Original Article

Statutory obligations for banks to comply with the anti-money laundering legislation in Malaysia: Lessons from the United Kingdom

Norhashimah Mohd Yasin

is a professor of law in the Department of Civil Law at the International Islamic University Malaysia (IIUM). Her areas of expertise are comparative banking law and the legal aspects of money laundering and terrorism financing. She has conducted numerous training courses in both areas of law to banks as well as regulatory and enforcement bodies. She has an LLM and PhD from Warwick University, England. She is also an Advocate and Solicitor in the High Court in Malaya.

Correspondence: Norhashimah Mohd. Yasin, Ahmad Ibrahim Kulliyyah of Laws, International Islamic University Malaysia, P.O. Box 10, Kuala Lumpur 50728, Malaysia
E-mail: norhashimah@iium.edu.my

ABSTRACT As a result of the existence of the 'Forty Recommendations', all countries are expected to have anti-money laundering and anti-terrorism financing legislation and regulations. Because most national legislation came into being due to the existence of the Recommendations, the laws of all countries ought to be *in pari materia* with each other. To illustrate this fact, this article will compare United Kingdom and Malaysia legislation and regulation and how they match each other. The focus is on banks because although money launderers use many methods to clean their dirty money, the banking system is still a popular way to launder money. The article will look at Part 4 of the Malaysian Anti-Money Laundering and Anti-Terrorism Financing Act 2001 (AMLATFA) and its UK equivalent. It can be seen that despite banks being subject to regulation for at least 20 years, banks in countries such as the United Kingdom are still being given huge fines for not having adequate anti-money laundering procedures.

Journal of Banking Regulation (2015) **16,** 326–344. doi:10.1057/jbr.2014.21; published online 5 November 2014

Keywords: banks; money laundering; legislation; guidelines; regulation

INTRODUCTION

As a result of the existence of the 40 Recommendations issued by the Financial Action Task Force, and supported by the United Nations, all UN member countries have to have some kind of anti-money laundering and counter terrorism financing legislation (AML/CFT) in place to avoid being blacklisted as Non-Cooperative Countries and Territories (NCCT). Currently, no country falls under the NCCT, which can lead to all sorts of risks that include reputational risk as well as a financial embargo that might be enforced by the major powers. However, some countries are listed as having specific AML/CFT problems that still need to be resolved: Iran, North Korea, Bolivia, Cuba, Equador, Ethiopia, Ghana, Indonesia, Kenya, Myanmar, Nigeria, Pakistan, Sao Tome and Principe, Sri Lanka, Syria, Tanzania, Thailand, Turkey, Vietnam and Yemen.[1]

There is another list of countries that have been deemed to be improving their AML/CFT legislation and processes, but are proceeding too slowly: Afghanistan, Albania, Algeria, Angola, Antigua, Argentina, Bangladesh, Brunei, Cambodia, Kuwait, Kyrgyzstan, Mongolia, Morocco, Namibia, Nepal,

Nicaragua, Philippines, Sudan, Tajikistan, Trinidad and Tobago, Venezuela and Zimbabwe.[2] There is one country, Turkmenistan, that is now off the list as their AML/CFT is at an acceptable standard.

This article is intended to illustrate the *pari materia* aspect of money laundering and terrorism financing legislation, and accompanying regulations and guidelines, by examining the regulation of banks in Malaysia and the United Kingdom.

The basic money-laundering legislation in Malaysia is the Anti-Money Laundering and Anti-Terrorism Financing Act 2001 (AMLATFA).[3] Part 4 of the Act is directed at 'Reporting Institutions', which include 34 types of institutions that fall under the following legislation:

1. Banking and Financial Institutions Act 1989 (BAFIA)[4]
2. Islamic Banking Act 1983[5]
3. Insurance Act 1996[4]
4. Takaful Act 1998[5]
5. Security Industry Act 1983[6]
6. Money Changers Act 1998[7]
7. Future Industries Act 1993[6]
8. Development Financial Institutions Act 2002
9. Tabung Haji Act 1995
10. Postal Services Act 1991
11. Common Gaming Houses Act 1953
12. Payment System Act 2003
13. Accountants Act 1967
14. Legal Profession Act 1976
15. Advocates Ordinance Sabah 1953
16. Advocates Ordinance Sarawak 1953
17. Section 139A of Companies Act 1965 (Company Secretaries)
18. Pool Betting Act 1967
19. Racing (Totalizer Board) Act 1961
20. Racing Club (Public Sweepstakes) Act 1965
21. Notories Public Act 1959
22. Trust Companies Act 1949
23. Public Trust Corporation Act 1995
24. Moneylenders Act 1951
25. Pawnbrokers Act 1972
26. Valuers, Appraisals and Estate Agents Act 1981
27. Securities Commission Act 1993
28. Exchange Control Act 1953
29. The Moneylenders Ordinance Sabah
30. The Money Lenders Ordinance Sarawak
31. Companies Act 1965 (dealers in precious metals and precious stones)
32. Registration of Business Act 1956 (dealers in precious metals and precious stones)
33. Exchange Control Act 1953
34. Money Changing Act 1998
35. Labuan Offshore Financial Services Act 1996 (this covers offshore financial services)
36. Labuan Offshore Security Industry Act 1998 (listing, sponsor and trading agent)

This article will therefore concentrate on the sections of Part 4. Part 4 only gives a general framework for banks and other institutions to follow, as such, detailed instructions are given in Guidelines issued by the Malaysian Central Bank pursuant to AMLATFA.

Of all 'Reporting Institutions', Malaysian banks[8] should have the most experience in the area of anti-money laundering procedures as they have operated under various money-laundering guidance for nearly 20 years. All banks, the world over, are covered by anti-money laundering laws, regulations and rules resulting from international agreements such as the Financial Action Task Force's 40 Recommendations.[9] British banks[10] are no exception. Unlike some countries, in Britain the criminal aspects of money laundering and terrorism financing are separate from the regulatory aspects.

Rules and Regulations that British banks must follow have force of law as they are issued pursuant to legislation by the Minister, or by an organization that is authorized to do so by legislation. The main criminal legislation is the Proceeds of Crime Act 2002[11] and the Terrorism Act 2000[12], which banks have to be aware of.

MALAYSIAN ANTI-MONEY LAUNDERING AND ANTI-TERRORISM FINANCING ACT AND UNITED KINGDOM PROCEEDS OF CRIME ACT

The Anti-Money Laundering and Anti-Terrorism Financing Act was enacted in 2001 to provide the legal framework to combat money laundering and came into force in January 2002 with banks covered from the effective date. A 2007 Amendment Act extended the Anti-Money Laundering Act, as it then was, to cover terrorism financing. The Act defines its purpose is to:

> provide for the offence of money laundering, the measures to be taken for the prevention of money laundering and terrorism financing offences and to provide for the forfeiture of terrorist property and property involved in, or derived from, money laundering and terrorism financing offences, and for matters incidental thereto and connected therewith.[13]

In Malaysia, the actual money laundering offence is given in Section 4 of AMLATFA, to be read with the definition in s3. In Britain, the offence of money laundering is given in Sections 327, 328 and 329 of POCA.[14]

Banks are specifically covered by AMLATFA by being included in its Schedule 1:

First Schedule
[Section 3, definition of 'reporting institution']
Part 1

1. Banking business, finance company business, merchant banking business, discount house business and money-broking business as defined in the Banking and Financial Institutions Act 1989.
2. Islamic banking business as defined in the Islamic Banking Act 1983.[15]

Therefore, a 'reporting institution' is:

> any person, including branches and subsidiaries outside Malaysia of that person, who carries on any activity listed in the First Schedule[16];

As such, Malaysian banks are bound by the regulatory provisions of Part 4 of AMLATFA and come under Bank Negara as the AMLATFA 'competent authority'.

British Banks are subject to the Money Laundering Regulations 2007 (MLR)[17] issued under the Financial Services and Markets Act 2000[18] to satisfy the requirements of a European Union Directive.[19] This Directive emphasizes the issue of Customer Due Diligence, the various Reporting Obligations, Record Keeping, and Enforcement. The Regulations cover the same subject matter as the Directive, but according to UK legislation drafting rules.

Banks are covered by the MLR as they come under the definition of 'Credit Institution', which is defined as[20]:

(a) a credit institution as defined in Article 4(1)(a) of the banking consolidation directive; or
(b) a branch (within the meaning of Article 4(3) of that directive) located in an EEA state of an institution falling within sub-paragraph (a) (or an equivalent institution whose head office is located in a non-EEA state) wherever its head office is located, when it accepts deposits or other repayable funds from the public or grants credits for its own account (within the meaning of the banking consolidation directive).

Therefore, banks come under the supervision of the Financial Conduct Authority (FCA).[21]

23. (1) Subject to paragraph (2), the following bodies are supervisory authorities—

(a) the Authority is the supervisory authority for -
  (i) credit and financial institutions that are authorised persons;
  (ii) trust or company service providers that are authorised persons;
  (iii) Annex I financial institutions;

Banks in the United Kingdom have to report suspicions (Suspicious Activity Report – SAR)

as a result of being under 'business in the regulated sector'. A bank falls under the 'regulated sector' if it carries out certain defined activities as per Schedule 9 (Regulated sector and supervisory authorities) of POCA 2002.

Part 1(1) of the Schedule states:

A business is in the regulated sector to the extent that it engages in any of the following activities -

(a) accepting deposits by a person with permission under Part 4 of the Financial Services and Markets Act 2000 (c. 8) to accept deposits (including, in the case of a building society, the raising of money from members of the society by the issue of shares);

This definition covers banks. Banks may also come under investment activity.[22] Therefore, banks are covered by Part 7 (Money Laundering)[23] of POCA.

PART 4 OF MALAYSIAN AMLATFA – (REPORTING OBLIGATIONS), REGULATIONS AND GUIDELINES AND UK MONEY LAUNDERING REGULATIONS 2007

Part 4 of AMLATFA contains 16 sections (13–28), most of which are directly relevant to reporting institutions in their day-to-day business. Banks have been subject to all the provisions of Part 4 since 15 January 2002 when AMLATFA came into force. Some sections of Part 4 – 14(b), 16 and 17 – have since been 'modified' by Regulations issued by the Minister under S84 of AMLATFA.[24] These Regulations must be read together with the relevant section of the Act. The Regulations seem to have been issued to enable these sections of AMLATFA to be in conformity with the terminology of the Bank Negara Guidelines.

Detailed implementation of the Act for all reporting institutions is given by the Guidelines[25] issued by Bank Negara in September 2013.[26] These have force of law as they are issued pursuant to AMLATFA.[27] Bank Negara issues specific Sector Guidelines[28] for particular types of reporting institution. Sector 1[29] covers banks.[30]

Part 4 contains 16 sections:

S13: Record Keeping by Reporting Institutions
S14: Report by Reporting Institutions
S15: Centralisation of Information
S16: Identification of Account Holder
S17: retention of records
S18: Opening Account in false name
S19: Compliance Programme
S20: Secrecy obligation overridden
S21: Obligation of Supervisory or Licensing Authority
S22: Powers to enforce compliance
S23: Currency reporting at border
S24: Protection of persons reporting
S25: Examination of a reporting institution
S26: Examination of a person other than a reporting institution
S27: Appearance before examiner
S28: Destruction of examination record

S13 deals with 'Record Keeping by Reporting Institutions'.[31] It is important to keep records of transactions so that an investigator of any Malaysian law enforcement agency is able to follow the 'paper trail' of any laundered criminal assets. It gives a list of record data that is required.[32] It should be noted that the BNM Guidelines go into greater detail as to transaction information required.

S13(1) seems to imply that records only need to be kept that relate to transactions 'exceeding such amount as the competent authority may specify'. Whether these are the same amounts as are specified in S14 is unclear. In subsection (4), transactions by one person within a certain time must be counted as one transaction. This is to avoid 'smurfing' or 'structuring', where a large single transaction will be broken up into several smaller transactions in order to attempt to avoid the reporting requirements of S14.

REPORTING OF SUSPICIONS

S14 (Report by reporting institutions) states:

A reporting institution shall promptly report to the competent authority any transaction –

(a) exceeding such amount as the competent authority may specify; and
(b) where the identity of the persons involved, the transaction itself or any other circumstances concerning that transaction gives any officer or employee of the reporting institution reason to suspect that the transaction involves proceeds of an unlawful activity.

Point (a) is known as a Cash Transaction Report (CTR). Any transaction above the threshold must be notified.[33] Point (b) is known as a Suspicious Transaction Report (STR). A report must be made if there is a suspicion of money laundering. Money laundering investigation usually begins from these STR and CTR.

A Regulation[34] has been issued to modify s14(b) to make it a requirement to make an STR if the transaction is only attempted and also to emphasize that the amount of any attempted or actual transaction is irrelevant, as long as it suspicious.[35]

Part 29 of the Sector 1 Guidelines give details on the submission of an STR to the Financial Intelligence and Enforcement Department (FIED)[36] of Bank Negara Malaysia (BNM), which is standard for all reporting institutions.

In the case of offshore institutions, there is co-reporting to both BNM-FIED and Labuan Financial Services Authority's (LFSA) Anti-Money Laundering Unit (AMLU). It is likely that some offshore and foreign subsidiary institutions, banks especially, may have to report to the FIU of their home country as well.

In the United Kingdom, SARs,[37] must be made to the UKFIU of the National Crime Agency.

Reporting[38] of suspicious activities is authorized, and criminalized by failure to do so, by Sections 330 (Failure to disclose: regulated sector) and 331 (Failure to disclose: nominated officers in the regulated sector) of the Proceeds of Crime Act 2002.[39]

A lesson in what not to do regarding a suspicious transaction can be found in the *Hosni Tayeb* case.[40]

Hosni Tayeb was a Tunisian national who was an architect, but also had an IT business. In 2000 his company, which owned a database of.ly (Libya) internet addresses, agreed to sell the database to the Libyan state telephone company for USD1.5 million. For various reasons, he did not want to keep the money in Tunisia, but instead opened an account in Britain at HSBC in Derby where a relative lived. As he was a foreign non-resident customer, he was only allowed to open a savings account, which he did by depositing 10 pounds. Soon after this, the payment for the database (944 000 pounds) was credited into the account. The Assistant Manager of the branch was suspicious and 'froze' the account. He contacted the customer for an explanation for the transfer, but was still not satisfied. Therefore he had the money transferred back to the Transmitting Bank and closed the account. Hosni then sued for the return of the money.

It was noted in the court that although the Assistant Manager claimed to have followed standard banking practice, what he did went against all the procedures of the legislation at the time (Sections 93A, B and C of the Criminal Justice Act 1988[41] as well as the Money Laundering Regulations 1993 and the Joint Money Laundering Steering Committee Guidance 1997).

What he should have done was to make a SAR to the FIU at that time (Economic Crime Unit of the National Criminal Intelligence Service) and wait for their instructions. The acts of returning the money and closing the account could have been acts of 'tipping off' by the Assistant Manager had Hosni been a money launderer. Tipping off is an offence under POCA and AMLATFA.[42]

Section 15 of AMLATFA states:

> A reporting institution shall provide for the centralisation of the information collected pursuant to this Part.

This section means that the bank must have the material that is kept pursuant to s13 in such a way that an investigator can easily access it.

CUSTOMER DUE DILIGENCE/ KNOW YOUR CUSTOMER

Section 16 is concerned with the identification of the account holder:

1. A reporting institution -

   (a) shall maintain accounts in the name of the account holder; and
   (b) shall not open, operate or maintain any anonymous account or any account that is in a fictitious, false or incorrect name.

This subsection is self-explanatory. An account must be in the name of the actual holder.

2. A reporting institution shall -

   (a) verify, by reliable means, the identity, representative capacity, domicile, legal capacity, occupation or business purpose of any person, as well as other identifying information on that person, whether he be an occasional or usual client, through the use of documents *such as* identity card, passport, birth certificate, driver's licence and constituent document, or any other official or private document, when establishing or conducting business relations, particularly when opening new accounts or passbooks, entering into any fiduciary transaction, renting of a safe deposit box, or performing any cash transaction exceeding such amount as the competent authority may specify; and
   (b) include such details in a record.

This subsection is an advisory one regarding the documentary material to be used to verify the identity of a customer. Specific guidance on what documents should be used are given in Bank Negara's Guidance.

Subsection 16 (3) of AMLATFA deals with what is now known as 'Customer Due Diligence'.[43] This is covered in great detail in the Bank Negara Guidelines.

3. A reporting institution shall take reasonable measures to obtain and record information about the true identity of the person on whose behalf an account is opened or a transaction is conducted if there are any doubts that any person is not acting on his own behalf, particularly in the case of a person who is not conducting any commercial, financial, or industrial operations in the foreign State where it has its headquarters or domicile.

A Regulation[44] has since been issued that has to be read together with S16, which emphasizes Customer Due Diligence:[45] This Regulation appears to have been made to ensure greater compatibility with the BNM Guidance.[46]

The Guidelines ask for 'risk profiles' of customers to be made, which means that the following has to be taken into account namely the origin of the customer and location of business; background or profile of the customer; nature of the customer's business; structure of ownership for a corporate customer; and any other information suggesting that the customer is of higher risk.[47]

A large part of the Guidelines covers various aspects of CDD.[48] The Documentary material to be provided by prospective customers is defined. For instance an individual customer needs to provide at least: full name; NRIC/ passport number; permanent and mailing address; date of birth; and nationality.[49]

The best case to illustrate KYC/CDD and the importance of verifying the customer's identity is the Industrial Court case of *Southern Bank Berhad v Yahya Talib*.[50] Yahya Talib was an account manager at a branch of Southern Bank. A prospective customer named Supandi wanted to open a current account and Saiful stood as an introducer. The account was opened on 7 December 2003. After the branch operations manager found that Saiful was not eligible to stand as an introducer as he was a DeCheque[51] offender, she requested Yahya to stand in as the introducer to regularize the account on

7 February 2004. Soon after the account was opened, Supandi deposited a RM10 billion cheque into his account. The Maybank cheque was collected, but subsequently returned unpaid with the reason that 'Account closed'. The collection of this cheque, even though it was unpaid, caused disruption to the money market in Malaysia.

Supandi, when applying to open an account, had claimed that his occupation was a trustee and mandate of the Federation. Although Yahya did not know Supandi, he was willing to be his introducer. However, he did know Saiful as a former member of the bank's staff. The charge against Yahya by the disciplinary panel was a breach of the bank's prescribed procedure by acting as an introducer although he did not know, and had not even met, the customer. Yahya, with 31 years experience as a banker, claimed that he was unaware of BNM/GP9[52] and also claimed that he had never been sent on an AML course.

The Tribunal noted that he had failed to follow the correct procedure for account opening as per the bank's Accounting & Procedure Manual and was in breach of the Know-Your-Customer policy. Therefore his dismissal was valid.

RECORDS

Section 17 specifies the retention of records policy. Documents relating to STRs and CTRs must be kept for a minimum of six years, along with any associated material.[53]

1. (1) Notwithstanding any provision of any written law pertaining to the retention of documents, a reporting institution shall maintain any record under this Part for a period of not less than six years from the date an account has been closed or the transaction has been completed or terminated.
2. A reporting institution shall also maintain records to enable the reconstruction of any transaction in excess of such amount as the competent authority may specify, for a period of not less than six years from the date the transaction has been completed or terminated.

A Regulation[54] has been issued for s17, which requires additional material regarding the customer's account to be kept and to be available for Bank Negara to access:

1. A reporting institution shall ensure that any records under Part IV of the Act including account holder identification records are maintained and any information relating to such records are made available on a timely basis when required by the competent authority.

It makes it clear that the information to be retained is not just related to STR and CTR but also all information related to customers and their accounts.

Paragraph 27.2 of the Sector Guidelines requires all transaction and CDD documents be kept for at least 6 years, longer if there is an ongoing investigation or a prosecution (para 27.3).

Section 19 of the UK MLR 2007 deals with Record Keeping. All relevant records must be kept for at least 5 years. This is so a money laundering 'paper trail' can be reconstructed if necessary.

Section 18(1) of AMLAFTA states that:

1. No person shall open, operate or authorise the opening or the operation of an account with a reporting institution in a fictitious, false or incorrect name.

The section[55] refers to a 'person' involved with an account in a reporting institution, which is a wider term and can include any of the bank's staff, the customer or customers, as well as the bank itself.

The Act's definition of a false name is given in subsection (4):

For the purposes of this section -

(a) a person opens an account in a false name if the person, in opening the account, or becoming a signatory to the account, uses

a name other than a name by which the person is commonly known;
(b) a person operates an account in a false name if the person does any act or thing in relation to the account (whether by way of making a deposit or withdrawal or by way of communication with the reporting institution concerned or otherwise) and, in doing so, uses a name other than a name by which the person is commonly known; and
(c) an account is in a false name if it was opened in a false name, whether before or after the commencement date of this Act.

Obviously, bank staff must avoid allowing a customer account in a false name, which is a requirement of CDD.

COMPLIANCE POLICY – STAFF TRAINING ETC

Section 19 (Compliance programme) is the basis for all the procedures specified in Bank Negara's Standard and Sectoral Guidelines:

1. A reporting institution shall adopt, develop and implement internal programmes, policies, procedures and controls to guard against and detect any offence under this Act.
2. The programmes in subsection (1) shall include -

   (a) the establishment of procedures to ensure high standards of integrity of its employees and a system to evaluate the personal, employment and financial history of these employees;
   (b) ongoing employee training programmes, such as 'know-your-customer' programmes, and instructing employees with regard to the responsibilities specified in Sections 13, 14, 15, 16 and 17; and
   (c) an independent audit function to check compliance with such programmes.

The most important aspect in S19 is not only about KYC/CDD but also Know Your Employee (KYE). A survey conducted by a reputable accountancy firm[56] in Malaysia revealed that the main reasons for employee fraud are as follows:

(i) Greed/Lifestyle 55 per cent
(ii) Personal Financial Pressure 42 per cent
(iii) Family Pressure 18 per cent
(iv) Gambling 13 per cent
(v) Drugs 8 per cent
(vi) Corporate Financial Pressure 8 per cent

There are a few unreported cases of bank employees who have been charged and convicted for money laundering. One interesting case involved Faisal Hussin, a bank executive at Maybank Sri Gombak who was found guilty of 99 counts of money laundering resulting from 100 counts of forgery and 3 of criminal breach of trust (CBT). He was sentenced to a total of 31 years and was fined for RM1 million for the money he had used and 15 months jail in default of that.[57] He was entrusted to look after the money belonging to a customer Syed Vickar Ahmad, a professor from the United States who was doing consultancy job in Malaysia, Faisal stole RM1.3 million from the account over the period of December 2001 to December 2003. He was committing a breach of trust as he was actually a trustee of the account. He basically laundered the money by buying cars, properties and travelling overseas. The prosecution asked for the accused to be appropriately sentenced to send a message to all parties dealing with trust that such crime has severe punishment. The judge said every sen must be earned from their own effort.[58]

Another case involved a bank manager of RHB at Mergong branch, Alor Star named Tan Khay Quan. He was charged and convicted for money laundering, CBT and forgery. He was sentenced to 5 years for CBT, 5 years for forgery and 3 years for money laundering. As CBT and forgery is concurrent, his real sentence is 8 years, he was also fined RM19.3 million, the amount he sent to Hong Kong, undiscovered, in default 1 year. Tan opened up two accounts in the name of existing customers, he then approved RM21 million to the two

accounts, then he withdrew the whole money and sent RM19.3 million to Hong Kong to buy shares.[59]

The Section requires the bank to establish procedures to ensure high standards of integrity of its employees and a system to evaluate the personal, employment and financial history of these employees. Appendix 1 of the Sector Guidelines gives examples of transactions that may trigger suspicion under the sub-heading of 'employees and agents' suggest the following: Changes in employees characteristics, for example: lavish lifestyle or avoiding taking holidays; Changes in employees or agents performance or Sudden strong performance or sudden increase in spending by employees in trust/private banking service.

Section 19 of AMLATFA requires that the procedures also apply to all domestic and foreign branches and subsidiaries, and that each of them also have a money-laundering compliance officer responsible for ensuring that the bank carries out all of its obligations under Part 4. The bank must have its own 'audit functions' to test these procedures as well as the independent audit in 2(c).

Part 28 of the Sector 1 Guidelines gives more detail on compliance:

28.1. Policies, Procedures and Controls
28.2. Board of Directors
28.3. Senior Management
28.4. Compliance Management Arrangements at the Head Office
28.5. Employee Screening Procedures
28.6. Employee Training and Awareness Programmes
28.7. Independent Audit Function

Section 28(7) of the Sector Guidelines has specific requirements for banks regarding the independent audits: ensure that independent audits are conducted to check and test the effectiveness of the policies, procedures and controls for AML/CFT measures; ensure the effectiveness of internal audit function in assessing and evaluating the AML/CFT controls; ensure the AML/CFT measures are in compliance with the AMLATFA, its regulations and the relevant Guidelines; and assess whether current AML/CFT measures that have been put in place are in line with the latest developments and changes of the relevant AML/CFT requirements.

S20 of the UK MLR deals with the basic anti-money laundering procedures and list down the procedures to be carried out as follows:

1. A relevant person must establish and maintain appropriate and risk-sensitive policies and procedures relating to -

   (a) customer due diligence measures and ongoing monitoring;
   (b) reporting;
   (c) record-keeping;
   (d) internal control;
   (e) risk assessment and management;
   (f) the monitoring and management of compliance with, and the internal communication of, such policies and procedures, in order to prevent activities related to money laundering and terrorist financing.

While Section 21 of the MLR relates to training, and stipulates:

21. A relevant person must take appropriate measures so that all relevant employees of his are -

(a) made aware of the law relating to money laundering and terrorist financing; and
(b) regularly given training in how to recognise and deal with transactions and other activities that may be related to money laundering or terrorist financing.

From the above, the bank employees are supposed to know and be conversant about the AML/CFT law as the legal maxim says 'ignorance of the law is no excuse'. The MLR also stresses about ongoing staff training as these will help the staff to be more alert as well as proficient in detecting suspicious transactions. Basically, the money launderers, especially the organized criminals, are also well trained and

experienced and it is just like playing catch-up with them. The criminals have come up with many new typologies to circumvent the law and procedures. As such, the staff members of banks need to keep themselves abreast with the latest developments and typologies of these launderers and terrorists.

S20 of AMLATFA (Secrecy obligations overridden), states:

> The provisions of this Part shall have effect notwithstanding any obligation as to secrecy or other restriction on the disclosure of information imposed by any written law or otherwise.

As such, S133 (Secrecy) of the Financial Services Act 2013 (FSA) does not apply to any AMLATFA-related issue. Similarly, banking secrecy does not apply in a criminal investigation of any case under BAFIA. Compliance with AMLATFA and the Guidelines are overseen by Bank Negara in its role as the supervisory authority for banks as well as the competent authority under AMLATFA.

S21 lays out the role of Bank Negara as the 'relevant supervisory authority' of banks in regard to money laundering.[60] The section gives Bank Negara the power to revoke or suspend a bank's licence if the reporting institution is convicted of an offence under AMLATFA.

Section 22 covers the issue of a financial institution's compliance with Part 4 of AMLATFA. S22(1) states:

> An officer of a reporting institution shall take all reasonable steps to ensure the reporting institution's compliance with its obligations under this Part.

This subsection has the effect of placing a legal obligation on the money laundering compliance officer. Subsection (4) states that anyone contravening (1) commits an offence.

Subsection (2) allows Bank Negara as the competent authority to apply to the High Court for an Order against individuals at a reporting institution to force compliance with AMLATFA. Bank Negara can also have an agreement, under (3), with a reporting institution for it to become compliant. Failure to comply with a subsection (3) directive is an offence, as also stated in (4). Oddly, Bank Negara does not appear to be able to simply issue a fine for non-compliance, as under (4), a conviction is required.

UNITED KINGDOM

Money Laundering Regulations 2007

The actual money laundering offence is found in Part 7 of Proceeds of Crime Act 2002, covering sections 327, 328 and 329.

The MLR does not only apply to banks, but also to a variety of institutions that handle money in whatever form, that is

1. (1) Subject to regulation 4, these Regulations apply to the following persons acting in the course of business carried on by them in the United Kingdom ('relevant persons') -

   (a) credit institutions;
   (b) financial institutions;
   (c) auditors, insolvency practitioners, external accountants and tax advisers;
   (d) independent legal professionals;
   (e) trust or company service providers;
   (f) estate agents;
   (g) high value dealers;
   (h) casinos.

If a registered institution contravenes the MLR, the relevant supervisory body, the FCA in the case of banks, can have the offending institution prosecuted.

The main emphasis of the current Regulations is on Customer Due Diligence[61] (CDD). S5 applies to all types of institution and is likewise fundamental for banks when accepting a customer:

'Customer due diligence measures' means -

(a) identifying the customer and verifying the customer's identity on the basis of

documents, data or information obtained from a reliable and independent source;
(b) identifying, where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures, on a risk-sensitive basis, to verify his identity so that the relevant person is satisfied that he knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement; and
(c) obtaining information on the purpose and intended nature of the business relationship.

A case that illustrates the failure of CDD by the bank officer is the case of *T R Drakes v Abbey PLC*.[62] This was an appeal by Mr Drake, the Claimant, before the London Employment Tribunal against a judgment of a lower Tribunal that dismissed his various complaints against his former employer, the Respondent, Abbey PLC. On appeal, the Appeal Tribunal found that the Claimant was not unfairly dismissed.

The Tribunal found:

> That the Respondent's AML procedures required that mortgage applications should not be accepted until original documents such as a passport, to verify identity, and a current bank statement to verify an address, were seen by the person processing the application.

That process included the 'four eye check' whereby two separate employees, who had to be branch managers and mortgage advisors, had to verify that they had seen the relevant original documents. An investigation was carried out by a principal investigator into a number of possibly fraudulent mortgage applications. As a result of that investigation, it was concluded that the Claimant had:

> failed to follow the Respondent's AML procedures, in that he had processed mortgage applications on the basis of photocopied documents supplied by Mr Baduge, in some cases via the South Kensington branch managed by Mrs Drakes, as she now is.[63]

The current definition of CDD has remained relatively constant for the last 20 years. What is more recent is the requirement to maintain CDD over the lifetime of the relationship:

1. (1) A relevant person must conduct ongoing monitoring of a business relationship.
2. 'Ongoing monitoring' of a business relationship means -

   (a) 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
   (b) keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up-to-date.
   (c) Regulation 7(3) applies to the duty to conduct ongoing monitoring under paragraph (1) as it applies to customer due diligence measures.

This is to take into account the fact that a customer who passes the original CDD may subsequently engage in money laundering. Therefore, CDD is now a continuous process for a bank.

The MLR is brief because detailed provisions of money laundering and terrorist financing are found in the Joint Money Laundering Steering Group Guidance.

FINANCIAL CONDUCT AUTHORITY HANDBOOK

The FCA issues a Handbook covering all aspects of banking operations. Failure to adhere to the Rules therein can result in heavy fines that the FCA has the power to enforce on offending banks and related institutions,

Chapter 6.1[64] covers general compliance. As 6.1.1 states:

> A firm must establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the firm including its managers, employees and appointed representatives (or where applicable, tied agents) with its obligations under the regulatory system and for countering the risk that the firm might be used to further financial crime.

This Chapter 6.1 gives an obligation to a bank to ensure that the procedures that it has in place are sufficient to maintain compliance with the Money Laundering Regulations 2007, as well as any possible obligations under the Proceeds of Crime Act 2002 and the Terrorism Act 2000.

Chapter 6.3[64] of the Handbook contains the Rules[65] that specifically cover Anti-Money Laundering for banks. A firm must have *inter alia* systems and controls that:

1. Identify, assess, monitor and manage the risk, and must be comprehensive and proportionate to the type of activities;
2. Mentions about money laundering risk and failure to manage the risk;
3. Have regular assessments to ensure compliance with 6.3.1;
4. 6.1.1, 6.3.1 and 6.3.10 are not relevant for R42(3) and R45(2) of the Money Laundering Regulations 2007, S330(8) of the Proceeds of Crime Act 2002 and S21A(6) of the Terrorism Act 2000;
5. The FSA will see if the business has followed the JMLSG Guidance when considering if any Rules have been broken;
6. To identify risk a range of factors should be considered, such as the customer's product, distribution and complexity and volume of transactions;
7. Systems and controls must include employee training, provide information to the 'governing body' and senior management, which must include annual report by MLRO, documentation for risk management and risk profile, take into account risk in daily operations for new products, new customers and business profile changes, and measures to ensure that identity procedures for new customers are not unreasonable;
8. A director or senior manager must be responsible for AML systems and controls (can also be MLRO);
9. An MLRO (with sufficient seniority) must be appointed with responsibility for compliance with FSA Rules who has the resources and information to carry this out;
10. The MLRO must be the focal point for AML, and is expected to be in the United Kingdom;
11. FSA has guidance on how to reduce the risk of being used for financial crime (including money laundering).

The FCA fines for failure to follow these rules can be very heavy. In July 2012, Turkish Bank (UK) Ltd[66] was fined 294 000 pounds for breaching the Money Laundering Regulations. It had failed to:

1. establish and maintain appropriate and risk-sensitive AML policies and procedures for its correspondent banking relationships;
2. carry out adequate due diligence on and ongoing monitoring of the firm's customers acting as respondent banks in TBUK's correspondent banking relationships (the Respondent(s)) and reconsider these relationships when this was not possible; and
3. maintain adequate records relating to the above.

In May 2012, a fine of 525 000 pounds was imposed on Habib Bank AG Zurich[67] for breaches of Rules 6.1.1, 6.3.1 and 6.3.3. These faults had remained in place for about 3 years. The FCA found that the bank had failed to:

(a) establish and maintain an adequate procedure for assessing the level of money laundering risk posed by prospective and existing customers (including maintaining a flawed High Risk Country List);

(b) conduct sufficient enhanced due diligence ('EDD') in relation to higher risk customers;
(c) carry out adequate reviews of its AML systems and controls; and
(d) revise training adequately to address shortcomings in AML practice identified by the MLRO and to maintain sufficient records of staff completion of AML training and of all AML steps taken on individual customer accounts.

Similarly, in March 2012, Coutts & Co[68] was fined 8.75 million pounds for breaches of Rules 6.1.1 and 6.3.1. The faults, which the FCA found had existed for three years, were that the bank did not:

(i) assess adequately the level of money laundering risk posed by prospective and existing high-risk customers. This included failing properly to identify and record all politically exposed persons (PEPs);
(ii) gather the appropriate level of due diligence information about a large number of prospective high risk customers;
(iii) apply robust controls when establishing relationships with high-risk customers. In particular, the AML team failed to provide an appropriate level of scrutiny and challenge;
(iv) consistently apply appropriate ongoing monitoring to its existing high-risk customers to ensure that changes in circumstances and risk profiles were identified, assessed and managed appropriately and that all unusual transactions would be identified; and
(v) carry out adequate reviews of its AML systems and controls for high-risk customers.

The issues highlighted in (c) and (d), and in (v), regarding failures of the AML systems and controls are common to all FCA fined banks, but those regarding high-risk customers/politically exposed persons have come to the fore.[69] This explains why there is such an emphasis on this CDD issue in the United Kingdom, and international, regulatory framework.

However, in the above cases, no money laundering appeared to have occurred, but the serious lapses by the banks allowed the possibility of money laundering. The FCA, and earlier the FSA, has imposed fines on other banks for breaching the rules as follows:[70]

No	*Date*	*Bank*	*Fine (in pounds)*	*Offence*
(1).	December 2002	Royal Bank of Scotland	750 000	Non-compliance with KYC/CDD
(2).	August 2003	Northern Bank	1 250 000	Non-compliance with KYC/CDD
(3).	December 2003	Abbey National	2 000 000	Non-compliance with KYC/CDD
(4).	January 2004	Bank of Scotland	1 250 000	Failure to keep proper records
(5).	April 2004	Raiffeisen Zentralbank Osterreich	150 000	Failure to update AML manual
(6).	September 2004	Bank of Ireland	375 000	STR failures
(7).	May 2007	BNP Paribas Private Bank	350 000	Fraud/AML failings
(8).	August 2010	Royal Bank of Scotland Group	5 600 000	Sanctions control (TF) failings

The FCA also has fined some compliance officers (Money Laundering Reporting Officer) for personal failure to maintain compliance with ML rules. So far two non-bank cases have been reported by FCA, namely Sudipto Chattopadhyay[71] and Michael Wheelhouse.[72] Sudipto, who was the MLRO for Alpari (UK) Ltd, was fined 14 000 pounds in 2010 and barred from compliance oversight and money laundering reporting for 3 years. FSA listed six failures:

(i) Failed to assess ML and financial crime risk;
(ii) Failed to monitor the compliance and AML and ensure it was adequately resourced;
(iii) Failed to check customers against UK and Other Sanctions List or to find out whether a customer is a PEP;

(iv) Failed to adequately carry out CDD in relation to high-risk jurisdiction customers (non-face-face relationship)
(v) Failed to adequately carry out ongoing monitoring business relationship;
(vi) Failed to adequately train himself and the employees.

Michael Wheelhouse was the MLRO of Sindicatum Holdings Ltd and was fined 17 500 pounds by FSA in October 2008 for failure to ensure the compliance of relevant standards and requirement of ML rules. He also failed to take adequate steps for verifying the identity of the firm's clients.

The most recent case of failings in money laundering procedures regards Standard Bank,[73] which had a very large fine (7.6 million pounds) applied to it by the FCA. It was noted that it failed to

> carry out adequate EDD measures before establishing business relationships with corporate customers that had connections with PEPs; and conduct the appropriate level of ongoing monitoring for existing business relationships by keeping customer due diligence up to date.

There have been criticisms of the approaches that the FSA took regarding AML in the 'Regulated Sector'. Until 2006, the FSA had a risk-based policy in its Handbook. This was unpopular because it put extra pressure on small firms. It was changed to a principles-based policy in that year by transferring the relevant obligations under the Handbook from the Money Laundering section to the Senior Management Arrangements, Systems and Controls section. As a result, firms needed systems and controls appropriate to their business.[74]

The large fines being imposed on banks seem to reflect the fact that they are in a better position to have appropriate controls than small institutions and therefore have no excuse. However, the level of fines imposed does not necessarily imply that it is an effective way to combat money laundering. An article by Ryder (2008) notes the following:[75]

> The imposition of financial penalties has had its desired effect, to make the Regulated Sector comply with the AML regulations. However, it can be concluded that the threat of sanctions has led to a great deal of resentment from the sector and scepticism as to whether the regulations introduced by the FSA are reducing the level of money laundering. The article suggests that the success of the enforcement powers could be cynically measured in the total amount of the fine. It is likely that headline figure of a 2 Million Pound fine is politically satisfying to some; it is not a true measure of effectiveness.

The FSA, and now the FCA, has had a policy of 'credible deterrence' regarding market misconduct such as market abuse. An article by Wilson G and Wilson S[76] argues that the FSA is taking a tough stance regarding such offences, including an increase in criminal prosecutions. Although the article does not cover money laundering, the implication is that the large fines imposed on banks for AML failures is a result of this policy. The article notes that:

> The FSA is very mindful of the complexities of conducting investigations and framing prosecutions around the resourcefulness of offenders to conceal their behaviour; the difficulties of "jury presentation"; and manageability as far as costs and court time are concerned, which it cites as factors informing its commitment to make full use of its regulatory as well as criminal powers (Cole 2010). Indeed, in January 2013 the FSA was keen to publicise that its decision to fine Canadian based Swift Trade 8 Million Pounds had been upheld on appeal to the Upper Tribunal, which had described the firm's activity as "as serious a case of market abuse […] that might be imagined". (FSA Press Notice, 2013)

UK JOINT MONEY LAUNDERING STEERING GROUP GUIDANCE

This group is made up of all the various financial representative bodies, including the British Bankers Association (BBA). Their Guidance is given legal status through Treasury[77] approval. It is recognized by the FSA in its Handbook. The FSA's own Guidance,[78] as mentioned in 6.3.11[79] of the FSA Handbook, states in the first point on page 6:

> This Guide consolidates FSA guidance on financial crime. It does not contain rules and its contents are not binding.

The FSA Guidance also states in its Introduction:[80]

> 1.10 The Joint Money Laundering Steering Group's (JMLSG) guidance for the UK financial sector on the prevention of money laundering and combating terrorist financing is 'relevant guidance' under these regulations. As confirmed in DEPP 6.2.3G, EG 12.2 and EG 19.82 the FSA will continue to have regard to whether firms have followed the relevant provisions of JMLSG's guidance when deciding whether conduct amounts to a breach of relevant requirements.

The FCA Handbook further emphasizes that the JMLSG Guidance takes precedence over the FCA Guidance:

> 6.3.5. The FCA, when considering whether a breach of its rules on systems and controls against money laundering has occurred, will have regard to whether a firm has followed relevant provisions in the guidance for the United Kingdom financial sector issued by the Joint Money Laundering Steering Group.

In other words, a bank would only have to follow the JMLSG Guidance, rather than the FCA Guidance, to satisfy the requirements of the Money Laundering Regulations 2007. Therefore, the question arises as to whether a bank needs to take notice of the FCA Guidance.

It would appear that despite the FCA Guidance being 'non-binding', it is connected to the FCA Handbook and the Rules contained therein, so it might make sense for a bank to follow the FCA Guidance as well, especially in respect of anything that may not be covered by the JMLSG Guidance.

The JMLSG Guidance is in three Parts. Part 1 is Guidance for the UK Financial Sector. Part 2 is Sectoral Guidance and Part 3 is Specialist Guidance.

Part 1 of the Guidance has eight chapters: Senior Management Responsibility; Internal Controls; Nominated Officer/MLRO; Risk-Based Approach; Customer Due Diligence; Suspicious Activities, Reporting and Data Protection; Staff Awareness, Training and Alertness; and Record Keeping.

Needless to say, the chapter on Customer Due Diligence is the longest and is very detailed. This is because stopping laundered money getting into the banking system in the first place by not allowing launderers to open and operate accounts is the most effective way of preventing laundering.

Part 2 is for specific financial sectors. For example, Sector 1 is specifically for Retail Banking. Each Sectoral guidance must be read together with the general guidance in Part 1. The guidance for this Sector covers specific details of CDD. An important point made here is that the systems to detect fraud and those used to detect money laundering are similar:

> 1.11 The AML/CTF checks carried out at account opening are very closely linked to anti-fraud measures and are one of the primary controls for preventing criminals opening accounts or obtaining services from banks. Firms should co-ordinate these processes, in order to provide as strong a gatekeeper control as possible.

Part 3 is relevant to any bank that carries out any kind of international activity under the headings of:

1. Transparency in electronic payments (Wire transfers)

2. Equivalent jurisdictions
3. Equivalent markets
4. Compliance with the UK financial sanctions regime
5. Directions under the Counter-Terrorism Act 2008, Schedule 7

Of course, nearly all banks will be subject to this guidance merely by receiving and transmitting funds between accounts.

CONCLUSION

As Malaysian banks have been subject to varying degrees of money laundering regulation for 20 years there should be no excuse for failure to follow their legal requirements. The fact that no Malaysian banks have been prosecuted or fined to date does not mean that they can just sit back, as being found to be non-compliant can have far-reaching and serious consequences.

Major banks in countries, such as the United Kingdom and the United States, have been given multi-million pound and dollar fines for compliance failures and Malaysian banks should not think that they are immune to failures. Therefore, constant oversight of their various systems is very important.

It is a defence that an institute took all reasonable steps and followed due diligence in the event of proceedings against it. Following the legislation and the Guidelines would back up this defence. It is not just a legal requirement, but is also good business sense.

Banks in Britain have also been subject to various money laundering rules, regulations and legislation for 20 years, but despite this, major banks are still being fined heavily for breaching FCA Rules. However, these banks have been fortunate not to be prosecuted as many FCA Rules are similar to legal requirements under the Money Laundering Regulations 2007.

Banks have to be very serious about anti-money laundering compliance, particularly regarding CDD of 'high risk customers' and this highlights the importance of the Money Laundering Reporting Officers in ensuring that all compliance systems work at all times. Failure to do so can result in the MLRO also being found liable in his personal capacity. At the very least, as case law in the United Kingdom and Malaysia has shown, anyone working at a bank not following AML/CFT rules can be dismissed from employment.

It should also be noted that apart from ever larger fines, there is also the possibility of criminal prosecution if the FSA decided to do so, as it has this power. Malaysian banks should take note of the situation in Britain as Bank Negara has similar power that it could use if it chooses to do so.

REFERENCES AND NOTES

1 These countries come under High Risk and Non-Cooperative Jurisdiction, Iran and North Korea have been asked to apply counter measures against AML/CFT risk and so far they are not doing anything. For more details, see the FATF website at www.fatf-gafi.org.
2 See www.fatf-gafi.org.
3 With effect from 15 January 2002.
4 Replaced by the Financial Services Act 2013.
5 Replaced by the Islamic Financial Services Act 2013.
6 Replaced by Capital Market and Securities Act 2007.
7 Replaced by Money Services Business Act 2011.
8 There is no statutory definition of the word 'bank' in the current FSA 2013 (which repealed and replaced BAFIA); however, FSA defines 'banking business' in Section 2 as: '(a) the business of - (i) accepting deposits on current account, deposit account, savings account or other similar account; (ii) paying or collecting cheques drawn by or paid in by customers; and (iii) provision of finance; and (b) such other business as prescribed under section 3'.
9 It should be noted that all legislative and regulatory matters relating to money laundering derive from the FATF Recommendations. As such, the EC Directives and UK Regulations can be traced back to the FATF Recommendations. Although the general content will be the same, the amount of detail provided is much greater.
10 There is no statutory definition of a bank in England. However, Section 2 of the English Bills of Exchange Act 1882 provides that '"Banker" includes a body of persons whether incorporated or not who carry on the business of banking '. From the common law perspective, also, there is no definition of a bank, but only the word 'banking business'. In the leading case of United Dominions Trust Ltd *v* Kirkwood [1966] 2 QB 431, the Court of Appeal defined the characteristics of banking business as (1) the conduct of current accounts; (2) the payment of cheques drawn on bankers; (3) the collection of cheques for customers. Another cases expressing this view are Re District Savings Bank, ex parte Coe (1861) 3 De GF & J at p. 335,

Halifax Union *v* Wheelwright (1875) LR 10 Exch at p. 1883 and Re Birkbeck Permanent Benefit Building [1912] 2 Ch 1833. However, the above view that a person cannot be considered a banker unless he operates current account for customers has been rejected by other judges in the case of R *v* Industrial Dispute Tribunal, ex parte East Anglian Trustee Savings Bank [1954] 11 WLR at p. 1093 held that the bank carried on the business of banking notwithstanding the fact that it did not issue cheque books to its customers. Other cases of this view include Re Bottomgate Industrial Co-Operative Society (1891) 65 LTT at p. 712, Commissioners of the State Savings Bank of Victoria *v* Permewan Wright & Co Ltd 91914) 119 CLR at p. 457 and Re Shields Estate [1901] IR at p. 172.

11 This Act contains the actual offences of money laundering.

12 Further provisions relating to terrorism financing can be found in the Anti-terrorism, Crime and Security Act 2001 and the Counter-terrorism Act 2008.

13 AMLATFA Preamble.

14 S340(11) states: Money laundering is an act which - (a) constitutes an offence under sections 327, 328 or 329, (b) constitutes an attempt, conspiracy or incitement to commit an offence specified in paragraph (a), (c) constitutes aiding, abetting, counselling or procuring the commission of an offence specified in paragraph (a), or (d) would constitute an offence specified in paragraph (a), (b) or (c) if done in the United Kingdom.

15 For the purposes of AMLATFA, conventional and Islamic banks are the same. Banks have been subject to AMLATFA since the Act came into effect.

16 Section 3 – Interpretation.

17 With effect from 15 December 2007, which replaced the Money Laundering Regulations 2003. This Directive is, in turn, designed to satisfy the latest requirements of the FATF 40 Recommendations at the time.

18 Sections 168(4)(b), 402(1)(b), 417(1)(c) and 428(3).

19 Directive 2005/60/EC of the European parliament and of the council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. A draft for the latest 4th Anti-Money Laundering Directive was voted on, and passed, by the European Parliament. It will become law in due course. See http://www.europarl.europa.eu/news/en/news-room/content/20140307IPR38110/html/Parliament-toughens-up-anti-money-laundering-rules. This creates new obligations regarding Risk Assessments, Due Diligence, Record Keeping and Beneficial Ownership.

20 3(2).

21 References to the FCA also include its predecessor, the Financial Services Authority. The FCA came into being in April 2013. Part of the FSA's responsibilities were passed on to the Bank of England under its Prudential Supervision Authority.

22 (2) An activity falls within this sub-paragraph if it constitutes any of the following kinds of regulated activity in the United Kingdom: (a) dealing in investments as principal or as agent; (b) arranging deals in investments; (c) managing investments; (d) safeguarding and administering investments; (e) sending dematerialised instructions; (f) establishing (and taking other steps in relation to) collective investment schemes; (g) advising on investments.

23 This Part has 14 sections from s327 to s340.

24 84(1) The Minister of Finance or the Minister of Home Affairs, as the case may be, may make such regulations as are necessary or expedient to give full effect to or for carrying out the provisions of this Act. (2) Without prejudice to the generality of subsection (1), regulations may be made - (a) to prescribe anything that is required or permitted to be prescribed under this Act; (b) to provide that any act or omission in contravention of any provision of such regulations shall be an offence; (c) to provide for the imposition of penalties for such offences which shall not exceed a fine of one million ringgit or imprisonment for a term not exceeding one year or both; and (d) to provide for the imposition of an additional penalty for a continuing offence which shall not exceed one thousand ringgit for each day that the offence continues after conviction.

25 Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Banking and Deposit-Taking Institutions (Sector 1).

26 With effect from 15 September 2013. It replaces the Standard Guidelines, UPW/GP1 and the Sectoral Guidelines, UPWGP1[1].

27 (83). The competent authority may, upon consultation with the relevant supervisory authority, issue to a reporting institution such guidelines, circulars, or notices as are necessary or expedient to give full effect to or for carrying out the provisions of this Act and in particular for the detection or prevention of money laundering.

28 There are currently five Sector Guidelines covering a large variety of reporting institutions. The Securities Commission and the Labuan Financial Services Authority issue their own Guidelines. Other supervisory bodies, such as the Law Society, issue Guidelines to be read with the relevant Sector Guidelines.

29 These Guidelines supersede the 1993 Guidelines on Money Laundering and Know Your Customer Policy (BNM/GP9).

30 Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Banking and Deposit-Taking Institutions (Sector 1).This replaces UPW/GP1[1]: Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) Sectoral Guidelines 1 for Banking and Financial Institutions.

31 The 'competent authority' in this and other sections of Part 4 is defined in S3 as 'the person appointed under subsection 7(1)'. Therefore, pursuant to 7(1) the Minister of Finance appointed the Malaysian central bank as the 'competent authority'.

32 (3) The record referred to in subsection (1) shall include the following information for each transaction: (a) the identity and address of the person in whose name the transaction is conducted; (b) the identity and address of the beneficiary or the person on whose behalf the transaction is conducted, where applicable; (c) the identity of the accounts affected by the transaction, if any; (d) the type of transaction involved, such as deposit, withdrawal, exchange of currency, cheque cashing, purchase of cashier's cheques or money orders or other payment or transfer by, through, or to such reporting institution; (e) the identity of the reporting institution where the transaction occurred; and (f) the date, time and amount of the transaction.

33 The amount has been set at RM 50 000 as of 1 September 2006.
34 PU(A) 104/2007. Anti-Money Laundering and Anti-Terrorism Financing (Reporting Obligations) Regulations 2007.
35 'A reporting institution shall promptly report to the competent authority any attempted transaction or transactions where the identity of the persons involved, the transaction itself or any other circumstances concerning that transaction gives any officer or employee of the reporting institution reason to suspect that the transaction involves proceeds of an unlawful activity regardless of the amount of the transaction'.
36 This is the Malaysian Financial Intelligence Unit (FIU).
37 The terms STR and SAR are not found in any legislation. These terms are what the Malaysian and UK FIUs, respectively, have decided to call these reports.
38 How the SAR is reported will result from s339 (Form and manner of disclosures): (1) The Secretary of State may by order prescribe the form and manner in which a disclosure under Sections 330, 331, 332 or 338 must be made. (2) An order under this section may also provide that the form may include a request to the discloser to provide additional information specified in the form. (3) The additional information must be information which is necessary to enable the person to whom the disclosure is made to decide whether to start a money laundering investigation. (4) A disclosure made in pursuance of a request under subsection (2) is not to be taken to breach any restriction on the disclosure of information (however imposed). (5) The discloser is the person making a disclosure mentioned in subsection (1). (6) Money laundering investigation must be construed in accordance with Section 341(4). (7) Subsection (2) does not apply to a disclosure made to a nominated officer.
39 Also sections 21ZA and 21ZB of the Terrorism Act 2000 in relation to terrorism financing.
40 Hosni Tayeb and (1) HSBC Bank PLC, (2) Al Foursan Company [2004] EWHC 1529 (Comm).
41 Equivalent to sections 327, 328 and 329 of the Proceeds of Crime Act 2002.
42 S93D of the CJA 1993, now s333 of POCA 2002. An equivalent provision exists in s35 of AMLATFA 2001. Tipping off is an unauthorized disclosure to someone that an SAR/STR has been made, and also whether a criminal investigation is being made against a customer.
43 Previously known as 'Know Your Customer' (KYC).
44 PU(A)104/2007. Anti-Money Laundering and Anti Terrorism Financing (Reporting Obligations) Regulations 2007.
45 There appears to be no specific definition of CDD in AMLATFA or the Guidelines. In the Definition and Interpretation Part (10) of the Guidance it merely states that CDD 'Refers to any measures undertaken pursuant to Section 16 of the AMLATFA'. It is presumed to be essentially the same as the previous 'know your customer' (KYC) policy. CDD is basically knowing all about the customer so that a potential money launderer is detected at the initial account opening stage, or if not then by an ongoing CDD process.
46 13.2.1. Reporting institutions are required to: (a) identify the customer and verify that customer's identity using reliable, independent source documents, data or information; (b) verify that any person purporting to act on behalf of the customer is so authorised, and identify and verify the identity of that person; (c) identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that the reporting institution is satisfied that it knows who the beneficial owner is; and (d) understand and, where relevant, obtain information on, the purpose and intended nature of the business relationship.
47 See Part 12.4.
48 13.1.1. Reporting institutions are required to conduct CDD on the customer and the person conducting the transaction, when: (a) establishing business relations; (b) providing money changing and wholesale currency business for transactions involving an amount equivalent to RM3000 and above; (c) providing wire transfer services; (d) carrying out occasional transactions involving an amount equivalent to RM50 000 and above, including in situations where the transaction is carried out in a single transaction or several transactions in a day that appear to be linked; (e) carrying out cash transactions involving an amount equivalent to RM50 000 and above; (f) it has any suspicion of ML/TF, regardless of amount; or (g) it has any doubt about the veracity or adequacy of previously obtained information.
49 See 13.4.1.
50 Industrial Court KL, award no. 1692 of 2006, case no. 4/4-626/05.
51 Holds a database of individuals who have been blacklisted for issuing cheques that 'bounce'.
52 The predecessor of UPW/GP1[1].
53 If the Supervisory Authority specifies a longer period, the record must be kept for that period. For example, for lawyers, it has to be for 12 years as it involves land matters.
54 PU(A)104/2007.
55 Subsections (2) and (3) deal with the technical issues of a person known by more than one name.
56 KPMG Malaysia Fraud, Bribery and Corruption Survey 2013. See http://www.kpmg.com/MY/en/IssuesAndInsights/ArticlesPublications/Documents/2013/fraud-survey-report.pdf.
57 Faisal went on appeal but he got more than he bargained for, that is, he was given two strokes on top of the original sentence, obtained from *The Star*, 18 September 2009.
58 *The Star*, 13 May 2008.
59 *The Star*, 26 January 2007.
60 (1) The relevant supervisory authority of a reporting institution or such other person as the relevant supervisory authority may deem fit may - (a) adopt the necessary measures to prevent or avoid having any person who is unsuitable from controlling, or participating, directly or indirectly, in the directorship, management or operation of the reporting institution; (b) examine and supervise reporting institutions, and regulate and verify, through regular examinations, that a reporting institution adopts and implements the compliance programmes in Section 19; (c) issue guidelines to assist reporting institutions in detecting suspicious patterns of behaviour in their clients and these guidelines shall be developed taking into account modern and secure techniques of money management and will serve as an educational tool for reporting institutions' personnel; and (d) cooperate with other enforcement agencies and lend technical assistance in any investigation, prosecution or proceedings relating to any unlawful activity or offence under this Act.

61 Has also been known as 'Know Your Customer' (KYC).
62 Heard by the Employment Appeal Tribunal in UKEAT/0369/07. See http://www.bailii.org/cgi-bin/markup.cgi?doc=/uk/cases/UKEAT/2008/0369_07_1801.html&query=drakes+and+abbey&method=boolean.
63 The dismissal letter stated that one of the two reasons for his dismissal was: '(1) Failure to follow Anti Money Laundering procedure – in that you did not seek clarification of whether original ID had been seen and directly accepted photocopied ID on at least one or two occasions from an Introduced Mortgage Broker and you knowingly allowed applications to be processed without the customer present. This is a very serious breach of AML procedures and potentially exposed the company to financial and regulatory risk'.
64 Chapter 6 (Compliance, internal audit and financial crime) in Senior Management Arrangements, Systems and Controls.
65 Only 1, 3, 8 and 9 of the Chapter are actual Rules, the rest are regarded as guidance.
66 See http://webarchive.nationalarchives.gov.uk/20130301170532/http://www.fsa.gov.uk/static/pubs/final/turkish-bank.pdf.
67 The private banking subsidiary of Habib Bank Pakistan. See http://webarchive.nationalarchives.gov.uk/20130301170532/http://www.fsa.gov.uk/library/communication/pr/2012/055.shtml.
68 The private banking unit of the Royal Bank of Scotland Group. See http://webarchive.nationalarchives.gov.uk/20130301170532/http://www.fsa.gov.uk/library/communication/pr/2012/032.shtml.
69 Most of the banks that have been fined by the FSA in recent years are 'private banks' (see http://www.fca.org.uk/news/standard-bank-plc-fined-for-failures-in-its-antimoney-laundering-controls).
70 See http://webarchive.nationalarchives.gov.uk/20130301170532/http:/www.fsa.gov.uk/about/press/facts/fines/2012.
71 See http://webarchive.nationalarchives.gov.uk/20130301170532/http://www.fsa.gov.uk/pages/library/communication/pr/2010/077.shtml.
72 See http://webarchive.nationalarchives.gov.uk/20130301170532/http://www.fsa.gov.uk/pages/library/communication/pr/2008/125.shtml.
73 The British subsidiary of a South African Bank.
74 Ryder, N. (2008) The financial services authority and money laundering: A game of cat and mouse. *Cambridge Law Journal* 67(3): 645.
75 Ryder, N. (2008) The financial services authority and money laundering: A game of cat and mouse. *Cambridge Law Journal* 67(3): 652.
76 Wilson, G. and Wilson, S. (2014) The FSA, 'credible deterrence', and criminal enforcement – A 'haphazard pursuit'? *Journal of Financial Crime* 21(1): 4–28.
77 The UK Finance Ministry.
78 Not to be confused with the Handbook. 'Financial Crime: A Guide For Firms. Part 1: A Firm's Guide to Preventing Financial Crime'. Issued in April 2013.
79 'The FCA provides guidance on steps that a firm can take to reduce the risk that it might be used to further financial crime. (Financial Crime: A guide For Firms)'.
80 1.5 The material in the Guide *does not* form part of the Handbook, but it does contain guidance on Handbook rules and principles, 1.7 The Guide contains 'general guidance' as defined in section 158 of the Financial Services and Markets Act 2000 (FSMA). 'The guidance *is not binding* and we will not presume that a firm's departure from our guidance indicates that it has breached our rules'.