GUIDANCE NOTES ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING AND TERRORIST FINANCING IN THE CAYMAN ISLANDS

PART III

BANKS AND OTHER DEPOSIT TAKING FINANCIAL INSTITUTIONS SECTOR SPECIFIC AML/CFT GUIDANCE

The purpose of this part of the Guidance Notes is to provide some guidance specifically for the Banks and Other Deposit Taking Financial Institutions sector. The types of FSPs covered in Part III are: (1) Retail and Non-Retail Banks; (2) Credit Unions; and (3) Building Societies. This sector specific guidance addresses specialised areas of relevant financial business that require more and / or different guidance or explanation than dealt with in the general body of these Guidance Notes. PART III should be read in conjunction with Part I and Part II of the Guidance Notes and the Appendices.

SECTION 1

RETAIL BANKS AND NON-RETAIL BANKS

A. OVERVIEW

1. Section 2 of the Banks and Trust Companies Law defines "banking business" as:

> "the business of receiving (other than from a bank or trust company) and holding on current, savings, deposit or other similar account money which is repayable by cheque or order and may be invested by way of advances to customers or otherwise".

2. Banking encompasses a wide range of financial products and services, which include, but are not limited to:

   (1) Retail banking, where banks offer products and services directly to personal and business customers (including legal arrangements), such as current accounts, loans (including mortgages) and savings products;
   (2) Corporate and investment banking, where banks provide corporate finance and corporate banking products and investment services to corporations, governments and institutions;
   (3) Investment services (or wealth management), where banks provide products and services to manage their customers' wealth (sometimes referred to as private banking); and
   (4) Correspondent services, where banking services are provided by one bank (the "correspondent bank") to another bank (the "respondent bank").[1] Guidance on correspondent banking is provided in Part II of these Guidance Notes.

B. SCOPE

1. This sector specific guidance seeks to provide practical assistance to Retail Banks and Non-Retail Banks (collectively, "Banks") in complying with the AMLRs, interpreting and applying the general provisions of these Guidance Notes, and for Banks to adopt sound risk management and internal controls for their operations.

2. The AMLRs apply to Banks as indicated in the list of activities falling within the definition of "Relevant Financial Business" in the Sixth Schedule of the Law.

3. It is the responsibility of each Bank to have systems and training in place to prevent ML/TF. This means that each Bank must maintain AML/CFT policies

[1] FATF Guidance for a Risk-Based Approach – The Banking Sector (October 2014)

and procedures appropriate for the purposes of forestalling and preventing ML/TF.

C. ML/TF RISKS

1. Certain products and services offered by Banks may pose a higher risk of ML or TF depending on the nature of the specific product or service offered.

2. Such products and services may facilitate a higher degree of anonymity, or involve the handling of high volumes of currency or currency equivalents. Some of these products and services are listed below, but the list is not all inclusive:

Retail Banking

(1) The provision of services to cash-intensive businesses is a particular area of risk associated with retail banking. Some businesses are legitimately cash based and so there will often be a high level of cash deposits associated with some accounts. The risk is in failing to identify such businesses where the level of cash activity is higher than the underlying business would justify. [2]

Wealth Management

(2) Wealthy and powerful customers may be reluctant or unwilling to provide adequate documents, details and explanations. The situation with regards to these types of customers can be exacerbated where the customer occupies a high public profile, and may fall into the category of a PEP indicating that they wield or have recently wielded political or economic power or influence. Additionally, wealthy customers often have many accounts in more than one jurisdiction, either within the same firm or group, or within different firms, which may be more difficult for wealth managers to accurately assess the true purpose and business rationale for individual transactions. [3]

Correspondent Banking

(3) The correspondent bank often has no direct relationship with the underlying customers of the respondent bank and therefore may have limited information on a transaction and may not be in a position to verify their identities. Correspondent banks often have limited information regarding the nature or purpose of the underlying transactions, particularly when processing electronic payments. Correspondent banking relationships, if poorly controlled, can allow other financial services firms with inadequate AML/CFT systems and

[2 - 4] The Joint Money Laundering Steering Group – Prevention of money laundering/combating terrorist financing – Guidance for the UK Financial Sector Part II Sectoral Guidance (Amended November 2014)

controls, and customers of those firms[4], direct access to international banking systems.

Lending

(4) The main ML/TF risk arises through the acceleration of an agreed repayment schedule, either by means of lump sum payments, or early termination. Additionally, the involvement of multiple parties may increase the risk of ML/TF when the source and use of the funds are not transparent. This lack of transparency can create opportunities in any of the three stages of ML/TF financing schemes.

Payable Through Accounts ("PTA")

(5) PTA may be prone to higher risk because banks may not implement the same due diligence requirements for PTAs that they require of other customers who want to open checking and other accounts. These banks then process thousands of sub-accountholder cheques and other transactions, including currency deposits, through the foreign financial institution's PTA. In most cases, little or no independent effort is expended to obtain or confirm information about the individual and business sub-accountholders that use the PTAs. The potential for facilitating ML or TF and other serious crimes increases when a bank is unable to identify and adequately understand the transactions of the ultimate users of its account with a foreign correspondent.[5]

Trade Financing

(6) The international trade system is subject to a wide range of risks and vulnerabilities that provide criminal organizations with the opportunity to launder the proceeds of crime and move funds to terrorist organizations with a relatively low risk of detection. The involvement of multiple parties on both sides of any international trade transaction can make the process of due diligence more difficult. Also, due to the fact that trade finance can be more document-based than other banking activities, it can be susceptible to documentary fraud, which can be linked to ML/TF. While banks should be alert to transactions involving high-risk goods (e.g., trade in weapons or nuclear equipment), they need to be aware that any good may be over or under-valued in an effort to evade AML/CFT or customs regulations, or to move funds or value across national borders. [6]

[4] Financial institutions with poor AML/CFT systems are vulnerable to ML/TF risks and could be misused by the money launderers.

[5] Bank Secrecy Act Anti-Money Laundering Examination Manual – Payable Through Accounts - Overview

[6] Bank Secrecy Act Anti-Money Laundering Examination Manual – Trade Finance Activities - Overview

D. RISK BASED APPROACH

1. Banks must adopt a risk-based approach to managing ML/TF risks. The risk based approach to AML/CFT aims to support the development of prevention and mitigation measures that are commensurate to the ML/TF risks identified. This applies to the way banks allocate their compliance resources, organize their internal controls and internal structures, and implement policies and procedures to deter and detect ML/TF.

2. The bank's risk assessment forms the basis of a bank's RBA. In identifying and assessing the ML/TF risk to which they are exposed, Banks should consider a range of factors which may include[7]:

   (1) The nature, scale, diversity and complexity of their business;
   (2) Target markets;
   (3) The number of customers already identified as high risk;
   (4) The jurisdictions the bank is exposed to, either through its own activities or the activities of customers, especially jurisdictions with relatively higher levels of corruption or organised crime;
   (5) The distribution channels, including the extent to which the bank deals directly with the customer or the extent to which it relies (or is allowed to rely on) third parties to conduct CDD and the use of technology;
   The internal audit and regulatory findings; and
   (6) The volume and size of its transactions, considering the usual activity of the bank and the profile of its customers.

E. CUSTOMER DUE DILIGENCE

Who is the Customer/Applicant for Business?

1. The applicant may be any one of the following:
   (1) Natural persons;
   (2) Corporate persons (including MSBs, other deposit taking financial institutions, trust and fiduciary customers, companies); and
   (3) Partnerships / Unincorporated Businesses.

2. The following are the applicants whose identity must be verified by Banks and the evidence of identity required in each case:

Applicant for Business	CDD Requirements (Highlights and supplementary only– please refer to section 4 of Part II of the Guidance Notes for the full (normal) CDD requirements).
Natural Persons	(1) CDD documentation to identify and verify that identity should be obtained for the customer and, where appropriate, beneficial owner(s) of accounts.

[7] FATF - Risk-based approach guidance for the banking sector

	(2) Satisfactory evidence of identity, name and address confirmed by using one or more of the verification methods outlined in section 4 of Part II of the Guidance Notes. (3) Information, including necessary documentation required to understand the purpose and intended nature of the business relationship as outlined in section 4 of Part II of the Guidance Notes. **Note:** As stated in paragraph 16, Section 4, Part II of these Guidance Notes, it is usually not sufficient to rely on one document or data source and the extent of documentation and data that an FSP needs to collect depends on the risk assessment of the customer. FSPs must also be aware that some documents are more easily forged than others. Banks should supplement their verification documentation with references from other FSPs that are banks as below. (4) Current, satisfactory bank reference from at least one bank with whom the prospective customer has had a relationship for not less than 3 years. If one is not forthcoming, satisfactory reference from a person or entity who has personal knowledge of the prospective customer and which establish his bona fides and integrity. References confirmed for genuineness. Genuineness may be confirmed by directly contacting the referee either via email or telephone. (5) For non-face-to-face verification, suitably certified or authenticated documents. **Note:** Given the international nature of banking business in and from the Cayman Islands, Bank FSPs should also be particularly vigilant in ensuring that CDD documentation collected that are in a foreign language are appropriately translated **and** verified and the copy of the translation kept with the original document. (6) Evidence of identity required for assets bought, sold or managed through the relationship
Corporate customers (including MSBs, other deposit taking financial institutions, trust and fiduciary customers, companies)	(1) CDD as set out in Part II Section 4. N.B. Paragraphs 14 to 17 and 42 to 49 (of Part II Section 4).. (2) Consistent with that required for natural persons, documentary evidence of identity for all directors that are natural persons; all those with signing powers, including third parties; and beneficial owners. (See section 4 of Part II in the Guidance Notes). (3) Documentary evidence of identity of the new owner/controller where there is a change in ownership or control, in accordance with that required of natural persons.

Partnerships / Unincorporated Businesses	(1) Identification information and satisfactory evidence of its existence, confirmed by at least one of the following independent checks, of existence of partnership / unincorporated business: (a) Partnership agreement or excerpt if relevant (b) Certificate of Registration (if applicable); (2) Consistent with that required for direct personal customers, documentary evidence of identity required for partners/managers; all those with signing powers; all relevant parties, including third parties; and controlling partners / shareholders/beneficial owners as defined in the Guidance Notes, Section 4 (e.g., excerpt from partnership document. (3) Documentary evidence of identity of the new owner/controller where there is a change in ownership or control, in accordance with that required of direct personal relationships.

When must identify be verified?

3. Customer verification information must be obtained and verification should be conducted prior to opening the account or establishing the business relationship.

4. Where the verification information is not forthcoming at the outset or within a reasonable time after initial contact, the relationship must be re-evaluated and transactions must not proceed.

When might it be possible to rely on third-parties to verify identity?

5. Banks should use their judgment in determining whether or not in the context of banking they should place reliance on third parties for conducting the due diligence procedures (verification). However, such reliance should only be considered in situations where the ML/TF risks have been assessed as low and where there is no suspicion of ML/TF.

6. Refer to section 5 of the Part II of the Guidance Notes, for guidance on SDD and "Procedure for Introduced Business".

F. ENHANCED DUE DILIGENCE ("EDD")

7. In case of high-risk situations/customers, the bank has to conduct EDD. Customers that pose high ML or TF risks present increased exposure to banks; in such cases, banks should apply EDD. EDD for high-risk customers is especially critical in understanding their anticipated transactions and implementing a suspicious activity monitoring system that reduces the bank's reputation, compliance, and transaction risks. High-risk customers and their

transactions should be reviewed more closely and more frequently throughout the term of their relationship with the bank.

8. NPOs (including Charities), PEPs, Correspondent Banking, Trade Financing and customers in High-Risk Countries are some factors to consider which may result in EDD. Additional examples would include cases whereby a customer is confidentiality-driven, or presents a multi-layered structure of beneficial ownership.

9. In applying EDD, banks may for example collect sufficient information regarding intra-group relationships, if any; types of customers; service providers; and trading partners to establish a trading profile which can be monitored against transactions. More examples of enhanced CDD measures are provided in section 6, Part II of the Guidance Notes.

G. ON-GOING MONITORING

1. Banks should conduct on-going monitoring of the business relationship. On-going monitoring includes the scrutiny of transactions to determine whether those transactions are consistent with the Bank's knowledge of the customer and the nature and purpose of the business relationship. Monitoring also involves identifying changes to the customer profile and keeping it up to date, which may require the application of new, or additional CDD measures. Monitoring transactions is an essential component in identifying transactions/activities that are potentially suspicious.

2. Monitoring should be carried out on a continuous basis or triggered by specific transactions. It could also be used to compare a customer's activity with that of a peer group. For some types of banking activity where large volumes of transactions occur on a regular basis, automated systems may be the only realistic method of monitoring transactions. However, where automated systems are used, banks should understand their operating rules, verify their integrity on a regular basis and check that they address the identified ML/TF risks.

3. Banks should adjust the level of monitoring in line with their institutional risk assessment and individual customer risk profiles. Enhanced monitoring should be required for high risk situations. The adequacy of monitoring systems and the factors leading banks to adjust the level of monitoring should be reviewed regularly for continued relevance to the bank's AML/CFT risk programme.[8]

4. Refer to section 4 of the Part II of the Guidance Notes, "On-Going Monitoring of Business Relationships", for additional guidance.

[8] FATF Guidance for a Risk-Based Approach – The Banking Sector (October 2014)

H. ML/TF WARNING SIGNS OR "RED FLAGS"

1. The following are examples of potentially suspicious activities or "red flags" for ML/TF. Although these lists are not all-inclusive, they may help banks recognize possible ML/TF schemes. The below red flags, when encountered, may warrant additional scrutiny. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny will assist in determining whether the activity is unusual/suspicious or one for which there does not appear to be a reasonable business or legal purpose.

Transactions Involving Large Amounts of Cash

2. The following are some of the warning signs and red flags that Banks should be alert to in respect of transactions. The list is not exhaustive, but includes:

(1) Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity.

(2) Frequent withdrawal of large amounts by means of cheques, including traveller's cheques.

(3) Customers making large and frequent cash deposits but cheques drawn on the accounts are mostly to individuals and firms not normally associated with their business.

(4) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.

(5) A large amount of cash is withdrawn and immediately deposited into another account.

(6) Exchanging an unusually large amount of small-denominated notes for those of higher denomination.

(7) Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank.

(8) Company transactions, both deposits and withdrawals, that are denominated by unusually large amounts of cash, rather than by way of debits and credits normally associated with the normal commercial operations of the company (e.g. cheques, letters of credit, bills of exchange).

(9) Depositing cash by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the cumulative total of which is substantial.

(10) The deposit of unusually large amounts of cash by a customer to cover requests for bankers' drafts, money transfers or other negotiable and readily marketable money instruments.

(11) Aberrant customer transactions of large cash deposits using cash deposit machines or similar facilities, thereby avoiding direct contact with the bank.

(12) Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.

(13) Customers whose deposits contain counterfeit notes or forged instruments.

(14) Customers who use cash advances from a credit card or charge card account to purchase money orders or bank drafts to transfer funds to foreign destinations.

(15) Customers who take cash advances from a credit card or charge card account to deposit into another account.

(16) Large cash payments for outstanding credit card or charge card balances.

(17) Customers who maintain positive balances on their credit card or charge card and then request cash advances or other type of refunds.

Transactions Involving Transfers Abroad

3. The following are some of the warning signs and red flags that Banks should be alert to in respect of transactions involving cross-border transfers. The list is not exhaustive, but includes:

(1) Large and regular payments that cannot be clearly identified as bona fide transactions, from and to countries or jurisdictions that are high-risk, which include jurisdictions that are associated with (a) the production, processing or marketing of narcotics or other illegal drugs or (b) terrorism or related criminal conduct.

(2) Substantial increase in cash deposits by a customer without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account or to a destination not normally associated with the customer.

(3) Repeated transfers of large amounts of money abroad accompanied by the instruction to pay the beneficiary in cash.

(4) Building up large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas.

(5) Cash payments remitted to a single account by a large number of different persons without an adequate explanation.

(6) "U-turn" transactions, i.e. where funds received from a person or company in a foreign country or jurisdiction are immediately remitted to another person or company in the same country or foreign jurisdiction, or to the sender's account in another country or jurisdiction.

Electronic Payments

1. The following are some of the warning signs and red flags that Banks should be alert to in respect of electronic payments. The list is not exhaustive, but includes:

(1) Electronic payments ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.

(2) Electronic payments to or for an individual where information on the originator, or the person on whose behalf the transaction is conducted, is not provided with the wire transfer, when the inclusion of such information would be expected.

(3) Use of multiple personal and business accounts or the accounts of NPOs to collect and then funnel funds immediately or after a short time to a small number of foreign beneficiaries.

(4) Foreign exchange transactions that are performed on behalf of a customer by a third party followed by electronic payments of the funds to locations having no apparent business connection with the customer or to countries of ML/TF concern.

Lending

5. The following are some of the warning signs and red flags that Banks should be alert to in respect of lending. The list is not exhaustive, but includes:

(1) Loans secured by pledged assets held by third parties unrelated to the borrower.

(2) Loans secured by deposits or other readily marketable assets, such as securities, particularly when owned by apparently unrelated third parties.

(3) Borrower defaults on cash-secured loan or any loan that is secured by assets that are readily convertible into currency.

(4) Loans are made for, or are paid on behalf of, a third party with no reasonable explanation.

(5) To secure a loan, the customer purchases a certificate of deposit using an unknown source of funds, particularly when funds are provided via a currency or multiple monetary instruments.

(6) Loans that lack a legitimate business purpose, provide the bank with significant fees or assuming little or no risk, or tend to obscure the movement of funds (e.g., loans made to a borrower and immediately sold to an entity related to the borrower or back to back loans without any identifiable and legally admissible purpose).

Trade Finance

6. The following are some of the warning signs and red flags that Banks should be alert to in respect of trade finance. The list is not exhaustive, but includes:

(1) Items shipped that are inconsistent with the nature of the customer's business (e.g., a steel company that starts dealing in paper products, or an information technology company that starts dealing in paper products).

(2) Customers conducting business in high-risk jurisdictions.

(3) Customers shipping items through high-risk jurisdictions.
(4) Customers involved in potentially high-risk activities, including activities that may be subject to export/import restrictions.
(5) Obvious over or under pricing of goods and services.
(6) Obvious misrepresentation of quantity or type of goods imported or exported.
(7) Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.
(8) Customer requests payment of proceeds to an unrelated third party.
(9) Shipment locations or description of goods not consistent with letter of credit.
(10) Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment.

Employee Activity

7. The following are some of the warning signs and red flags that Banks should be alert to activities of their own employees. The list is not exhaustive, but includes:
   (1) Employee lives a lavish lifestyle that cannot be supported by his salary.
   (2) Employee fails to adhere to bank's internal policies, procedures, and processes and frequently overrides internal controls.
   (3) Employee is reluctant to take a vacation.

SECTION 2

CREDIT UNIONS

A. CREDIT UNIONS

1. Section 2 of the Cooperative Societies Law defines "credit union business", in relation to a registered society (i.e., a society that, among other criteria, has as its object the promotion of the economic interest of its members in accordance with cooperative principles), as:

   "The business of –
   (1) promoting thrift among the members of the society by the accumulation of their savings;
   (2) creating sources of credit for the benefit of the members of the society at a fair and reasonable rate of interest;
   (3) using and controlling the members' savings for their mutual benefit; and
   (4) training and educating the members in the wise use of money and in the management of their financial affairs.

B. SCOPE

1. This sector specific guidance seeks to provide practical assistance to credit unions in complying with the AMLRs, interpreting and applying the general provisions of these Guidance Notes, and for credit unions to adopt sound risk management and internal controls for their operations.

2. The AMLRs apply to credit unions as indicated in the list of activities falling within the definition of "Relevant Financial Business" in the Sixth Schedule of the Law.

3. It is the responsibility of each credit union to have systems and training in place to prevent ML/TF. This means that each credit union must maintain identification procedures, record-keeping procedures, and such other procedures and controls appropriate for the purposes of forestalling and preventing ML/TF.

C. ML/TF RISKS

1. Credit unions should consider all relevant risk factors at the sectorial and business relationship levels in conducting risk assessments and determining the appropriate level of mitigating measures to be applied.

2. Risk factors related to credit union business activities include, but are not limited to:

(1) Money transfers to third parties;
(2) Third parties paying in cash on behalf of the member;
(3) Unusual loan or savings patterns (including regular significant payments);
(4) Reluctance to provide documentary evidence of identity when joining;
(5) Large One-Off transactions – e.g. sudden loan repayment; and
(6) Regular requests for loans that are soon repaid.

D. RISK BASED APPROACH

1. Credit unions must adopt a risk-based approach to managing ML/TF risks. The risk based approach to AML/CFT aims to support the development of prevention and mitigation measures that are commensurate to the ML/TF risks identified.

2. The credit union needs to take a number of steps, documented in a formal policy which assesses the most effectual and proportionate way to manage ML and TF risks. These steps are:
   (1) Identify the ML and TF risks that are relevant to the credit union;
   (2) Assess the risks presented by the credit unions':
      (a) Members
      (b) Products
      (c) Delivery channels
   (3) Design and implement controls to manage and mitigate these assessed risks; and
   (4) Monitor and improve the effective operation of these controls.

E. CUSTOMER DUE DILIGENCE ("CDD")

Who is the Applicant for Business?

1. The applicant for business is a natural person.

2. The following are the applicants whose identity must be verified by credit unions and the evidence of identity required in each case:

	Applicant for Business	Requirements
1.	Natural Persons	(1) Identification documentation should be obtained for the customer and beneficial owners of accounts. (2) Evidence of identity required for assets bought, sold or managed through the relationship. (3) Satisfactory evidence, confirmed by using one or more of the verification methods outlined in section 4 Part II of the Guidance Notes. (4) Current, satisfactory bank reference from at least one bank with whom the prospective customer has had a relationship for not less than 3 years. If one

		is not forthcoming, satisfactory reference from a person or entity who has personal knowledge of the prospective customer and which establish his bona fides and integrity. (5) References confirmed for genuineness. This can be achieved by email or telephone confirmations. (6) For non face to face verification, suitably certified or authenticated documents.

When must identity be verified?

3. A credit union must obtain identity information prior to accepting a person's application to become a member.

F. ENHANCED DUE DILIGENCE ("EDD")

4. It is recommended that EDD be applied in situations where the credit union is exposed to high risks. There will be certain occasions where EDD will be required, for example:

   (1) when there is no face-to-face contact with the member;
   (2) where the member is a PEP; and
   (3) when the member is involved in a business that is considered to present a high ML/TF risk.

5. With respect to EDD measures, refer to recommendations made and examples provided in Part II of the Guidance Notes.

G. ON-GOING MONITORING

1. Credit unions must establish a process for monitoring member transactions and activities, which will highlight unusual transactions and those which need further investigation. It is important to take into account the frequency, volume and size of transactions. The key elements to monitoring are having up-to-date member information on the basis of which it will be possible to recognize the unusual transaction, and to ask pertinent questions to elicit the reasons for unusual transactions.

2. Refer to section 4 of Part II of the Guidance Notes, "On-Going Monitoring of Business Relationships".

H. ML/TF WARNING SIGNS OR "RED FLAGS"

1. The following are examples of potentially suspicious activities or "red flags" for ML/TF. Although these lists are not all-inclusive, they may help credit unions recognize possible ML/TF schemes. The below red flags, when encountered, may warrant additional scrutiny. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny will assist in determining whether the activity is unusual/suspicious or one for which these does not appear to be a reasonable business or legal purpose.

Customer Behaviour

2. The following are some of the warning signs and red flags that Credit Unions should be alert to in respect of customer behaviour. The list is not exhaustive, but includes:
   (1) Member uses unusual or suspicious identification documents, or refuses to produce originals for verification.
   (2) Member refuses to provide personal background information when opening an account.
   (3) Member's permanent address is outside of the credit union's service area.
   (4) Member indicates that he/she does not want a statement of account or any mail sent to his/her address.
   (5) A member is reluctant to provide information about the nature and purpose of the member's business or expected account activity.
   (6) Member asks about record-keeping or reporting requirements.
   (7) Member discourages employee from filing required reports or complying with recordkeeping requirements.
   (8) Member reluctant to proceed with cash transaction after being told it must be reported.

Cash Transactions

3. The following are some of the warning signs and red flags that Credit Unions should be alert to in respect of cash transactions. The list is not exhaustive, but includes:
   (1) Member regularly uses ATMs to make several deposits below the reporting threshold.
   (2) Member comes in with another member and they go to different tellers to conduct currency transactions under the reporting threshold.
   (3) Member opens different accounts under different names, and then makes several cash deposits under the reporting threshold.
   (4) Member deposits cash into several accounts in amounts below the reporting threshold and subsequently transfers the funds into one account and wire transfers them overseas.
   (5) Member attempts to take back a portion of the proposed cash deposit after learning that the proposed cash deposit exceeds the reporting threshold.

(6) Member makes numerous purchases of monetary instruments with cash in amounts less than the reporting threshold.

(7) Member purchases a number of prepaid cards for large amounts, inconsistent with normal account activity.

Credit Transactions

4. The following are some of the warning signs and red flags that Credit Unions should be alert to in respect of credit transactions. The list is not exhaustive, but includes:

(1) Member suddenly pays down or pays off a large loan with no credible explanation as to where the funds came from.

(2) Member purchases certificates of deposit and uses them as loan collateral.

(3) Loans are made for, or paid on behalf of, a third party with no plausible explanation.

(4) Member's loan proceeds are unexpectedly transferred offshore or member requests that loan proceeds be wire transferred.

Employee Activity

5. The following are some of the warning signs and red flags that Credit Unions should be alert to in respect of employee activity. The list is not exhaustive, but includes:

(1) Employee lives a lavish lifestyle that cannot be supported by his salary.

(2) Employee fails to adhere to credit union's internal policies, procedures, and processes and frequently overrides internal controls.

(3) Employee is reluctant to take a vacation.

SECTION 3

BUILDING SOCIETIES

A. BUILDING SOCIETIES

1. A Building Society is a financial institution that provides banking and other financial services to its members (i.e. the people who invest in savings schemes and those who hold mortgages and other accounts with them). Building societies offer banking and related financial services, especially savings and mortgage lending.

B. SCOPE

1. This sector specific guidance seeks to provide practical assistance to Building Societies in complying with the AMLRs, interpreting and applying the general provisions of these Guidance Notes, and for Building Societies to adopt sound risk management and internal controls for their operations.

2. The AMLRs apply to Societies as indicated in the list of activities falling within the definition of "Relevant Financial Business" in the Sixth Schedule of the Law.

3. It is the responsibility of each building society to have systems and training in place to prevent ML/TF. This means that each building society must maintain identification procedures, record-keeping procedures, and such other procedures and controls appropriate for the purposes of forestalling and preventing ML/TF.

C. ML/TF RISKS

1. Building societies should consider all relevant risk factors at the sectorial and business relationship levels in order to assess the ML/TF risks and determine the appropriate level of mitigating measures to be applied.

2. Risk factors related to building society business activities include, but are not limited to:
   (1) Third parties paying in cash on behalf of the member;
   (2) Unusual loan or savings patterns (including regular significant payments);
   (3) Reluctance to provide documentary evidence of identity when joining;
   (4) Large One-Off transactions – e.g. sudden loan repayment; and
   (5) Regular requests for loans that are soon repaid.

D. RISK BASED APPROACH

1. Building societies must adopt a risk-based approach to managing ML/TF risks. The risk based approach to AML/CFT aims to support the development of

prevention and mitigation measures that are commensurate to the ML/TF risks identified.

2. The building society needs to take a number of steps, documented in a formal policy which assesses the most effectual and proportionate way to manage ML and TF risks. These steps are:
   (1) Identify the ML and TF risks that are relevant to the building society;
   (2) Assess the risks presented by the building societies':
      (a) Members
      (b) Products
      (c) Delivery channels
      (d) Geographical areas of operation
   (3) Design and implement controls to manage and mitigate these assessed risks; and
   (4) Monitor and improve the effective operation of these controls.

E. CUSTOMER DUE DILIGENCE

Who is the applicant for business?

1. The applicant may be any one of the following:
   (1) Natural persons;
   (2) Corporate persons (including MSBs, companies); and
   (3) Partnerships / Unincorporated Businesses.

2. The following are the applicants for business whose identity must be verified by building societies and the evidence of identity required in each case:

	Applicant for Business	**Requirements**
	Natural Persons	(1) Identification documentation should be obtained for the customer and beneficial owners of accounts. (2) Evidence of identity required for assets bought, sold or managed through the relationship. (3) Satisfactory evidence, confirmed by using one or more of the verification methods outlined in section 4 of the Guidance Notes. (4) Current, satisfactory bank reference from at least one bank with whom the prospective customer has had a relationship for not less than 3 years. If one is not forthcoming, satisfactory reference from a person or entity who has personal knowledge of the prospective customer and which establish his bona fides and integrity. (5) References confirmed for genuineness. Genuineness may be confirmed by directly contacting the referee either via email or telephone. (6) For non face to face verification, suitably certified or authenticated documents.

	Corporate customers (including MSBs, companies)	(a) CDD as set out in Part II Section 4. N.B. Paragraphs 14 to 17 and 42 to 49 (of Part II Section 4).. (b) Consistent with that required for natural persons, documentary evidence of identity for all directors that are natural persons; all those with signing powers, including third parties; and beneficial owners. (See section 4 of Part II in the Guidance Notes). (c) Documentary evidence of identity of the new owner/controller where there is a change in ownership or control, in accordance with that required of natural persons.
	Partnerships / Unincorporated Businesses	(1) Identification information and satisfactory evidence of its existence, confirmed by at least one of the following independent checks, of existence of partnership / unincorporated business: (a) Partnership agreement or excerpt if relevant (b) Certificate of Registration (if applicable); (2) Consistent with that required for direct personal customers, documentary evidence of identity required for partners/managers; all those with signing powers; all relevant parties, including third parties; and controlling partners / shareholders/beneficial owners as defined in the Guidance Notes, Section 4 (e.g., excerpt from partnership document. (3) Documentary evidence of identity of the new owner/controller where there is a change in ownership or control, in accordance with that required of direct personal relationships.

When must identity be verified?

3. A building society must obtain identity information prior to accepting a person's application to become a member.

4. Where the verification information is not forthcoming at the outset or within a reasonable time after initial contact, the relationship must be re-evaluated and transactions must not proceed.

When might it be possible for identity to be verified by a party not based in the Cayman Islands?

5. Where the building society is relying on another entity within its group to verify the identity of a member who may not be physically present in the jurisdiction, all documentation must be certified by a senior manager within the group entity and copies provided prior to any outward transaction.

F. ENHANCED DUE DILIGENCE ("EDD")

6. It is recommended that EDD be applied in situations where the building society is exposed to high ML/TF risks. There will be certain occasions where EDD will be required, for example:

   (1) when there is no face-to-face contact with the member;
   (2) where the member is a PEP; or
   (3) when the member is involved in or is a business that is considered to present a high risk for ML/TF.

7. In applying EDD the building society may for example, collect sufficient information regarding intra-group relationships, if any; types of customers; service providers; and trading partners to establish a trading profile which can be monitored against transactions. More examples of enhanced CDD measures are provided in section 6, Part II of the Guidance Notes.

G. ON-GOING MONITORING

1. Building societies must conduct on-going monitoring of the business relationship with its members. On-going monitoring of a business relationship includes:
   (1) Scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions are consistent with the building society's knowledge of the member, his/her business and risk profile;
   (2) Ensuring that the documents, data or information held by the building society are kept up to date and relevant.

2. Monitoring member activity is useful in identifying unusual/suspicious transactions/activities. On-going monitoring helps to adjust the mitigating measures proportionate to the risks and apply appropriate CDD measures.

3. Refer to section 4 of Part II of the Guidance Notes, "On-Going Monitoring of Business Relationships", for additional guidance.

H. ML/TF WARNING SIGNS OR "RED FLAGS"

1. The following are examples of potentially suspicious activities or "red flags" for ML/TF. Although these lists are not all-inclusive, they may help building societies recognize possible ML/TF schemes. The below red flags, when encountered, may warrant additional scrutiny. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny will assist in determining whether the activity is suspicious or one for which these does not appear to be a reasonable business or legal purpose.
   (1) A member provides minimal, vague or fictitious information that cannot be easily verified.
   (2) Frequent deposits or withdrawals of large amounts of cash with no apparent business source, or the business is of a type not known to generate substantial amounts of cash.
   (3) Accounts with a high volume of activity, which carry low balances or are frequently overdrawn.
   (4) A member makes large deposits and maintains large balances with little or no apparent justification.
   (5) A sudden, unexplained increase in account activity, both from cash and non-cash items. An account may be opened with a nominal balance that subsequently increases rapidly and significantly.
   (6) Reluctance to provide the purpose of the loan, or the stated purpose is ambiguous.
   (7) Inappropriate disbursement of loan proceeds, or disbursements for purposes other than the stated loan purpose.
   (8) A member suddenly pays down or pays off a large loan, with no evidence of refinancing or other explanation.
   (9) Loans are made for, or are paid on behalf of, a third party with no reasonable explanation.
   (10) Loans secured by pledged assets held by third parties unrelated to the borrower.
   (11) Loans that lack a legitimate business purpose.

<u>Employee Activity</u>

2. The following are some of the warning signs and red flags that Building Societies should be alert to in respect of employee activity. The list is not exhaustive, but includes:

   (1) Employee lives a lavish lifestyle that cannot be supported by his salary.
   (2) Employee fails to adhere to the FSP's internal policies, procedures and processes and frequently overrides internal controls.
   (3) Employee is reluctant to take a vacation.