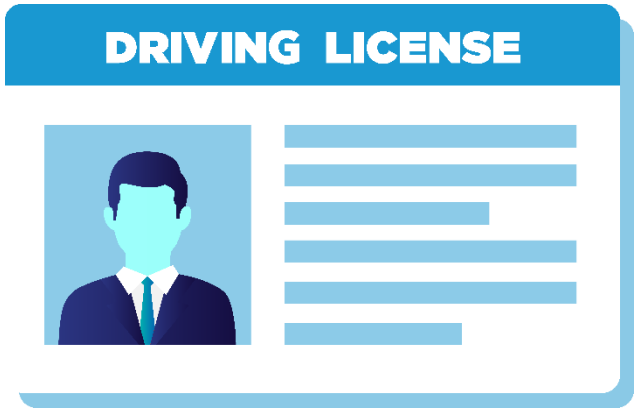
- Basic Information: Sender details: Full Name, current residential address, date of birth, Phone no, Profession; Receivers Details: full name, phone no, Relationship, Purpose of money sending.

- 1st form of ID:

*If only 1 form of ID (UK Full Driving License, Provisional License, Valid UK Visa with work Permit, International Passport with UK Valid Visa, British Passport, Asylum seeker Registration Card).

- 2nd form of ID:

*UK Driving License+ Posted Recent Bank Statement/UK Passport/Utility Bills of Gas/Electricity/Water/Council letter.



Source of Income verification procedures: You can have wages pay slips and last 3 months bank statement and see paid in side carefully. Try to find out how he is getting money and depositing amount of money in bank account and please find the evidence of source of those amounts. Please investigate and find the evidence of the source of paid in amounts. If he does not have any income coming through bank, please find out alternative source of fund and evidence as well. Or, written documents showing the sale of legal asset, his/her pay slips/ Bank Statement that showing the income either salary, Sale of asset that matches or is near to the amount being transferred.

Further information on EDD:

- Purpose of Use of the Fund: Any letter or Documents from firm/shop/lawyer/accountant/asset Buyer indicating the purpose and Use of Fund.
- Guidelines: FCA and HMRC ML Guidelines and Company MLR policy to be followed + Customer Due Diligence with every customer.

ABM Global Compliance

Chapter 4: Risk Based Approach

An Approach used by organization's to assess that Risk Standing of the customer and transaction and then make the decision about the CDD procedures needs to be performed

It enables the Senior Management to make system, controls, and implement the most useful procedures in relation to CDD, EDD as well as ongoing Monitoring of the Compliance areas of customers.

It starts with identification of risks, assessment of risks, then mitigating the risks, monitoring the post risk effects and keeping all the records of the processes

Types of Risks include:

- Customer Risk
- Transaction Risk
- Agent Risks
- Geographical Risks
- Volume of transaction
- Delivery Channel
- New customers
- Transactions
- Inward money transmission from another country into the UK
- Third party payments
- Third party cheque cashing
- Cashing scrap metal dealers’ cheques
- Currency exchanges
- Types of customer
- Risk appetite of Organization

ABM Global Compliance

Chapter 4: Risk Based Approach

Customer Risk

Higher-risk categories of customer will include:

- PEPs
- Customer with Unusual behavior
- Customer doing on someone else behalf
- Customer getting instructions from Someone
- Customer Sending to High Risk Jurisdictions
- Customer non Local

Transaction risk

Higher-risk transactions will include:

- Cash intensive business
- Customer sending to high risk country
- Transaction is of high value
- Transaction does not make economic sense
- Transaction through third party

Other risks like Jurisdiction of weak AML regime are also effective risks and can only be counter by strong monitoring and review process and Senior Management is responsible for the overall review of risk Factors and proper record Keeping is Mandatory.

ABM Global Compliance

Chapter 4: Risk Based Approach

Agent Risk

Payment institutions in the UK are allowed to bring on-board an agent to help them increase the business without the need for opening a separate branch. If you arrange for another business on your behalf they're acting as your agent and you're the principal.

There's a significant risk that criminals will seek to exploit your business for money laundering by becoming your agent. When you take on board an agent you must make sure, you understand who the beneficial owner of the business is, and that they're fit and proper persons with regard to the risk of money laundering.

You should be more careful on appointing agents and managing an agency relationship and must perform agent’s due diligence and risk assessment on each agents.

Risk related to agents:

- Agents conducting unusually high numbers of transactions (particularly with an agent in A geographic area of high risk linked to drugs, corruption or other criminal activity).
- Agents with high/disproportionate transaction values.
- Agents with poor data/CDD collection standards.
- Agents with seasonal business fluctuations not consistent with other agents (which could indicate links to illegal drugs).
- Agents who are established by criminals as A front for criminal activity or recruited by criminals to facilitate the laundering of the proceeds of crime.
- Agents who are not complying with internal policies and procedures related to AML complex ownership models.

ABM Global Compliance

Chapter 4: Risk Based Approach

Senior Management

Senior management means:

- A manager, secretary
- Chief executive
- Member of the committee of management, or a person purporting to act in that capacity
- Any partner in a partnership
- A sole proprietor
- A sole Director
- A nominated officer or a compliance officer

The aim of the Senior Managers and Certification Regime (SM&CR) is to reduce harm to consumers and strengthen market integrity by making individuals more accountable for their conduct and competence.

Roles and Responsibility of Senior Management/MLRO

To Perform the risk assessment for identifying where your business is vulnerable to money laundering and terrorist financing;

Prepare a policy statement and procedures to show how the business will manage the risks of money laundering and terrorist financing identified in risk assessments;

Make sure there are enough trained people equipped to implement the policy adequately, and systems to help them;

monitor effectiveness of the business's policy and controls and make improvements where required.

ABM Global Compliance

Chapter 4: Risk Based Approach

The risk-based approach requires the senior management to identify and assess the money laundering risks and take steps to mitigate and monitor those risks.

- Ensure relevant staff are aware of the risks of money laundering and terrorist financing, the relevant legislation, and their obligations under that legislation, know who the nominated officer is and what their responsibilities are, trained in the firm's procedures and in how to recognize and deal with potential money laundering or terrorist financing transactions (suspicious) or activity
- Ensure staff are trained at regular intervals
- Maintain a written record of what you have done to raise awareness of the law and the training given to staff

As per Regulation 42 of Money Laundering Regulations 2019 gives HMRC the power to impose civil penalties on businesses that fail to comply with the requirements of the regulations in respect of:

- Appointing a Nominated Officer and internal reporting procedures
- Customer due diligence measures
- On-going monitoring of a business relationship
- Enhanced customer due diligence and
- Risk Assessment (Policies and procedures to prevent money laundering and terrorist financing)
- Training of employees.
- Record keeping
- Notification and registration requirements
- On-going monitoring

ABM Global Compliance

Chapter 4: Risk Based Approach

Legal Consequences:

Beneficial Owners, Officers and Managers must make sure the business is meeting its responsibilities and following the MLRs. If this is you, you will be guilty of committing a crime if you do not follow the MLRs. You may incur an unlimited fine and/or a prison term of up to two years.

You may also be committing offences under the Proceeds of Crime Act 2002 & the Terrorism Act 2000.

Staff Training

As per MLR2019, Staff Training is mandatory.

MLR ensure that staff and agents receive appropriate levels of training and awareness, relevant to their roles. The management should ensure that all relevant central staff receive AML training, with more specialized training provided to senior management and key control staff, e.g. agent trainers, audit staff and AML teams.

The AML training programmed should ensure that agents receive training before commencing business and that there is regular refresher training. Staff and agents should be tested to ensure that their competence is maintained, and records and management information must be retained.

ABM Global Compliance

Chapter 4: Risk Based Approach

Record Keeping:

The risk-based approach requires a robust audit trail documenting risk assessment, control measures implemented and the management information produced from monitoring. Effective record keeping will provide assurance to regulators and equip senior management with a powerful management tool

Core obligations:

- Copies of the evidence obtained of a customer's identity for 5 (five) years after the end of the business relationship
- Details of customer transactions for five years from the date of the transaction
- Details of actions taken in respect of internal and external suspicion reports
- Details of information considered by the nominated officer in respect of an internal report, where the nominated officer does not make a suspicious activity report
- Copies of the evidence obtained if you are relied on by another person to carry out customer due diligence, for five years from the date of the agreement, the agreement should be in writing

You must also maintain:

- A written record of your risk assessment.
- A written record of your policies, controls and procedure.

ABM Global Compliance

Chapter 4: Risk Based Approach

Record Keeping:

You must keep records of customer due diligence checks and business transactions:

- For 5 years after the end of the business relationship.
- For 5 years from the date an occasional transaction was completed.
- You should also keep supporting records for 5 years from the date of transaction.
- You should keep records from closed branches or agents.
- The records should be reviewed periodically to ensure, for example, that a fresh copy of expired documents is held.

ABM Global Compliance

Chapter 5: SAR and Regulatory Reporting

What is SAR:

A SAR is a Suspicious Activity Report, a piece of information which alerts law enforcement that certain client/customer activity is in some way suspicious and

- might indicate money laundering or terrorist financing.
- You must make a report as soon as possible after you know of or suspect that money laundering or terrorist financing is happening.
- nominated officer can send a SAR to the NCA. It's easiest to send the report online.
- The NCA website explains how to send a report.

If you need help with a report you can contact the NCA. The National Crime Agency has a secure, encrypted system for submitting reports called ' SAR Online'

Reporting Suspicious Activity:

- The duty to report suspicious activity, including possible terrorist financing activity, rests with every employee within the financial sector,
- The level of evidence required to form a suspicion is relatively low. Any possible suspicious activity must be reported as set out in your own organization's policy and procedure on reporting.

Common examples of suspicious activity may include:

- A transaction that is unusually large given what we know about the client
- An activity or type of transaction that is out of line with that normally seen on the client's account
- An inconsistency or discrepancies in the CDD provided

ABM Global Compliance

Chapter 5: SAR and Regulatory Reporting

The suspicious activity reporting (SAR) process:

All SAR's should be made in writing as this provides the employee with statutory protection, particularly if the MLRO/nominated officer subsequently decides not to report the suspicion to the authorities.

Client Confidentiality is very Important in relation to that. All SAR's should be made in writing as this provides the employee with statutory protection, particularly if the MLRO/nominated officer subsequently decides not to report the suspicion to the authorities under the POCA 2002 the reason for not reporting should be noted.

Tipping off:

Offences in relation to Tipping off include:

- Any person has made a report under the proceeds of crime act 2002 to the police, HM revenue and customs or the NCA concerning money laundering, where that disclosure is likely to prejudice any investigation into the report; or
- An investigation into allegations that an offence of money laundering has been committed, is being contemplated or is being carried out.

See section 333A of the Proceeds of Crime Act 2002. A similar offence exists in relation to terrorism (including terrorism financing) by virtue of section 21D of the Terrorism Act 2000.

- There are many reasons why you or one of your employees might become suspicious about a transaction or activity. Often it's just because it's something unusual for your business - perhaps a customer has tried to make an exceptionally large cash payment.
- Maybe the customer behaved strangely, or made unusual requests that did not seem to make sense. Perhaps the transaction they wanted to make just did not add up commercially. You must look carefully at all unusual transactions to see if there's anything suspicious about them

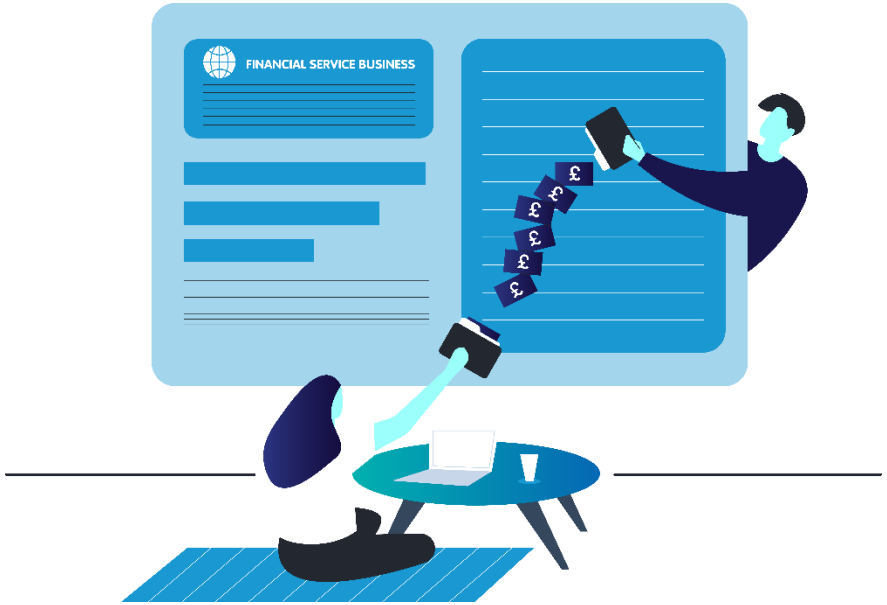
ABM Global Compliance

Chapter 5: SAR and Regulatory Reporting

Procedures for making a report to the Nominated Officer:

You / staff must carry out the following:

- Staff must raise an internal report where they know or suspect, or have reason to believe, that another person is engaged in money laundering, or that terrorist property exists
- The business's nominated officer must consider all internal reports - the officer must make a report to the national crime agency as soon as it's feasible to do so, even if no transaction takes place, if the officer considers that there's knowledge, suspicion, or reasonable belief that another person is engaged in money laundering, or financing terrorism
- The business must seek consent from the national crime agency before proceeding with a suspicious transaction or entering into arrangements if it's to provide itself with a defense to a charge of money laundering.
- It's a criminal offence for anyone to do or say anything that 'tips off' another person that a disclosure has been made where the tip-off is likely to prejudice any investigation that might take place



Staff and Tipping off:

- Tipping off does, however, become a very real danger once a SAR is made to law enforcement, after which all communications between a financial service business, its employees and suspected clients must be handled with care. All employees should look for guidance from either the MLRO or from management on how to deal with suspected clients.

Legal Consequences:

- Conviction for this offence can incur up to 5 years' imprisonment and or/an unlimited fine.

ABM Global Compliance

Chapter 5: SAR and Regulatory Reporting

Receiving a decision from NCA - Get consent for a transaction:

- You must consider whether you need a defense against money laundering
- Charges from the NCA before you can proceed with suspicious transaction or activity.
- You'll find out if the NCA have granted a defense when they reply to your SAR.
- If you do not get a reply from the NCA within 7 working days and think you've correctly reported the activity, you can choose to assume a defense is granted.
- If you get a reply that says you do not have permission to proceed, the NCA have a further 31 calendar days to take action.
- If you've not heard from the NCA after the 31 days, you can proceed if you want to. You will not be committing an offence.
- The 31 day period does not apply to terrorist financing cases, you will not have a defense until the NCA grants your request.

Reporting And Notifications:

- All the payment Institutions have to setup the Regulatory reporting with FCA.
- Late reporting are fined 250GBP.
- Reg data is the platform that is replacing the Gabriel and all the reports will be made at that.

Below are some of the Types of Report:

- Authorized Payment Institution Capital Adequacy Return.
- Payment Services Directive Transactions.
- EMI and SEMI Annual Return.
- Total outstanding e-money at 31 Dec.
- Average outstanding e-money.
- Payment services and electronic money complaints report.
- Half-yearly Payments Fraud Report.
- Quarterly Operational and Security Risk Report.
- Annual controllers report and annual close links report.
- Annual financial crime report.

ABM Global Compliance

ABM Global Compliance | Financial Service Regulatory Advisor

Thank You