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

PART VII

MONEY SERVICES BUSINESS, OTHER REGULATED FINANCIAL INSTITUTIONS & UNSUPERVISED LENDERS SECTOR SPECIFIC AML/CFT GUIDANCE NOTES

The purpose of this part of the Guidance Notes is to provide some guidance specifically for the Money Services Business Sector, the Cayman Islands Development Bank ("CIDB") and Un-supervised Lenders. This guidance (Part VII) covers MSB sector in section 1 and CIDB in section 2 and un-supervised lending activity in section 3. This Part VII should be read in conjunction with Part I, Part II and the Appendices of the Guidance Notes.

SECTION 1

MONEY SERVICES BUSINESS

A. OVERVIEW

1. Section 2 of the Money Services Law (2010 Revision) defines "money services business" (MSB) as-

   (1) the business of providing (as a principal business) any or all of the following services-
   - (a) money transmission;
   - (b) cheque cashing;
   - (c) currency exchange;
   - (d) the issuance, sale or redemption of money orders or traveller's cheques; and
   - (e) such other services as the Governor in Council may specify by notice published in the Gazette; or

   (2) the business of operating as an agent or franchise holder of a business mentioned in paragraph (1).

2. Money transmission business can be described as the business of accepting funds for their transmission to persons in another country or domestic location. MSBs cater primarily to the resident domestic market, in particular, the expatriate workers of lower income.

3. The cash-intensive nature of the industry raises potential ML/TF concerns. The money remittance sector has challenges accessing banking services, which is an increasing global trend. The lack of access to traditional banking services may increase the level of vulnerability.

4. Typically, users of money remittance services are individuals, expatriate workers and smaller entities that send cash to other individuals thereby bypassing a traditional bank. The speed with which transactions occur can help individuals dispose of illicit proceeds instantaneously. Cross border fund flows also increase the risk of illicit funds being introduced into the Cayman Islands economy/financial system. With the Cayman Islands being a major cruise destination, employees of the cruise lines are known to be users of the remittance system, although this would be a miniscule population.

B. SCOPE

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

2. The AMLRs apply to MSBs as indicated in the list of activities falling within the definition of "Relevant Financial Business" in the Sixth Schedule of the Law. This section should be read in conjunction with Part I and II of these Guidance Notes.

3. It is the responsibility of each MSB to have systems and training in place to prevent ML/TF. Each MSB must maintain adequate AML/CFT systems which include CDD measures, record-keeping procedures, and such other procedures and controls appropriate for the purposes of forestalling and preventing ML/TF.

C. ML/TF RISKS

1. The fleeting relationship with their customers makes MSBs vulnerable to ML/TF. A person would typically have to be a customer with an account at a bank, for example, to be able to access the services of that bank, whereas a person does not have that type of relationship with the MSB and can repeatedly use different MSBs to transact business. The money transmission part of the MSB is particularly vulnerable, given the high volume of cash handled on a daily basis and the ability to transmit funds instantly to any part of the globe.

2. While the international remittance system is typically used by expatriate workers to send a part of their earnings back home, it can also be used to transmit the illegal proceeds of criminal activities and thereby poses ML/TF risk. The rapid movement of funds across multiple jurisdictions presents a challenge to investigators, particularly if the identity of the originator is unclear. For this reason, international standards have been developed with respect to payer (and payee) information that should accompany wire transfers to mitigate the above-mentioned risk.

3. Cheque cashing is another important segment of the business for some MSBs. MSBs should be aware that endorsed third party cheques from overseas are a ML/TF risk. Even where a Cayman Islands cheque, endorsed by a third party, is presented to the MSB for cashing, the MSB should take appropriate steps to ascertain the economic purpose behind the endorsement to that person presenting the cheque. Large value cheques originating from unknown individuals present a greater ML/TF risk compared to small cheques originating from well-established businesses. MSBs must have board approved AML/CFT policies and procedures that give staff clear guidance in dealing with these situations.

4. Currency exchange is another important segment of the business for some MSBs. MSBs who offer this type of service must have policies and procedures specific to the risks posed by this activity.

D. RISK BASED APPROACH

1. MSBs should adopt a risk-based approach to manage and mitigate ML/TF risks. In so doing, in addition to assessing risks inherent to their business,

MSBs should develop risk profiles of their customers, thereby familiarising themselves to customers' personal or business needs for the services provided.

2. While conducting risk assessments, MSBs should take into consideration the factors such as-

   (1) the types of products and services that they offer;

   (2) their customer types (customer occupation or type of business operated);

   (3) the geographical location of customers or where funds are transmitted; and

   (4) the average cash value of typical transactions and the $15,000 customer identification threshold as per the AMLRs.

3. As much as possible, MSBs should use computer technology to conduct the risk assessment. As provided in Part II of these Guidance Notes, customers, products, geography and services should be ranked (for example as "high," "medium," or "low" risk). For instance, the transfer of a part of an expatriate worker's weekly wage to his/her family in his/her home country should be less risky compared to the transmission of a large sum by a visitor to numerous recipients.

4. High risk customers, products, geographical regions and services should be subject to EDD and transaction monitoring. The risk model should be documented, with its rationale clearly stated, and should be updated on a regular basis to keep in line with changes in the business, customer profile or the ML/TF risks. See detailed guidance provided in section 3 of Part II of these Guidance Notes..

E. CUSTOMER DUE DILIGENCE

1. MSBs shall adopt sound customer due diligence policies and procedures. Requiring appropriate due diligence information and documentation, verifying the information, and being alert to unusual or suspicious transactions can help an MSB deter and detect ML/TF schemes.

2. A customer identification and verification policy tailored to the operations of a particular business:

   (a) helps detect unusual/suspicious activity in a timely manner;

   (b) promotes compliance with the relevant laws, regulations and guidance;

   (c) promotes safe and sound business practices;

   (d) minimises the risk that the MSB will be used for ML/TF and other criminal activities and as a result reduces the risk of government seizure and forfeiture of funds associated with customer transactions (such as outstanding money orders/traveller's cheques and outstanding money transfers); and

(e) protects the reputation of the MSB and reduces or minimises the risk of de-risking.

Whose Identity must be verified?

3. The applicant may be an individual, a corporate customer, a partnership or an unincorporated business.

4. The MSB must have documented steps that are utilized to distinguish between someone who is acting on his own behalf and someone who is acting on behalf of another (money mules/straw men). If it is determined that the person is acting on behalf of another, then the procedures for verifying the identity of the ultimate applicant must apply (see section 4 of Part II of these Guidance Notes).

5. All applicants for business undertaking money transmission via electronic funds transfer, in which case MSBs must comply with the requirements set out for wire transfers as specified in section 11 of Part II of the Guidance Notes and in the AMLRs. (Regulations in Part X of the AMLRs apply to transfers of funds which means "any transaction carried out on behalf of a payer through a payment service provider by electronic means…").

6. Notwithstanding that there may be some transaction that are definitely one-off, the nature of business for many of the MSBs licensed in Cayman, tend to be transactions carried out by customers on a frequent, habitual or regular basis or may be linked Given this and the ML / TF risks identified above, MSBs should therefore also:

   (1) verify identity for applicants, for money transmission and other services, where the customer, product or geography risk is deemed to be high risk in the risk assessment conducted;

   (2) Verify identity for applicants where there is an ongoing relationship akin to a business relationship as defined in the ALMRs;

   (3) For services other than wire transfer money transmission, establish more diligent thresholds other than the $15,000 stipulated in the AMLRs. The threshold should be derived from the risk assessment, bearing in mind what- (1) the amount that the average customer would transact and (2) the reporting threshold of US$3,500 on the quarterly MSB form reported to the Monetary Authority.

7. Applicants/Customers may fall within the following categories:

	Applicant for Business	**Requirements** (Highlights and supplementary only– please refer to section 4 of Part II of the Guidance Notes for the full (normal) CDD requirements).
1.	Natural Persons	(1) Identification documentation should be obtained for the applicant/customer him/herself (2) Identification documentation should be obtained for beneficial owner of funds (3) Identification documentation should be obtained for Third Party sending funds (4) Satisfactory evidence of identity, name and address, confirmed by using one or more of the verification methods in section 4 of Part II of these Guidance Notes
2.	Corporate Customer	(1) The company (evidence that it exists) e.g. a trade and business licence or a certificate of registration. (2) Consistent with that required for direct personal customers, documentary evidence of identity for all directors; all those with signing powers, including third parties; and beneficial owners. (3) Documentary evidence of identity of the new owner/controller where there is a change in ownership or control, in accordance with that required for direct personal relationships. (4) Satisfactory evidence, confirmed by at least one of the following independent checks, of company's existence: (a) Memorandum and Articles of Association and Certificate of Incorporation (b) Information about the identity of controlling shareholders and directors, e.g., Register of Directors, Register of Members (c) Understanding of all relevant third party and inter-company relationships (d) It may be appropriate to obtain information relating to customers or suppliers and the background of major shareholders and directors

3.	Partnerships / Unincorporated Businesses	(1) The entity, evidence that it exists. (2) Consistent with that required for direct personal customers, documentary evidence of identity required for partners/managers; all those with signing powers, including third parties; and beneficial owners. (3) Documentary evidence of identity of the new owner/partner/controller where there is a change in ownership/partnership or control, in accordance with that required of direct personal relationships. (4) Satisfactory evidence, 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; (c) Information about the identity of controlling partners / shareholders, e.g., excerpt from partnership document; (d) Establish all relevant third party relationships.

When must identification documentation be obtained?

8. Customer identification documentation is to be obtained prior to a transaction being carried out.

9. If identification information is not obtained, the transaction should not proceed.

What should be done if there are Doubts as to the Identity of an Existing Customer?

10. If in the process of reviewing identification documentation, the MSB has doubts about the veracity or adequacy of previously obtained customer identification data, then the MSB must take reasonable steps to verify the data.

11. Depending on the assessed ML/TF risk of the customer, the MSB could either wait for the customer to transact business again if he is a regular customer, or it can contact the individual by phone requesting that she/he submit the relevant additional documentation.

12. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of ML/TF in relation to that customer, or where the customer's pattern of transactions changes from what is deemed to be "normal" for that customer.

What Is Considered To Be An Appropriate Description Of "Source Of Funds"?

13. The appropriate description of a customer's "source of funds" include:

    (1) Salary supported by documentation on employment should be requested;
    (2) Sale of property including documentation evidencing the sale; and
    (3) Loan proceeds including documentation evidencing the grant of the loan.

14. The following on their own would not be considered appropriate descriptions of the ultimate "source of funds":

    (1) "Partners"[1];
    (2) Savings.

15. In the case of Partners, additional enquiries such as confirmation from the "banker" would be appropriate, while in the case of Savings, a bank statement should be provided. Partners and savings are nonetheless sources of funds for which additional proof of salary, dividends, sale proceeds, or loan (ultimate sources) should be provided.

Why Is It Important To Establish The Purpose Of The Transaction?

16. It is important to establish the purpose for those transactions that are large, complex or unusual (see section 2 B of this document for further guidance).

17. The threshold for large transactions should be determined from the MSB's risk assessment.

[1] Partners is an informal saving and credit scheme in the Caribbean in which a group of people regularly deposit a fixed amount of money with a main organiser, the 'banker', into a central fund. The banker distributes the total sum (the 'hand') to members in a pre-arranged order. This system of credit operates almost completely on trust, in that each person who collects his/her lump sum must be trusted to continue paying in the contributions until all members have collected their 'hand.' This scheme operates usually with no written agreement.

18. Similar to a Bank, an MSB should ask the customer about the purpose of the transaction that is beyond the MSB's threshold. In that way, the MSB should be able to establish if the purpose is lawful and whether the transaction will be a one-off event or part or a regular occurrence.

19. Information on the purpose of the transaction helps the MSB to develop a profile of "normal" activity for that customer. If the MSB is unable to establish what "normal" activity is, then it would be challenging to distinguish the unusual activities for further analysis to determine which ones are suspicious. It is therefore imperative for MSBs to consistently work towards developing customer profiles for all customers using the service.

20. Securing information on the relationship of the recipient of the transfer is useful in assisting with establishing the purpose of the transaction.

F. ELECTRONIC FUNDS TRANSFER

What Information Should Accompany The Transfer Of Funds?

1. MSBs must ensure that information on the payer and the payee accompanies the transfer of funds.

2. For guidance on the payer and payee information that need to accompany a transfer of funds, see section 11 of Part II of the Guidance Notes as that section and the regulations in Part X of the AMLRs apply to transfers of funds which means "any transaction carried out on behalf of a payer through a payment service provider by electronic means…".

G. SYSTEMS, POLICIES AND PROCEDURES

What policies and procedures should be documented?

1. At the very least, MSBs should have documented policies and procedures on:
   (1) the assessment of risks;
   (2) risk mitigation and management measures;
   (3) customer identification and due diligence;
   (4) when will enhanced due diligence be applied and what does it entail;
   (5) transaction monitoring, including complex and unusual transactions;
   (6) suspicious activity reporting;
   (7) internal controls; and
   (8) staff training.

How Should The Business Of A Customer Be Monitored?

2. Because of the large number of customers involved and the relative small amounts transacted, it is imperative for MSBs to have adequate systems in place to collate relevant information and monitor customers' activities.

3. The amount of information collected may be broadened to include details of the recipient of the funds. This information will assist MSBs to determine whether there is any ML/TF risk when the customer is utilising multiple recipients or whether multiple customers are remitting multiple small sums that are accumulated with one recipient.

What To Do About Complex And Unusual Transactions?

4. As mention in section 9 of the part II of these Guidance Notes, where a transaction is inconsistent in amount, origin, destination, or type with a customer's known, legitimate business or personal activities, the transaction must be considered unusual, and the staff member put the transaction "on enquiry". .

5. An example of an unusual pattern of transactions would be where an MSB's database reveals that several seemingly unrelated individuals are receiving or sending small amounts of money from or to one individual abroad. In such case, the MSB may request additional information on the receivers including the information on the relationship between sender and receiver(s). Additionally, the FSP may conduct an internet or screening database search to find out more about the senders and/or recipients.

6. MSBs should follow the procedures as explained in part II section 9 (and more particularly items D, E and F) of these guidance Notes for the purpose of identifying and dealing with unusual and suspicious transactions.

What Specific Records Should Be Kept And Where?

7. The MSB must keep adequate records of the identity of its customers and all transactions conducted by that customer for a period of 5 years following the last transaction, the closing of an account, or the termination of the business relationship.

8. Refer to section 8 of Part II of the Guidance Notes for guidance on "Record Keeping Procedures".

Filing A SAR

9. Refer to section 9 of Part II of the Guidance Notes, and section 34 of the AMLRs and section 136 of the Law for the role of the MLRO and reporting obligations.

10. It is important to note that SARs must be filed with the FRA in case of a suspicious transaction even if the transaction did not proceed.

Training

11. Staff should be educated in the "Know Your Customer" requirements for the prevention of ML/TF.

12. Training should therefore cover not only the need to know the customer's true identity, but also, where a business relationship is being established, the need to know enough about the type of business activity expected in relation to the customer at the outset (and on an ongoing basis) so that "normal" activity can be distinguished from suspicious activity in the future, as it relates to that person.

13. New frontline agents should not be allowed to process transactions until they have participated in the required training and successfully passed the requisite test(s). They should also be adequately trained on the factors which may give rise to suspicions about customers' activities and the procedures to adopt when a transaction appear suspicious.

14. For further details, refer to section 10 of Part II of the Guidance Notes.

Independent Audit Function

15. MSBs must have procedures of internal control including an appropriate internal audit function for the prevention of ML/TF. The internal audit function serves to test the MSB's system of internal control and is to be appropriate to the MSB's size and to the nature of its operations.

16. Testing should be risk-based, with particular emphasis on high-risk operations.

17. It should be independent, conducted periodically, and reported directly to the Board. The audit report should include, but not be limited to, the following:

    (1) review of high risk accounts, transactions, and customers;
    (2) one-off transactions in excess of the limit set by the MSB and suspicious activity reporting;
    (3) assessment of money remittance, currency exchange and check cashing transactions (to ensure whether they are in accordance with the relevant laws, regulations and guidance);
    (4) review of adequacy of customer identification information and customer due diligence; and
    (5) complex and unusual transactions.

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

Customer Profile

1. The following are some of the warning signs and red flags that money transmission/remittance provider (MRPs) should be alert to in respect of a customer's profile. The list is not exhaustive, but includes:

    (1) The Customer's area of residence is inconsistent with other profile details such as employment;
    (2) The size or frequency of the transaction(s) is not consistent with the normal activities of the customer;

(3) The goods/currencies purchased, and/or the payment arrangements are not consistent with normal practice for the type of business concerned;
(4) The customer's only address is a post office box or a c/o (in care of) address;
(5) The customer's address is that of a company service provider (domiciliation service);
(6) The customer's address information is difficult to verify;
(7) The stated address does not exist;
(8) A large number of persons are registered at the stated address, or there are a very large number of changing occupants, or other information is available indicating that it is not the real address of residence or domicile;
(9) The address of customer's residence does not correspond to the customer's financial arrangements;
(10) The customer changes address frequently;
(11) The customer is a business whose name and purpose do not correspond with its transactions;
(12) The customer cannot immediately provide additional identification documents;
(13) Identification documents appear to be unused;
(14) Identification documents are soiled making it difficult to read the necessary information;
(15) The customer is known to have a criminal history;
(16) The customer is close to a person who is known to have a criminal history;
(17) Sudden change in the customer's life style;
(18) The customer drives very expensive cars that do not correspond to his/her income situation;
(19) The customer hires or leases costly assets (e.g., real estate or cars) that do not correspond to his/her income situation.

<u>Customer Behaviour</u>

2. The following are some of the warning signs and red flags that MRPs should be alert to in respect of a customer's behaviour. The list is not exhaustive, but includes:

(1) The customer is unwilling to provide details of his/her identification information and references;
(2) Use of false identification documents to send money;
(3) Customer changes a transaction after learning that he/she must show ID;
(4) The customer shows no interest in costs or rates;
(5) The customer does not choose the simplest way to carry out a transaction;
(6) The customer has no connection with the area where the customer relationship is established;
(7) Transaction is a price-raising link in a series of transactions with no obvious reasons for the choice;

(8) The customer gives a rather detailed explanation that appears to be rehearsed concerning the reasons for the customer relationship or the transaction;
(9) The customer does not respond to communication/letters to the stated address;
(10) The customer has many newly established companies;
(11) The customer contracts a loan secured on lodging of equivalent security;
(12) The customer has companies abroad that are not justified by the customer's business;
(13) The customer explains that expensive assets are a loan from or financed by a third party;
(14) The customer uses a payment card from a country which is not his country of residence.

Transactions

General

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

(1) The transaction seems to involve unnecessary complexity;
(2) Use of front/straw men and/or shell companies;
(3) Transactions in a series are structured just below the threshold for due diligence identity checks;
(4) The customer appears to be trying to avoid reporting requirements by using two or more locations or cashiers on the same day or in quick succession to break one transaction into smaller transactions;
(5) Two or more customers appear to be trying to avoid reporting requirements and seem to be working together to break one transaction into two or more transactions;
(6) Transactions are carried out by the customer on behalf of third parties without there being an appropriate business relationship with such parties;
(7) Frequent transaction orders are made by the same customer;
(8) Sudden increases in the frequency/value of transactions of a particular customer without reasonable explanation;
(9) An unusually large (cash) transaction;
(10) The amount of the transaction is unusually large for the typical customer or for the MSB;
(11) The transaction has no apparent purpose or no obvious economic/financial basis;
(12) Unnecessary routing of funds through third parties;
(13) A customer sends/receives funds to/from him/herself, for no apparent purpose;
(14) There is no genuine reason for the customer to use the services of the MSB;
(15) Transfers of large sums of money to or from overseas locations with instructions for payment in cash;
(16) One legal/natural person transfers sums to many legal/natural persons;

(17) One legal/natural person receives sums from many legal/natural persons (from various countries);
(18) Many legal/natural persons (who have no obvious blood/business relation) are beneficial owners of transfers ordered by one legal/natural person;
(19) An under-aged person receives funds from many legal/natural persons and/or from different locations;
(20) A customer sends/receives funds to/from counterparts located in jurisdictions which are known to be exposed to ML/TF risks, for example, drug trafficking, terrorism financing, smuggling;
(21) Non face-to-face customers that are not physically present for identification purposes;
(22) Transactions are accompanied by information which appears clearly false or contradictory;
(23) The customer is unwilling to provide routine information when requested or the information provided is insufficient, false, or hard for the MSB to verify;
(24) No or limited information about the origin of funds;
(25) The explanation for the business activity and/or the funds involved is not credible;
(26) Electronic transfers involving large sums of money does not include data allowing for the clear identification of such transactions;
(27) The customer is accompanied by others who keep a low profile or stay just outside the location;
(28) The customer reads from a note he apparently did not write himself;
(29) The customer receives instructions from others;
(30) The customer appears to be in doubt when asked for further details;
(31) Difficulty in obtaining details of the beneficial owners;
(32) No relationship between sender and beneficiary;
(33) The supporting documentation does not add validity to the other information provided by the customer;
(34) The customer is in a hurry to rush a transaction through, with promises to provide the supporting information later;
(35) The customer represents a business but seems to have no business experience;
(36) The authority for others to collect funds does not seem to be well-founded;
(37) Correspondence is to be sent to another person other than the customer;
(38) Form is filled in advance;
(39) The pattern of transactions has changed since the business relationship was established;
(40) Money transfers to high-risk jurisdictions without reasonable explanation, which are not consistent with the customer's usual foreign business dealings;
(41) Sudden increases in the frequency/value of transactions of a particular customer without reasonable explanation;
(42) Instruction on the form of payment changes suddenly just before the transaction goes through;
(43) The customer, without a plausible reason, repeatedly goes to agents located far from his/her place of residence or work;
(44) Funds are sent at a time not associated with salary payments;

(45) Remittance sent or received outside customers' remittance corridors.

Cash transactions

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

(1) Unusually large cash payments in circumstances where payment would normally be made by cheque, bank draft, etc;
(2) Cash is in used notes and/or small denominations (possible indication that the money originates from the criminal offence) and dirty or has an unusual odour;
(3) Customer refuses to disclose the source of cash;
(4) Customer has made an unusual request for collection or delivery;
(5) Stains on the notes indicating that the funds have been carried or concealed, or the notes smell musty, are packaged carelessly and precipitately;
(6) When the funds are counted, there is a substantial difference between the actual amount and the amount indicated by the customer (over or under);
(7) Detection of counterfeit banknotes in the amount to be transferred or exchanged;
(8) Presenting funds in cash with further transfer of funds to another person on the same or next Day.

Other Indicators for Money Remittance /Transmission Providers

General

5. The following are some of other indicators to which MRPs should be alert. The list is not exhaustive, but includes:

(1) Transferring funds without any apparent economic reason;
(2) Money transfers to high-risk jurisdictions without reasonable explanation, which are not consistent with the customer's usual business dealing;
(3) Transfers paid by large cash amounts in different sums in a short period of time;
(4) Personal remittances sent to jurisdictions that do not have an apparent family or business link;
(5) Remittance made outside migrant remittance corridors (e.g., Asian foreign domestic remits funds to South America);
(6) Personal funds sent at a time not associated with salary payments;
(7) The customer seems only after the counting to know which amount is being transferred;
(8) The customer shows no interest in the transfer costs;
(9) The customer has no relation to the country where he/she sends/receives the money and cannot sufficiently explain why money is sent there/received from there;
(10) The customer has a note with information about payee but is hesitating if asked whether to mention the purpose of payment;

(11) Large or repeated transfers between the account of a legal person and a private account, especially if the legal person is not a resident;
(12) Large or frequent transfers of money;
(13) Use of groups of people to send money;
(14) Use of different money remittance businesses;
(15) Amounts sent are higher than usual;
(16) The operations are irregular;
(17) Receiving money from different parts of the world (developed countries) from different people;
(18) Money is received during short periods of time;
(19) Money is received from different money remittance companies;
(20) Multiple senders to a single individual.

Other Indicators for Currency Exchange Service Providers

General

6. The following are some of other indicators to which Currency Exchange Providers should be alert. The list is not exhaustive, but includes:

(1) Exchange of large quantities of low denomination notes for higher denominations;
(2) Exchange of large amounts or frequent exchanges that are not related to the customer's business;
(3) Structuring of large amounts;
(4) Repeated requests for foreign exchange purchasing-selling transactions in the amounts slightly less than the transaction limit for identification in a short period of time;
(5) The customer requests currency in large denomination notes;
(6) The customer buys currency that does not fit with what is known about the customer's destination;
(7) The customer buys currency from an unusual location in comparison to his/her own location;
(8) The customer apparently does not know the exact amount being exchanged;
(9) The customer looks around all the time and does not watch the counting of money;
(10) The customer is happy with a poor exchange rate;
(11) Currency purchases with large cash amounts;
(12) Large exchanges between foreign currencies;
(13) Frequent exchange of cash into other currencies;
(14) Exchange of primarily one type of currency;
(15) The amounts exchanged are significantly higher than usual;
(16) There is no link between the amount of money exchanged and holiday periods;
(17) High frequency of currency exchange transactions over a period of time;
(18) Many currency exchange offices used by the same person;
(19) Requests to exchange large amounts of foreign currency which is not convertible (or not frequently used) to another kind of foreign currency.

Section 2

CAYMAN ISLANDS DEVELOPMENT BANK

A. OVERVIEW

1. The Cayman Islands Development Bank (the "CIDB") is solely owned by the Cayman Islands Government. The principal function of CIDB is to mobilise, promote, facilitate, and provide finance for the expansion and strengthening of the economic development of the Islands. The Bank does this by providing financing for tertiary education, housing, agriculture and the development of small businesses. The CIDB does not accept deposits and therefore the sector guidance is geared toward ML/TF risks in loans.

B. Scope

1. This section is applicable to the Cayman Islands Development Bank (the "CIDB").

C. ML/TF

1. 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 schemes. These schemes could include the following:

   (1) Loans are made for an ambiguous or illegitimate purpose.

   (2) Loans are made for, or are paid for, a third party.

   (3) The customer attempts to sever the paper trail between the borrower and the illicit funds.

D. RISK BASED APPROACH

1. The CIDB must adopt a risk-based approach to managing ML/TF risks. The RBA aims to support the development of mitigation measures that are commensurate to the ML/TF risks identified. Entities should refer to section 3 of the Part II of these Guidance Notes.

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 or persons holding a trade and business licence.

2. The below table shows minimum identification information requirements; however, FSPs shall consider the relevant guidance provided under section 4 of Part II of these Guidance Notes.

	Applicant for Business	**Minimum Requirements**
1.	Natural Person	(1) Identification documentation should be obtained for the applicant/customer him/herself (2) Satisfactory evidence, confirmed by using one or more of the verification methods: (a) Current valid passport; (b) Any valid uniquely numbered government-issued ID card showing the photograph of the applicant, such as a driver's licence or a voter's registration card; and (c) A Cayman Islands employer ID card bearing the photograph and signature of the applicant.
2.	Corporate Customer	(1) The company (evidence that it exists) e.g. a trade and business licence or a certificate of registration. (2) Consistent with that required for direct personal customers, documentary evidence of identity for all directors; all those with signing powers, including third parties; and beneficial owners. (3) Satisfactory evidence, confirmed by at least one of the following independent checks, of company's existence: (a) Memorandum and Articles of Association and Certificate of Incorporation (b) Copy of Trade and Business Licence

When must identification be obtained?

3. Customer identification information is to be obtained prior to extending any loan facility to the customer.

4. If identification information is not obtained, the loan facility should not proceed.

F. INDEPENDENT AUDIT FUNCTION

1. The CIDB must have internal control procedures including an appropriate internal audit function for the prevention of ML/TF. The CIDB should have policies, procedures, and processes to monitor, identify, and report unusual and suspicious activities. The sophistication of the systems used to monitor lending account activity should conform to the size and complexity of the lending business.

2. The CIDB must liaise with the internal auditor to ensure that AML/CFT audits are regularly conducted in order to strengthen the processes and procedures and readily identify and address any risks of ML/TF.

G. WHAT WARNING SIGNS OR "RED FLAGS" SHOULD THE CIDB BE ALERT TO?

1. The following are some of the warning signs and red flags that the CIDB should be alert to in respect of a customer's profile. The list is not exhaustive, but includes:

   (a) Sudden/unexpected payment on loans. A customer may suddenly pay down or pay off a large loan, with no evidence of refinancing or other explanation.
   (b) Reluctance to provide the purpose of the loan, or the stated purpose is ambiguous, inconsistent or inappropriate (use of loan proceeds).
   (c) Loan payments by third parties. Loans that are paid by third party could indicate that the assets securing the loan are really those of the third party who may be attempting to hide the ownership of illegally gained funds.
   (d) Collateral pledged by a third party.
   (e) Financial statement composition of a business differs greatly from those of similar businesses.
   (f) Mortgage financing with a request for an unusually short maturity term.

H. TRAINING

1. Staff should be educated in various areas of AML/CFT compliance, and mainly in relation to CDD requirements and identification of suspicious activities for the prevention of ML/TF. Training should therefore cover not only the need to know the customer's true identity, but also, where a business relationship is being established, the need to know enough about the (type of business) activity expected in relation to the customer at the outset (and on an ongoing

basis) so that "normal" activity can be distinguished from suspicious activity in the future, as it relates to that person.

2. For further guidance, refer to section 10 of Part II of the Guidance Notes.

I. DOCUMENTATION OF POLICIES AND PROCEDURES

1. The CIDB should have documented policies and procedures in relation to various AML/CFT systems such as:

   (1) the assessment of risks;
   (2) Risk management and mitigation measures;
   (3) customer identification and due diligence;
   (4) when will enhanced due diligence be applied and what does it entail;
   (5) suspicious activity reporting;
   (6) internal controls; and
   (7) staff training.

J. RECORD KEEPING

1. The CIDB must keep adequate records of the identity of its customers, all transactions conducted by and any information relevant to that customer for a period of 5 years following the last transaction, the closing of an account, or the termination of the business relationship.

2. Refer to section 8 of Part II of the Guidance Notes for further guidance on record keeping procedures.

K. FILING A SAR

3. Refer to section 9 of Part II of the Guidance Notes, and section 34 of the AMLRs and section 136 of the Law for the role of the MLRO and reporting obligations.
4. It is important to note that SARs must be filed with the FRA in case of a suspicious transaction even if the transaction did not proceed.

Section 3

LOANS BY UN-SUPERVISED LENDERS

A. OVERVIEW

1. The Monetary Authority does not supervise all lenders within the Cayman Islands; however, there has been and continues to be a need for persons/organisations engaged in facilitating short term loans to adhere to the AML/CFT legislative requirements. These facilities usually include "Pay Day Loans".

2. Un-supervised lenders[2] are governed by the AMLRs and these Guidance Notes, and must operate their businesses in line with the laws of the Cayman Islands.

B. SCOPE

1. This section of the Guidance Notes provides guidance to the un-supervised lenders.

C. ML/TF RISKS

1. The Un-supervised lenders' risk assessments should take into consideration factors such as:
   (1) Its customer types (taking into account customer occupation or type of business operated);
   (2) The geographical location of customers or where funds are transmitted; and
   (3) The purpose of the loan.

D. RISK BASED APPROACH

1. Un-supervised lenders must adopt a risk-based approach to managing the ML/TF risks inherent to their business and associated with their customers. The RBA aims to support the development of mitigation measures that are commensurate to the ML/TF risks identified. Entities should refer to section 3 of the Part II of these Guidance Notes.

E. CUSTOMER DUE DILIGENCE

Who is the Customer/Applicant for business?

1. The applicant may be any one of the following:

[2] FSPs that are conducting lending activity but are not supervised (by any supervisory authority)

(1) Natural persons;

(2) Corporate persons; or

(3) Persons holding a trade and business licence.

2. The below table shows minimum identification information requirements; however, Un-supervised lenders shall consider the relevant guidance provided under section 4 of Part II of these Guidance Notes.

	Applicant for Business	**Minimum Requirements**
1.	Natural Person	(1) Identification documentation should be obtained for the customer him/herself (2) Satisfactory evidence, confirmed by using one or more of the verification methods: (a) Current valid passport; (b) Any valid uniquely numbered government-issued ID card showing the photograph of the applicant, such as a driver's licence or a voter's registration card; and (c) A Cayman Islands employer ID card bearing the photograph and signature of the applicant.
2.	Corporate Customer	(1) The company (evidence that it exists) e.g. a trade and business licence or a certificate of registration. (2) Consistent with that required for direct personal customers, documentary evidence of identity for all directors; all those with signing powers, including third parties; and beneficial owners. (3) Satisfactory evidence, confirmed by at least one of the following independent checks, of company's existence: (a) Memorandum and Articles of Association and Certificate of Incorporation (b) Copy of Trade and Business Licence

3. Un-supervised lenders are required to collect identification documentation for all loans issued. (See section 4 of Part II of the Guidance Notes)

F. WHAT WARNING SIGNS OR "RED FLAGS" SHOULD FSPs BE ALERT TO?

1. The following are some of the warning signs and red flags that should be alert to in respect of a customer's profile. The list is not exhaustive, but includes:

   (1) Sudden/unexpected payment on loans. A customer may suddenly pay down or pay off a large loan, with no evidence of refinancing or other explanation;
   (2) Reluctance to provide the purpose of the loan, or the stated purpose is ambiguous, inconsistent or inappropriate use of loan proceeds; and
   (3) Loan payments by third parties. Loans that are paid by a third party could indicate that the assets securing the loan are really those of the third party who may be attempting to hide the ownership of illegally gained funds.