Prevention of Money Laundering & Terrorism Financing

Role of Real Estate Agents (REAs)
Before We Begin: What do these cases have in common?

**Financial Times – April 18, 2017**

**UK Property**

London’s housing crisis is abetted by illicit funds
Revealing the true ownership of UK property may help stop the rot

**FT View**

There are two good reasons why the UK should be putting up more effective barriers to the illicit funds that wash up so prodigiously on Britain’s shores.

The first relates to the UK’s credibility in the campaign against corruption. Successive governments have taken centre stage in the global war against this scourge. But their stance has always looked a little Janus-faced, on the one hand offering support to those battling corrupt practices in the developing world, on the other doing too little in practical terms to prevent the proceeds from ending up in Britain.

---

**Financial Times – February 24, 2017**

**Money Laundering**

US prime property is magnet for illicit wealth, warns Treasury
Probe unearths string of dubious cash buyers in New York, Miami and other cities

**Property along the Miami Beach Coast**

FEBRUARY 24, 2017 by: Tom Burgis

US real estate’s reputation as a favourite destination for international money launderers has grown after a Treasury investigation confirmed fears that top-end property in New York, Miami and other cities is being used to channel illicit wealth.

The Financial Crimes Enforcement Network (FinCEN), a Treasury unit, found that one in three buyers who used shell companies for cash purchases of luxury property in leading cities had had the alarm raised about their financial dealings.
Learning Objectives

1. REA’s roles as a Reporting Institution within Malaysia’s AML/CFT Framework
2. AML/CFT requirements on REAs
3. How to comply with AML/CFT requirements
Presentation Outline

Overview of ML/TF & Malaysia’s AML/CFT Regime

ML/TF Vulnerabilities of Real Estate Sector

AML/CFT Requirements on REAs

BNM’s Supervisory Approach & Expectation
Money Laundering (ML) & Terrorism Financing (TF) defined

**ML**

“A process of converting cash or property derived from criminal activities to give it a **legitimate appearance**. It is the process of **cleaning and disguising** the criminal origin of ‘dirty’ money.”

**TF**

“Process of financing terrorist activity either through **legitimate** or **illegitimate** sources.”

Why Criminals Launder Their Money?

1. To **remove or distance themselves from the criminal activity** generating the illicit proceeds, thus making it more difficult to identify & prosecute key perpetrators
2. To **reinvest the profits** in future criminal activity or in legitimate businesses
3. To **enjoy the benefits of the illicit proceeds** without bringing undue attention to themselves

Impact of ML/TF

1. Proliferation of criminal activities
2. Existence of illegal businesses competing with legitimate businesses
3. Lower integrity and reputation of financial system
How Do Criminals Launder Money?

<table>
<thead>
<tr>
<th>Serious Offence</th>
<th>Laundering of Illegal Proceeds Activities</th>
</tr>
</thead>
</table>
| **Under Second Schedule of the AMLA** | **Placement**  
To distance illegal proceeds from its sources |
| Drug Exchange | Bank |
| Proceed | Deposit |
| **Layering**  
To complicate tracing of funds | Related Accounts |
| Credit Card | Wire Transfer |
| **Integration**  
To integrate illegal proceeds into economy | Proceed of Sales (even at lower price) |
| Companies | Clean Money |
| Profit | Luxurious Goods |
| Example:  
• Placement in FI  
• Breaking down transaction into smaller amount | Example:  
• Multiple transfer  
• Repeat Invoicing  
• Re-sale of assets |
| Example:  
• Purchasing of real properties and high value items  
• Engaging in legal business by providing capital or loans |
All countries are to comply with the FATF standards

**UN Conventions and Resolutions**

- The Vienna Convention
- The Palermo Convention
- Security Council Resolution 1373
- Security Council Resolutions 1267 and 1988
- International Convention for the Suppression of the Financing of Terrorism

**Financial Action Task Force (FATF), Headquartered in Paris [Malaysia is a ‘Member’]**


Implementation by FATF-Styled Regional Bodies (FSRBs)

**Principles under these Resolutions have been embedded into the FATF standards**

**APG – M’sia is a ‘Member’**

All countries are members of a FSRB (except Iran and DPRK)

- CFATF
- MONEYVAL
- EAG
- ESAAMLG
- GAFILAT
- GIABA
- MENAFATF
- GABAC

International Standards include requirements on DNFBPs
Malaysia’s AML/CFT Framework

- BNM the competent authority for AMLA
- Criminalisation of ML/TF i.e. More than 300 offences from more than 45 legislations
- Freezing, seizure & forfeiture of properties
- Identify & respond to emerging risks through National Risk Assessment
- Adequate investigation & enforcement powers
- Fully-functional FIU in BNM
- AML/CFT Units set-up in key law enforcement agencies (LEAs)
- Structured training programs for financial investigators

Responsibilities of Reporting Institutions (RIs)
- More than 43,000 RIs (both financial institutions and DNFBPs)
- Implement effective AML/CFT compliance programme to detect and deter ML/TF
- Submit CTRs and STRs to FIED, BNM

- National Coordination Committee for integrated approach across 16 Ministries/Agencies
- MoUs and Strategic Partnerships with Foreign FIUs & Counterparts
- Strong networks with International/regional bodies
  - FATF, APG, Egmont Group
Reporting Institutions (RIs) under the AMLA - A Snapshot

1. Financial Institutions (FIs)
   - Banks
   - Insurance companies
   - Securities / Fund managers
   - Money changers
   - E-money operators
   - Offshore financial institutions

2. Designated Non-Financial Businesses and Professions (DNFBPs)
   - Gatekeepers – Lawyers, accountants, company secretaries and trust companies
   - Dealers in precious metals and stones
   - Real estate agents
   - Casino
   - Gaming Houses
RIs are the First Line of Defence

Identify illicit activities and investigate crimes

1. Financial Institutions
   - Placement of proceeds from unlawful activities
   - Apply loan and use illegal proceeds for repayment

2. Submit Suspicious Transaction & Cash Threshold Reports

3. Financial Intelligence Unit (FIED, BNM)
   - Collect, analyse, disseminate financial intelligence
   - Supervisory authorities (BNM, SC, LFSA)
   - BNM in collab. with licensing bodies & SROs

4. Feedback on effectiveness of financial intelligence

5. Monitor & enforce AML/CTF requirements

AML/CFT PREVENTIVE MEASURES
- ML/TF Risk Assessment & Client Risk Profiling
- CDD and Enhanced CDD on Clients
- Record Keeping
- On-going Monitoring of Clients’ Transactions
- Promptly Detect & Report Suspicious Transactions

Criminals and Criminal Activities

Financial Institutions
- Non-bank FIs
- DNFBPs

Law enforcement Agencies (LEAs)
Interconnection in a Typical Anti-Money Laundering Regime

Supervision

Preventive Measures

Suspicious Transaction Reports

FIU Analysis

Investigation and Prosecution

Confiscation

TF Financial Sanctions

Terrorist Financing

Beneficial Ownership

International Cooperation

Risk and Coordination

Financing of Proliferation

TF Financial Sanctions

Terrorist Financing

Beneficial Ownership

International Cooperation

Risk and Coordination

Financing of Proliferation
Key Findings from Mutual Evaluation Exercise (MEE) 2014

- On-site visit by APG & FATF Assessors from 13/11/2014 to 25/11/2014

- Assessment made based on **Technical Compliance** and **Effectiveness of Malaysia’s AML/CFT System**

- Assessment areas relevant to DNFBPs included:
  - Supervision of DNFBPs (Immediate Outcome 3)
  - Preventive measures (Immediate Outcome 4)

- Findings on DNFBPs:
  - Low level of understanding (except for casino) of ML/TF risks and the NRA (para 5.10, pg. 95).

- Malaysia is required to **rectify the deficiencies identified and provide FATF with follow-up report** under the enhanced follow-up process every year.
Presentation Outline

- Overview of ML/TF & Malaysia’s AML/CFT Regime
- ML/TF Vulnerabilities of Real Estate Sector
- AML/CFT Requirements on REAs
- BNM’s Supervisory Approach & Expectation
<table>
<thead>
<tr>
<th>Extent of Vulnerability</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>POSSIBLE</td>
</tr>
<tr>
<td>HIGH</td>
<td></td>
</tr>
<tr>
<td>MEDIUM</td>
<td>• Gaming Companies • Jewellers (DPMS) • Accountants</td>
</tr>
<tr>
<td>LOW</td>
<td>• Pawn Brokers • Notaries</td>
</tr>
</tbody>
</table>
Example of ML Case Involving Real Estate Sector – Case 1

**Case 1: Misuse of real estate agents to gain introduction to a financial institution**

**Brief Facts of Case:**
1. Trustee of an offshore trust approached a REA to buy a property in Country A
2. REA assists to approach bank to enquire on loan application
3. Bank refused the application given unidentifiable identity of beneficiary owner of trust
4. The bank submitted suspicious transaction report
5. Analysis revealed that one of the members of the board of the trust was related to a bank with suspected links to terrorist organization

**Red Flag Indicators:**
- Use of trust accounts
- Unexplained geographic distance between agent, customer and the property

Source: FATF Paper on Money Laundering & Terrorist Financing Through The Real Estate Sector (June, 2007)
Example of ML Case Involving Real Estate Sector – Case 2

**Case 2: Use of solicitor to do multiple property purchase**

**Brief Facts of Case:**
1. Mr. A engaged solicitor to act on behalf for property transactions
2. Solicitor B established trust accounts for Mr. A to facilitate transactions
3. Solicitor B organised conveyancing for purchase of residential property and carried out structure transactions (cash deposits and mortgage pay off) to avoid detection
4. Properties were purchased either in the name or Mr. A or his relatives
5. Based on investigation, Mr. A is involved in money laundering

**Red Flag Indicators:**
- Use of trust accounts
- Structured cash transactions
- Multiple purchase of properties

Source: FATF Paper on Money Laundering & Terrorist Financing Through The Real Estate Sector (June, 2007)
Presentation Outline

Overview of ML/TF & Malaysia’s AML/CFT Regime

ML/TF Vulnerabilities of Real Estate Sector

AML/CFT Requirements on REAs

BNM’s Supervisory Approach & Expectation
How Do We Protect the Sector from Being Abused?

Preventive
- AMLA
- Sector 5
- Subsidiary Legislations / Gazette order
- Circulars

Combative
- Financial Intelligence
- Investigation
- Enforcement

AML/CFT Requirements
- CDD
- Record Keeping
- Reporting of STR
- Risk Profiling
- Compliance Officer
- Compliance Programme
AML/CFT Awareness Session

Legal Instruments

**Legislation**

As specified in First Schedule of AMLA and Sector 5 Guidelines, AML/CFT reporting requirements extend to "registered estate agent as defined in the Valuers, Appraisers and Estate Agents Act 1981 [Act 242]"

- **Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (Act 613) – AMLA**
  - AML/CFT requirements w.e.f. 05/07/01 (01/09/14 for the new AMLA)

**SUBSIDIARY LEGISLATIONS/ GAZETTE ORDER**

- **Anti-Money Laundering (Invocation of Part IV) Order 2006**
  - P.U.(A) 293/2006: Invocation of sections 14(1)(b) and 24 of AMLA w.e.f. 10/08/2006
- **Anti-Money Laundering (Invocation of Part IV) Order 2006**
  - P.U.(A) 103/2007: Invocation of sections 15, 16, 17, 18, 19, 21, 22, 25, 26, 27 & 28 of AMLA w.e.f. 08/03/2007
  - Anti-Money Laundering (Terrorism Financing Orders)

**Guidelines/ Policy Document**

- AML/CFT – Designated Non-Financial Businesses and Professions (DNFBPs) & Other Non-Financial Sectors (Sector 5) Guidelines - Revised & Reissued on 1 Nov 2013

**Circulars**

- Periodic Circulars on FATF Public Statement
Examples of Legal Instruments

AML 2001

LAWS OF MALAYSIA

Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001

Act 613

Date of Royal Assent 23-Jun-2001
Date of publication in the Gazette 5-Jul-2001

An Act to provide for the offence of money laundering, the measures to be taken for the prevention of money laundering and terrorism financing, offences and provide for the institution of property involved in money laundering and terrorism financing. As well as serve as a basis for the establishment of an anti-money laundering and counter financing of terrorism and terrorist financing, and the matters incidental thereto and connected therewith.

ARRANGEMENT OF SECTIONS

PART I

Preliminary

1. Short title and commencement
2. Application
3. Interpretation

PART II

Money Laundering Offences

4. Offence of money laundering
5. Offence of structuring transactions to evade reporting requirement
6. Protection of informers and information
7. Restriction on revealing disclosure under section 5

PART III

Financial Intelligence

8. Functions of the competent authority
9. Provisions relating to the competent authority

Bank Negara Malaysia

Central Bank of Malaysia

AML/CFT Awareness Session

Periodic

Circular on

FATF

Public

Statement

BANK NEGARA MALAYSIA

CENTRAL BANK OF MALAYSIA

Tel: 603-2375-6600 Fax: 603-2375-6616

DigiCode: 8213112

Our Reference: 10 July 2017

To:

All institutions under the

Anti-Money Laundering, Anti-Terrorism Financing

and Proceeds of Unlawful Activities Act 2001 (AML)

Recent Statements by the Financial Action Task Force on Money Laundering

(FATF)

The purpose of this notice, issued pursuant to section 83 of the AMLA, is to inform the reporting institutions (RIs) of the recent Public Statement issued by the FATF on 23 June 2017 on jurisdictions having strategic deficiencies in their anti-money laundering and counter financing of terrorism (AML/CFT) regimes (please see Appendix I).

In the statement, FATF has called upon its members and other jurisdictions to apply effective countermeasures and targeted financial sanctions in accordance with applicable United Nations Security Council Resolutions against the Democratic People’s Republic of Korea (DPRK) arising from ongoing and substantial money laundering and terrorist financing risks emanating from and threats posed by DPRK’s illicit activities in relation to proliferation of weapons of mass destruction and its financing.

In accordance with the AML/CFT Policy Documents issued to your sector, please be advised that RIs are required to conduct enhanced customer due diligence for business relationships and transactions with any person from DPRK including those acting on their behalf. In addition to enhanced CDD requirements, the RIs are also required to apply any relevant countermeasures proportionate to the risk, including limiting business relationship and financial transactions with DPRK or its person and terminating correspondent relationships with DPRK banks, where necessary.

The FATF continues the suspension on the call for countermeasures on Iran, following its commitment and progress made to an agreed Action Plan. The FATF will continue monitor the progress made by Iran. As such, countermeasures as stipulated under respective AML/CFT Policy Documents will not be applicable. However, enhanced due diligence measures which are proportionate to the risk remain applicable to all business relationships and transactions with any person from Iran.

All documents are publicly available @ http://amlcft.bnm.gov.my/
AML/CFT Awareness Session

AML/CFT Requirements

- CDD
- Compliance Programme
- Record Keeping
- Compliance Officer
- Reporting of STR
- Risk Profiling

AMERICAN FOUNDATION FOR INDEPENDENT LEARNING
Customer Due Diligence (CDD) – An Overview

- On-Board
  - Normal
  - Enhanced

- On-Going
  - Normal
  - Enhanced
Customer Due Diligence (CDD) – When?

Three elements:

i. Identification
   - Identify
   - Sight ID document

ii. Verification
   - Make a copy of ID document

iii. On-going Due Diligence
    - Review and update profile
    - Transaction monitoring for consistency with known profile
Customer Due Diligence (CDD) – Individual Customer

**Identification**
- **Customers**
- **Person Conducting Transactions**
- **Beneficial Owners**

**Verification**
- **Individuals**
  - Name
  - Date of Birth
  - Nationality
  - Address & Purpose of Transaction
  - Verification: NRIC / Passport / Other ID Documents

- **Legal Persons/ Legal Arrangements**
  - Name, Legal Form & Proof of Existence
  - Beneficial Owner: Identify directors / shareholders with equity interest of > 25%
  - IC/passport of authorized person
  - Verification: M&A, Forms 24, 49, SSM's Superform etc.
Customer Due Diligence (CDD) – Verification of Individual Customers

ACCEPTABLE DOCUMENTS FOR INDIVIDUAL CUSTOMERS AND BENEFICIAL OWNER

- NRIC/ Passport
- Any other official documents bearing the photograph of the customer, provided that the RI is satisfied with the authenticity of the document.
- If biometric ID is used, verification requirement deemed to have been fulfilled. No photocopy of ID is necessary

If there is doubt – require the customer to produce other supporting official identification documents bearing his/ her photograph
Customer Due Diligence (CDD) – Verification of Customers who are **Legal Persons**

**Identify and verify customer**

- (a) Name, legal form and proof of existence
- (b) Powers that regulate and bind customers
- (c) Address of registered office

**Identify and take reasonable measures to verify beneficial owner (BO)**

(a) **Identity of the natural person who ultimately has a controlling ownership interest in a legal person**
   i. Identification of directors/shareholders with **equity interest of 25% or more**;
   ii. Proper authorisation for persons authorised to represent the company (letter of authority/directors’ resolution); and
   iii. NRIC / Passport to identify the authorised person(s)

(b) **If there is a doubt on the controlling interest** - the identity of the natural person exercising control through other means

(c) **Where there is no natural person identified** - the identity of the natural person who holds the senior management position

**Identification & verification of the BOs up to the level of natural persons who have control**
Customer Due Diligence (CDD) – Politically Exposed Persons (PEPs)

PEPs do not include middle ranking or junior level individuals

Para 14.2.2 – Foreign PEPs to be assessed as having high ML/TF risks which required enhanced due diligence
Customer Due Diligence (CDD) – Enhanced CDD

When is Enhanced CDD Required?

**Conditions**
- Foreign PEPs
- Domestic PEPs assessed as higher risk
- Customers from high risk jurisdictions (black and grey list)

**Requirements**
1. Obtain CDD information
2. Obtain additional information
3. Inquire on source of wealth and/or funds
4. Obtain approval from Senior Management
5. Requirements to conduct ongoing enhanced due diligence (frequency, depth etc.)
**Customer Due Diligence (CDD) – Meeting the Requirements**

**In practice, a Quick Guide….

<table>
<thead>
<tr>
<th>No.</th>
<th>Name of Clients</th>
<th>ID Info (NRIC/BRIC/Passport No.)</th>
<th>Info of beneficial owner (if client is a legal person/arrangement)</th>
<th>Nationality</th>
<th>Geographical location of business</th>
<th>Occupation / Nature of business</th>
<th>PEP Yes/No</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Info to obtain when conducting CDD
What if I cannot complete CDD process on my customer?

1. If the customer does not want to cooperate or refuses to provide information - What should a RI do?

<table>
<thead>
<tr>
<th>Potential Customers</th>
<th>Do not open the account or commence business relationship or perform transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing Customer</td>
<td>Terminate the business relationship</td>
</tr>
</tbody>
</table>

• Also, consider submitting a STR. Remember to document your rationale for submitting or not submitting the STR

2. If a RI finds a potential client to be suspicious, but believes that insistence on completing the CDD would tip-off the customer – What should a RI do?

• Proceed with the transaction, then immediately submit a STR
### Part B: Implementation of Anti Money Laundering / Counter Financing of Terrorism (AML/CFT)

*For each question please tick (\(\checkmark\)) either YES or NO.*

<table>
<thead>
<tr>
<th>NO</th>
<th>QUESTIONS</th>
<th>YES</th>
<th>NO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>CUSTOMER DUE DILIGENCE (CDD) / KNOW YOUR CUSTOMER (KYC)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>Do you <strong>conduct CDD</strong> when establishing a business relationship with your customers?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Do you <strong>identify (sight and record) and verify (make a copy)</strong> individual <strong>customers</strong> using reliable sources of independent document (e.g. Original NRIC/Passport)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Do you <strong>identify and verify</strong> customers/business counterparties that are <strong>companies/ businesses</strong> with original documents (e.g. Memorandum/ Article/ Certificate of Incorporation)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Do you <strong>identify and verify customers who are legal arrangements (e.g. trusts)</strong> with original documents (e.g. Trust Deed)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Do you identify and verify the <strong>beneficial owner</strong> of companies or legal arrangements e.g. directors of companies or trustor for legal arrangements?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Combating Financing of Terrorism

Obligations under Part VIA of the AMLA applicable to any person

1. Update and Maintain Lists
   - UNSCR 1267/1988 Consolidated List (section 66C of AMLA)
   - List under Section 66B (Domestic)
   - Other List (Optional)

2. Check on Names
   - On new customers, beneficial owners and beneficiary
   - Existing customers
   - Potential customers
   - Take measures to ascertain identity – not ‘false positive’

3. Freeze / Reject
   - Freeze/block fund for existing customers
   - Reject transactions for new/potential customers

4. Report
   - To FIED (including attempted transactions)
   - Inform relevant supervisory authority


- Database of names and particulars of listed persons in the United Nations Security Council Resolution (“UNSCR”) Consolidated List at:
  - [https://www.un.org/sc/suborg/en/sanctions/1267/aq_sanctions_list](https://www.un.org/sc/suborg/en/sanctions/1267/aq_sanctions_list); and
### COMBATING THE FINANCING OF TERRORISM

<table>
<thead>
<tr>
<th></th>
<th>Question</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td>Do you check the name of customers against the latest United Nations Security Council Terrorism Sanctions List?</td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>Do you check the name of customers against the latest Terrorism Sanctions Lists by the Minister of Home Affairs?</td>
<td></td>
</tr>
</tbody>
</table>
AML/CFT Awareness Session

AML/CFT Requirements

- CDD
- Record Keeping
- Compliance Officer
- Reporting of STR
- Risk Profiling
- Compliance Programme
Keep, Retain and Centralise Records

1. What?
   - CDD information
   - Copies of ID
   - Transaction details and documents

2. How?
   Management Information System (MIS)
   - In the form that is admissible in court
   - Not necessarily automated. Can be manual
   - To commensurate with nature, scale and complexity of operations

3. How Long?
   6 years
   From the date of the transaction completed or terminated

4. Why?
   Enable reconstruction of any transaction.
<table>
<thead>
<tr>
<th></th>
<th>RECORD KEEPING</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td>Do you make a copy and retain records of all customers' CDD information?</td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>Do you retain records of transactions?</td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>If YES, do you firm retain such record for 6 years or more?</td>
<td></td>
</tr>
</tbody>
</table>
AML/CFT Requirements

- CDD
- Record Keeping
- Compliance Programme
- Compliance Officer
- Risk Profiling
- Reporting of STR
**RIs to establish red-flags or ML/TF indicators**

**Customer Risk:**
1. Significant and unexplained geographic distance between agent and buyer
2. Unusual involvement of third parties / intermediaries
3. Structure/ nature of entity/ relationship that hide the identity of ultimate beneficial owner, true owner or controlling interest
4. Cash intensive business
5. Involvement of charities and other non-profit organisations
6. Involvement of higher risk clients such as individuals from high risk jurisdictions, foreign PEPs or domestic PEPs assessed as high risk etc.
7. Avoiding personal contact without good reason
8. Attempt by customer to maintain a high and unusual degree of secrecy

**Transaction Risk:**
1. Transactions unduly expedited without reasonable explanation
2. Successive transactions, especially of same property in short period of time with explained changes in value
3. Introduction of unknown parties at a late stage of transactions
4. Under or over-valued properties
5. Use of large amount of cash
6. High speed of transaction (without reasonable explanation)
7. Transactions where there are doubts about the validity of the documents submitted
Suspicious Transaction Report (STR): Reporting Mechanism

Internal reporting mechanism:
- RI to have in place policies on duration taken by Compliance Officer to review internal STR and circumstances the timeframe can be exceeded

Tipping Off:
- If RI has formed a suspicion of ML/TF but believes that performing CDD process would tip-off the customer, RI is permitted not to pursue CDD, to proceed with the transaction and immediately file a STR

Establish clear P&P to guide all staff, which should include:
- Guidance on the type of client behavior or transactions that could be considered as suspicious i.e. internal criteria/red-flags
- What to do when doubt arises e.g. types of further scrutiny to conduct, consider submitting STR if suspicion remains
- Who to submit STR to within the firm and where to get STR forms i.e. sample/template
- Method for submitting STRs - by staff to CO, by CO to FIED,BNM - to preserve confidentiality
- Timeframe for initial assessment by staff upon formation of doubt before raising STR to CO, assessment by CO before submitting STR to FIED, BNM
- Method for recording of assessment and decision not to submit STR received from staff and secure filing of these documents for at least 6 years.
Suspicious Transaction Report (STR): Information Required

Details of Subject Reported
- Name of Subject
- Identification No.
- Address
- Contact No.
- Employment details i.e. occupation, name of employer

Transaction Details
- Mode of transaction
- Transaction Amount
- Transaction Date

Description of Suspicious Transaction
- Reasons given by the reporting institutions on why they feel the conduct of account is suspicious

Submission Mode
Mail
Director of FIED
Bank Negara Malaysia
Jalan Dato’ Onn
50480 Kuala Lumpur
(To be opened by addressee only)

Fax
+603-2693 3625

Email
str@bnm.gov.my

Section 24: protection of persons reporting STR from disciplinary, civil and criminal actions provide STR is submitted in good faith

When in doubt, SUBMIT STR
A copy of STR form can be obtained from Appendix III of Sector 5 Policy Document @ http://amlcft.bnm.gov.my/AMLCFT05a.html
<table>
<thead>
<tr>
<th>Questions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.</td>
<td>Does your firm maintain written internal criteria (i.e. red flags) to identify transactions that are suspicious in nature?</td>
</tr>
<tr>
<td>12.</td>
<td>Does your firm maintain and establish a reporting mechanism for reporting of Suspicious Transaction Report (STR) to BNM?</td>
</tr>
<tr>
<td>13.</td>
<td>Does the reporting mechanism of STR preserve confidentiality of the report?</td>
</tr>
</tbody>
</table>
AML/CFT Awareness Session

AML/CFT Requirements

- CDD
- Record Keeping
- Compliance Programme
- Compliance Officer
- Reporting of STR
- Risk Profiling
Risk Assessment & Customer Risk Profiling

RISK ASSESSMENT

1. Customer risk
   - Resident or non-resident
   - Company or individual
   - Company structure
   - PEPs

2. Geography
   - Business location
   - Country of origin
   - Country on sanctions list
   - Etc.

3. Products, services, transactions/delivery channels
   - Cash-based
   - Non face-to-face
   - Simple/complex transactions
   - Etc.

4. Other information
   - Suggesting higher risk, if any

RISK PROFILING

RISK CONTROL AND MITIGATION
Customer Risk Profiling – Meeting the Requirements

Risk profile customer based on CDD info collected
- Examples of CDD info that can be used as risk profiling factors

<table>
<thead>
<tr>
<th>No.</th>
<th>Name of Clients</th>
<th>Nationality</th>
<th>Geographical location of business</th>
<th>Occupation / Nature of business</th>
<th>With or without Loan</th>
<th>Transaction Value (RM)</th>
<th>Mode of Payment</th>
<th>ML/TF Risk Rating e.g.: Low, Medium, High</th>
<th>Check against UNSCR List?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- i. Customer risk
- ii. Geographical risk
- iii. Risk associated with Transaction / Delivery Channel

Automatically a high risk customer when there is a positive name match

Document Client’s risk profile
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CUSTOMER RISK PROFILING</strong></td>
<td></td>
</tr>
<tr>
<td>14.</td>
<td>Do you establish parameters/guides to classify higher/lower risk customers from perspective of money laundering and terrorist financing?</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>15.</td>
<td>Do you obtain more information such as source of fund/wealth on higher risk customers?</td>
</tr>
</tbody>
</table>
AML/CFT Awareness Session

AML/CFT Requirements

- CDD
- Record Keeping
- Reporting of STR
- Risk Profiling
- Compliance Programme
- Compliance Officer
Roles & Responsibilities of Compliance Officer

High expectation on role and duty of AML/CFT Compliance Officer (CO)

1. Who
   1. Individual with management responsibilities
   2. Fit and proper
   3. Necessary knowledge and expertise

2. Duty to Ensure
   - Compliance to AML/CFT requirements
   - Appropriate AML/CFT procedures
   - Proper and effective implementation of procedures
   - Communication channel between staff and compliance is kept secured and confidential
   - Internally generated STR are evaluated before submission
   - Identification of ML/TF risk associated with new products and services
   - Staff’s awareness on AML/CFT measures

For individual RIs who operate within a group (e.g. partnership):
- responsible for own obligation under AMLA;
- may appoint particular person (with management responsibilities) within such group to perform the role of CO
<table>
<thead>
<tr>
<th>COMPLIANCE OFFICER</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>16.</strong> Does your firm have a dedicated person looking at compliance with AML/CFT requirements i.e. AML/CFT Compliance Officer?</td>
</tr>
<tr>
<td><strong>17.</strong> If YES, please provide the details of the Compliance Officer.</td>
</tr>
<tr>
<td>a) Name:</td>
</tr>
<tr>
<td>b) Contact No.:</td>
</tr>
</tbody>
</table>
## Compliance Programme

<table>
<thead>
<tr>
<th>Policies &amp; Procedures</th>
<th>Board of Directors &amp; Senior Management</th>
<th>Employee Screening</th>
<th>AML/CFT Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Commensurate with the firm’s ML/TF risks and size of business</td>
<td>• Spearhead the AML/CFT efforts and compliance</td>
<td>• Checks on employee’s personal information including employment and financial history</td>
<td>• Tailored to staff level &amp; nature of works</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Upon hiring and throughout the course of employment</td>
<td>• Frequency – correlate with level of risk</td>
</tr>
</tbody>
</table>
## OTHER REQUIREMENTS

<table>
<thead>
<tr>
<th></th>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.</td>
<td>Does your firm maintain any written policies, procedures or AML/CFT manual as a guide for employees?</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>19.</td>
<td>Does your firm conduct any AML/CFT Training/ Awareness for employees?</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>20.</td>
<td>If YES, is the training provided upon employment / recruitment?</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>21.</td>
<td>If YES, is the training provided annually?</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>
Presentation Outline

Overview of ML/TF & Malaysia’s AML/CFT Regime

ML/TF Vulnerabilities of Real Estate Sector

AML/CFT Requirements on REAs

BNM’s Supervisory Approach & Expectation
BNM’s Supervisory Expectation & Approach

Expectations

• Understand ML/TF risk which the business is exposed to
• Assess ML/TF risk profile of clients
• Implement AML/CFT compliance programme
• Appointment of Compliance Officer to oversee AML/CFT compliance matters

Understand and mitigate risks

Approach

• Conduct robust CDD/ECDD, identify BOs & conduct on-going monitoring
• Maintain records for minimum of 6 years
• Detect & report suspicious transactions
• Regular AML/CFT training for employees & employee screening
• Regular audits on effectiveness of AML/CFT compliance programme

Preventing abuse by criminals

1. Continuous engagement in increasing awareness and enhancing compliance to AML/CFT requirements
2. Off-site surveillance / monitoring by reviewing and analysing internal audit report and periodic statistical report
3. On-site examination to ensure compliance
4. Periodic review of sectoral guidelines to address key and emerging risks
AML/CFT On-site Examination – Common **Lapses Observed**

<table>
<thead>
<tr>
<th>No.</th>
<th>Areas</th>
<th>Lapses Observed</th>
<th>Ref. to AMLA / Sector 5 Policy Document</th>
</tr>
</thead>
</table>
| 1.  | Conduct of CDD and ODD                    | • Inadequate CDD conducted, whereby information obtained was limited to name, NRIC or passport number and address of client. There was no verification conducted on the client (i.e. sight and retain a copy of the identification document) in most instances.  
   • Did not conduct EDD on higher risk customers mainly due to absence of customer risk profiling. | Section 16 / Paragraph 13                  |
| 2.  | STR Reporting Mechanism                    | • Did not establish internal criteria (red-flags) to detect suspicious transactions.  
   • Did not establish reporting mechanism for suspicious transactions. | Section 19 / Paragraph 23                  |
| 3.  | Combating the Financing of Terrorism       | • Did not maintain a database of names and particulars of sanctioned individuals and entities.  
   • Did not conduct checks on the names of new and existing clients against list of sanctioned entities. | Section 66E / Paragraph 25                 |
| 4.  | ML/TF Risk Assessment and Customer Risk Profiling | • Did not conduct ML/TF risk assessment in relation to the firm’s customers, products and services, transactions or delivery channels and geographical presence.  
   • Did not conduct risk profiling of clients. | Section 19 / Paragraph 12                  |
| 5.  | AML/CFT Compliance Programme               | • Absence of written AML/CFT policies and procedures on all main areas of AML/CFT requirements.  
   • Absence of senior management oversight on AML/CFT matters.  
   • Did not appoint compliance officer to undertake compliance function for AML/CFT matters.  
   • Did not conduct AML/CFT awareness and training programmes for employees. | Section 19 / Paragraph 22                  |
## AML/CFT On-site Examination – **Good Practices Observed**

<table>
<thead>
<tr>
<th>No.</th>
<th>Areas</th>
<th>Good Practices Observed</th>
<th>Ref. to AMLA / Sector 5 Policy Document</th>
</tr>
</thead>
</table>
| 1   | Management Information System (MIS) | • Maintenance and centralisation of customers database at firm’s level despite customers were solicited by various RENs  
• Adequate MIS using both manual records and simple system to capture CDD and transaction records for accounting purpose | Sections 15 & 19 / Paragraph 12         |
| 2   | Retention of Records          | • Retention of basic CDD and transaction records for than 6 years                      | Section 19 / Paragraph 22              |
Consequence of Non-Compliance....

1. Enforcement action can be taken against a reporting institution, including directors, officers and employees for any non-compliance with AML/CFT requirements;

2. Penalties upon breaches include:
   - **General Offence** (section 86 of AMLA) – **Fine not exceeding RM1.0 million** e.g. for failure to conduct CDD, failure to submit STR and failure to adopt, develop and implement AML/CFT compliance programme;
   - **Retention of Records** (section 17 of AMLA) – **Fine not exceeding RM3.0 million or imprisonment for a term not exceeding five (5) year or both**
References & Contact Person


**BNM’s Officer-in-charge:**

- **Dr. Sarah Azlina Che Rohim**
  sarahlina@bnm.gov.my
  ext 8430
- **Mun Chooi Wan**
  chooiwan@bnm.gov.my
  03-2698 8044 ext 7129
- **Ahmad Farhan Sharifuddin**
  farhan@bnm.gov.my
  ext 8493
- **Shuhaira Shaidan**
  shuhaira@bnm.gov.my
  ext 8152
## Practical Guide on Key AML/CFT Requirements

<table>
<thead>
<tr>
<th>No.</th>
<th>What's required</th>
<th>Paragraph Reference in Sector 5 Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Appoint a <strong>Compliance officer</strong></td>
<td>• 22</td>
</tr>
<tr>
<td>2.</td>
<td>Develop and implement internal programme, policies, procedures and controls to</td>
<td>• 22</td>
</tr>
<tr>
<td></td>
<td>guard against and detect any offence under AMLA, including</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. Policies and procedures (P&amp;P) on <strong>overall ML/TF risk assessment</strong>, **client</td>
<td>• 12</td>
</tr>
<tr>
<td></td>
<td>risk profiling**, managing and mitigating risk identified, periodic update of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>risk assessment, and documentation of risk assessment and findings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. P&amp;P on <strong>customer due diligence</strong> (CDD) on customer and person conducting</td>
<td>• 13</td>
</tr>
<tr>
<td></td>
<td>transaction, enhanced due diligence (EDD) and on-going due diligence (ODD)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. Establish <strong>internal criteria</strong> (<em>red flags</em>) to detect suspicious</td>
<td>• 23</td>
</tr>
<tr>
<td></td>
<td>transactions; and establish a <strong>reporting system</strong> for assessment and submission</td>
<td></td>
</tr>
<tr>
<td></td>
<td>of suspicious transaction reports (STR) in a secure manner</td>
<td></td>
</tr>
</tbody>
</table>
## Practical Guide on Key AML/CFT Requirements

<table>
<thead>
<tr>
<th>No.</th>
<th>What’s required</th>
<th>Paragraph Reference in Sector 5 Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>When in ‘doubt’, submit STR</td>
<td>• 23</td>
</tr>
<tr>
<td>4.</td>
<td>Check new and existing client database against the UNSCR Consolidated List and gazette orders issued by MOHA on domestic list of sanctioned individuals and entities</td>
<td>• 25</td>
</tr>
<tr>
<td>5.</td>
<td>Conduct <strong>AML/CFT awareness and training programmes</strong> for employees</td>
<td>• 22</td>
</tr>
<tr>
<td>6.</td>
<td>Put in place adequate management information system (<strong>MIS</strong>) to complement CDD process</td>
<td>• 20</td>
</tr>
<tr>
<td>7.</td>
<td>Keep all CDD information and records for at least 6 years</td>
<td>• 21</td>
</tr>
<tr>
<td>8.</td>
<td><strong>Keeping ML/TF risk assessment up-to-date</strong> through periodic review, and having appropriate mechanisms to provide risk assessment information to the supervisory authority, when required</td>
<td>• 12</td>
</tr>
<tr>
<td>9.</td>
<td>Roles and responsibilities of Board of Directors</td>
<td>• 22</td>
</tr>
</tbody>
</table>