FijiFIU

Fiji Financial Intelligence Unit

FIU Enforceable Guideline 1

Financial Transactions Reporting Act

This Guideline is an enforceable instrument issued pursuant to the powers of the Financial Intelligence Unit under the Financial Transactions Reporting Act No.22 of 2004 [Section 25.1(j) FTR Act; Regulation 3.1; 24.3; 35 and 37 FTR Regulations].

Suspicious Transaction Reporting

1. INTRODUCTION

1.1. Financial institutions[1] are required under section 14(1) of the Financial Transactions Reporting (FTR) Act (2004) to report to the Financial Intelligence Unit (FIU) any transaction[2] (including attempted transactions) or information which it suspects or has reasonable grounds to suspect maybe related to the commission of:

a) a money laundering (ML) offence;
b) a financing of terrorism (TF) offence;
c) a *serious offence*[3].

1.2. Under section 7 of the FTR Act, if satisfactory evidence of the identity of a customer[4] is not produced to or obtained by a financial institution under section 4, 5, or 6, the financial institution must not proceed any further with the transaction unless directed in writing to do so by the FIU and must report the attempted transaction to the FIU as a suspicious transaction.

1.3. Furthermore, under regulation 19 of the FTR Regulations, if a financial institution is unable to ascertain or establish the general purpose, type, volume and value, and the origin and destination of funds involved in a transaction, the financial institution must not proceed any further with the transaction unless directed to do so by the FIU. It must also report such transaction to the FIU as a suspicious transaction.

1.4. The objective of this Guideline is to provide further guidelines and requirements on the obligations of financial institutions to identify and report suspicious transactions.

---

[1] Financial institutions include banks, non-bank financial institutions and other designated non-financial businesses and professions that are covered by the FTR Act as specified in the Schedule of the FTR Act.
[2] The term "*transaction*" is defined in the FTR Act and includes entering into a fiduciary relationship.
[3] A *serious offence* is defined as an offence for which the maximum penalty prescribed by law is death or imprisonment for not less than 6 months or a fine of not less than $500. A serious offence includes crimes such as tax evasion, drug related offences, offences related to national security and weapons proliferation, human trafficking, corruption and bribery, identity fraud, immigration fraud, cyber related scams, etc.
[4] The terms "customer" and "client" maybe used interchangeably.

2. MONITORING BUSINESS RELATIONSHIPS AND CUSTOMERS' TRANSACTIONS

2.1. Financial institutions must implement risk-based monitoring systems and controls to enable it to identify any complex, unusual or large transactions or patterns of transactions that have no apparent economic or lawful purpose.

2.2. The monitoring system may be a manual or an automated system (or a combination of both) depending on the nature and size of the financial institution and the complexity of its operations and services.

2.3. Financial institutions must, during the course of a business relationship with its customer, conduct continuous due diligence on the customer and the business relationship.

2.4. As part of this continuous due diligence, the financial institution must pay special attention to a customer's transactions to ensure that they are consistent with the financial institutions' knowledge of the customer, the customer's business, type of business and source of funds.

3. REASONABLE GROUNDS FOR SUSPICION

3.1. As part of its monitoring controls and system, a financial institution must have procedures and controls for identifying suspicious transactions. A financial institution must report any transaction (including attempted transactions) or information which it suspects or has reasonable grounds to suspect maybe related to the commission of a ML, TF or any other serious offence or criminal activities.

3.2. A financial institution's decision to report a suspicious transaction(s) must be based on *whether there is reasonable grounds to suspect that the transaction(s) (or attempted transaction) in question maybe related to the commission of a ML, TF or other serious offence.*

3.3. This means that there should be *"sufficient facts"* or credible and objective evidence to support a financial institution's suspicion and its decision to report a transaction(s) to the FIU.

3.4. Financial institutions should evaluate the *facts and context* regarding a transaction(s) to determine if there is *reasonable grounds* to suspect that the transaction(s) is related to the commission of a ML, TF or any other criminal offence.

4. IDENTIFICATION OF SUSPICIOUS TRANSACTIONS

4.1. Financial institutions can identify suspicious transactions by following these four steps:

a) **Detect** a suspicious indicator(s);
b) **Ask** the customer appropriate questions;
c) **Review** customer's records; and
d) **Evaluate** the above information.

4.2. **Detect** Suspicious Indicators

4.2.1. The first step in identifying a suspicious transaction is to detect indicators that a transaction(s) may involve funds that are derived from an illegal activity or that the transaction(s) is an attempt to disguise funds derived from illegal activity, or lacks a business or apparent lawful purpose. These indicators are facts.

4.2.2. The indicators act as "red flags" and alerts for the financial institution to pay more attention to a particular customer or transaction(s). These indicators include:

a) complex, unusual or large transactions that have no apparent economic or lawful purpose;

b) unusual pattern of transactions that have no apparent economic or lawful purpose;

c) the transaction (or attempted transaction) does not match the known background, nature and type of customer, including source of funds; or

d) unusual customer behavior.

4.2.3. The presence of suspicious indicators does not immediately equate to criminality or suspicion. Rather, the detection of an indicator especially a combination of indicators should prompt the financial institution to increase monitoring and to take further actions to assess whether the transaction(s) should be reported to the FIU as suspicious.

4.3. A non-exhaustive list of potential indicators is provided in the appendices.

4.4. **Ask** the Customer Appropriate Questions

4.4.1. If one or more suspicious indicators are detected, a financial institution and its employees may ask the customer relevant and appropriate questions to determine whether there is a reasonable explanation for that observed indicator.

4.4.2. Financial institutions must ensure that when asking such questions, they do not "tip-off" the customer. Instead questions could be asked using a service approach. For example, a customer who frequently conducts large cash transactions maybe offered a more secure way to transfer money or a customer who conducts business like transactions maybe offered a business account. Answers to the questions asked are facts.

4.5. **Review** Customer's Records

4.5.1. The next step is to determine whether the suspicious indicators identified earlier is justifiable given what is known about the customer. This is context.

4.5.2. To achieve this, a financial institution must review its customer's records and consider all information that is already known to it about the customer. This may include:

a) the customer's usual occupation, business or principal activity;
b) the customer's transaction history;
c) the customer's risk profile;
d) the customer's income level;

e) the customers source of income as stated during account opening or initial engagement;
f) reasons for the transactions as provided by the customer;
g) the "relationship" of the customer with the sender or beneficiary of funds;
h) the frequency of transactions;
i) the size and complexity of the transaction;
j) the identity or location of any other person(s) involved in the transaction;
k) the usual or typical financial, business or operational practices or behavior of customers in the similar occupation or business category; and
l) the availability of identification documents and other documentation.

4.5.3. There is a possibility that after asking the customer appropriate questions and reviewing the customer records, a financial institution may find that the indicator(s) observed is justifiable in view of the customer's profile or there was a reasonable explanation for the indicator(s).

4.5.4. Alternatively, the financial institution may determine that the customer's profile has changed and that the customer profile information held with the institution needs to be updated.

4.6. **Evaluate** Information Collected

4.6.1. Financial institutions must evaluate the (i) suspicious indicators, (ii) information solicited from the customer through questions asked, and (iii) known information about the customer to determine if there is reasonable grounds to suspect that the transaction(s) is related to the commission of a ML, TF or any other serious offence.

4.6.2. If the financial institution concludes that there is reasonable grounds to suspect that the transaction(s) or attempted transaction(s) is linked to a ML, TF or any other serious offence, it should report this suspicion to the FIU by completing and submitting a suspicious transaction report to the FIU.

4.6.3. A financial institution should then be able to clearly articulate the reasons for its suspicion based on this evaluation.

4.7. If a financial institution is unable to establish reasonable grounds of suspicion, it must continue monitoring the customer or the business relationship.

4.8. By monitoring a customer's activity, a financial institution may revert to any of the above steps (detect, ask, review and evaluate) at a later date and find that new facts and context may raise the suspicion to meet the reasonable grounds of suspicion threshold.

4.9. The requirement to report any suspicious transaction applies to all types of transaction[5] regardless of whether cash is involved. Thus, non-cash transactions, such as telegraphic transfers, that meet the threshold of suspicion, should also be reported.

4.10. There is no minimum monetary threshold amount for reporting suspicious transactions. Thus, a transaction considered suspicious should be reported to the FIU regardless of the dollar amount of the transaction.

[5] The term "transaction" is defined in the FTR Act and includes entering into a fiduciary relationship.

4.11. If a financial institution is not able to obtain satisfactory evidence of a customer's identity, the financial institution must not proceed any further with the transaction unless directed in writing to do so by the FIU.

4.12. If the financial institution considers the reasons for the customer's failure or refusal to produce adequate identification documentations as unreasonable or suspicious, it must report the attempted transaction to the FIU as a suspicious transaction.[6]

5. FORMAT AND TIMING FOR REPORTING OF SUSPICIOUS TRANSACTIONS

5.1. A suspicious transaction must be reported to the FIU as soon as practicable after a financial institution has formed its suspicion but no later than 2 working days after forming this suspicion.

5.2. A financial institution must report a suspicious transaction to the FIU in a suspicious transaction report (STR) form. This must be submitted to the FIU electronically or through paper reports.

5.3. A STR submitted to the FIU should be accurate and complete.

5.4. The STR should include the following information:

a. **Identification details** of the person(s) or entity involved in the suspicious transaction. For natural persons include their full name, date of birth, tax identification number and occupation details. For entities including companies include full legal name, trading name, company/business registration number, tax identification number, country of incorporation and details of the beneficial owners and account signatories.

b. **Details of the identification documents** used by the financial institution to identify the customer (including relevant reference or document numbers) such as passport, driving licence or Joint FNPF/FRCS card.

c. **Contact details** of the person(s) or entity reported on such as residential and business address, postal address, telephone number and mobile phone number.

d. **Details of the nature of the business relationship established** or attempted to be established (type of financial services provided; type of account; account number).

e. **Details of the suspicious financial activity**. Nature or type of the suspicious transaction or services provided. Date of the suspicious transaction and value of the transaction (or attempted transaction). The explanation, if any, given by the customer about the transaction.

f. **Grounds for Suspicion.** The financial institution should clearly and concisely explain the grounds or reason why it considers the transaction(s) suspicious.

This explanation should include: i) details of the suspicious indicators that were observed; and ii) reasons for its suspicion based on its evaluation of the facts and context information in section 4.6. The financial institution should also clearly state the criminal activity or activities that is suspected to be linked to the transaction(s) being reported on[7].

[6] Refer to FIU Guideline 4 for further requirements on engaging with customers with insufficient identification documents.

[7] Appendices 8 -13 provides a list of indicators or red flags that may be linked to key criminal or predicate offences.

5.5. When submitting a STR, a financial institution must provide all relevant facts, context and reasons for suspecting that a ML, TF or a serious offence is occurring, including attempted transaction. For attempted transactions where insufficient information may have been collected by a financial institution, the STR must include all information that is known to the financial institution at the time of completing the STR.

5.6. A financial institution must submit its STR to the FIU through its Anti-Money Laundering (AML) Compliance Officer or any other employee designated by the AML Compliance Officer. There must be clear internal reporting procedures in place to allow for this.

5.7. A financial institution may report a STR on telephone, secure email or other secure means in exceptional cases that require urgent attention of the FIU, however, a formal STR must subsequently be reported as required under sections 5.1 to 5.6 above.

6. TREATMENT OF A CUSTOMER PREVIOUSLY REPORTED AS SUSPICIOUS

6.1. A financial institution is not required to terminate a business relationship or to stop[8] providing a financial service to a customer for whom it has formed a suspicion on. Its internal risk assessment policy and procedures must guide any decision on whether to continue doing business with the customer.

6.2. Once a financial institution reports a customer or transaction to the FIU in a STR, the institution is not required to continue reporting on the subsequent financial activities of that customer unless any of the following conditions occurs:

a) new or additional information on the customer is obtained by the financial institution which was not included in the initial STR;
b) there is a change in the ground(s) of suspicion surrounding the activities that the customer is engaged in; or
c) the financial institution is specifically instructed by the FIU (either through an FIU Alert & Instruction Notice or other means) to inform the FIU of any further activities conducted by the customer or other parties reported in the initial STR.

[8] Section 7 of the FTR Act and section 19 of the FTR Regulations.

7. CONFIDENTIALITY OF SUSPICIOUS TRANSACTION REPORTS

7.1. A financial institution and its employees or agents must not disclose to any person (including the customer):

a) that it has reported or will be reporting a suspicious transaction to the FIU;
b) that the financial institution has formed a suspicion on a particular customer's transaction; or
c) any other information which may cause the person to conclude that a suspicion has been formed or that a report has been or may be made to the FIU.

7.2. A financial institution, its employees or agents, must not disclose to the customer being reported on, that it will be reporting (or has reported) his or her transaction or information to the FIU as being suspicious.

7.3. Disclosure of information on suspicious transactions is only allowed under the following circumstances:

a) disclosure to an officer, employee or agent of the financial institution for any purpose connected to the performance of that person's duties;
b) disclosure to a lawyer for the purpose of obtaining legal advice on the matter;
c) disclosure to a supervisory authority (such as the Reserve Bank of Fiji to enable it to carry out its supervisory role; or
d) disclosure as part of a court order.

7.4. A financial institution and its employees are protected from any civil, criminal or disciplinary action taken against it for reporting a suspicious transaction in good faith.

7.5. Furthermore, the FTR Act prohibits the disclosure of information that will identify or will likely identify any person who has handled a transaction for which a STR has been raised or any person which has prepared or made a STR.

7.6. A financial institution is required to comply with the STR and other obligations under the FTR Act notwithstanding any obligation as to secrecy or other restriction on the disclosure of information imposed by any written law or otherwise. This includes the overriding of legal professional privilege, professional secrecy, banking secrecy and other client/customer confidentiality.

8. FIU REQUESTS FOR FURTHER INFORMATION ON STRS SUBMITTED

8.1. The FIU may, as part of its STR analysis process, request[9] a financial institution to provide further information on a suspicious transaction reported on.

8.2. A financial institution must provide accurate and complete information in response to a FIU request for further information.

[9] Section 14(3) & 25(1)(h) of the FTR Act.

9. OVERSIGHT AND IMPLEMENTATION

9.1. The FIU and/or the relevant supervisory authority, in the course of its supervision, may assess the compliance of financial institutions with the requirements of this Guideline.

9.2. Non-compliance with this Guideline may result in sanctions as specified in section 43(2) of the FTR Act and regulation 42(2) and 42(3) of the FTR Regulations.

10. EFFECTIVE DATE

10.1. This Guideline is effective from 29 January 2021.

Financial Intelligence Unit

26 October 2007

12 January 2021 (Revised)

Attached Appendices:

1. Examples of Suspicious Transaction Indicators-Banks/Lending/Credit Financial Institutions
2. Examples of Suspicious Transaction Indicators-Foreign Exchange Dealers/Money Remitters
3. Examples of Suspicious Transaction Indicators-Investment Advisers, Brokers, Dealers and Investment Fund
4. Examples of Suspicious Transaction Indicators-Insurance Brokers, Agents, Businesses
5. Examples of Suspicious Transaction Indicators-Accountants
6. Examples of Suspicious Transaction Indicators-Lawyers
7. Examples of Suspicious Transaction Indicators-Real Estate Agents, Businesses
8. Indicators or Red Flags for Tax Evasion and other Related Offences
9. Indicators or Red Flags for Drug Trafficking and other Related Offences
10. Indicators or Red Flags for Cybercrime/Online Scams
11. Indicators or Red Flags for Fraud/Forgery
12. Indicators or Red Flags for Human Trafficking
13. Indicators or Red Flags for Terrorist Financing
14. List of Possible Predicate Offences for Money Laundering

Appendices 1

Examples of Suspicious Transaction Indicators –Banks/Lending/Credit Financial Institutions

The detection of an indicator especially a combination of indicators should prompt the financial institution to increase monitoring and to take further actions to assess whether the transaction(s) should be reported to the FIU as suspicious.

ACCOUNT OPENING

1. Customer attempts to open an account(s) in what appears to be a fictitious name or in the name of other persons.
2. Customer submits copies of identification documents while refusing to present the originals without any rational reasons.
3. Customer provides identification documents which are suspected to be forged or false.
4. Customer provides unclear or doubtful information during account opening process.
5. Customer refuses to present his or her personal identification documents without any rational reasons.
6. Customer insists on establishing his or her identity through means other than using personal identification documents.
7. Attempts by a customer to open an account by mail-order or email.
8. A customer, that is a legal entity or other form of legal arrangement, attempts to open a business account without proper documents or evidence to prove its incorporation or legal existence. Financial institution finds discrepancies in the identification data (e.g. address, business details) or documents (e.g. passport, driver's licence) of a customer after an account is opened.
9. Customer attempts to open multiple accounts.

CASH TRANSACTIONS

1. Customer conducts a series of large deposits and withdrawals within a short period of time in cash or by cheque. The customer keeps making withdrawals until all funds deposited has been depleted.
2. The stated occupation of the customer does not correspond to the level or type of transactions undertaken.(e.g. a student customer makes a series of large cash deposits and withdrawals at different locations).
3. Sudden increase in an account balance through large cash or cheque deposits.
4. Customer frequently exchanges small denomination notes for large ones.
5. Customer deposits very dirty or moist currency notes.
6. Customers who appear to be acting together, simultaneously using separate tellers to conduct large cash transactions or foreign exchange transactions.
7. Customer conducts several transactions on the same day at the same branch but in conducting the transactions the customer deliberately uses different tellers.

8. Customer frequently conducts cash transactions for amounts just below the reporting threshold of $10,000 e.g. $9,900, $9,000, $9,990 in an apparent attempt to avoid being reported on.
9. An *occasional customer* frequently conducts cash transactions below the occasional transaction threshold of $5,000 to avoid activating the customer identification requirements.
10. Company accounts that are dominated by cash transactions rather than other monetary instruments normally associated with commercial businesses such as cheques or credit cards.
11. Customer presents uncounted funds for a transaction. On counting of the funds by the financial institution employee, the customer reduces the amount of funds to be transacted to avoid activating the reporting requirements.
12. Customer frequently purchases travelers cheques, bank drafts or other negotiable instruments with cash.
13. Customer makes irregular large loan repayments exceeding the required monthly/weekly repayment amount using cash or other negotiable instruments.
14. Customer pays a large sum of deposit for a loan without reasonable evidence of source of funds.
15. Customer makes large cash payments which clears off his/her loan balance well before the end of the loan term.

TRANSACTIONS THROUGH EXISTING ACCOUNTS

1. Large deposits and withdrawals during a short period of time into an account immediately after being opened. The account is then closed or discontinued for any other transactions.
2. Customer frequently conducts transactions at particular branches instead of a branch conveniently located to where he/she resides or works.
3. Frequent telegraphic transfers of large sums into an account of customer.
4. Customer frequently receives large deposits into his/her account at a branch distantly located from the branch at which the customer maintains his/her account.
5. Transactions involving an account which is used frequently to remit funds to a large number of people.
6. Funds are deposited into several accounts, consolidated into one and transferred abroad.
7. Large deposits into a particular account before these funds are remitted abroad.
8. Customer deposits large sums of money into his/her account, obtains a certificate of balance before transferring the funds to another account. This transaction takes place within a couple of days.
9. An account receives frequent remittances from a large number of people followed by a large remittances or withdrawals from that accounts just after receiving the remittances.
10. An inactive account suddenly experiences significant activity with large deposits and withdrawals noted.

11. Customer gives conflicting information to different financial institution officials.
12. Multiple deposits into an account by third parties.
13. Deposits into personal accounts of what appears to be proceeds from business related activities.
14. Lack of documentary evidence to support large transactions.
15. Large value term deposits for a customer, however this is not supported by the customer's occupation or business activity.
16. Customer repays loan early, or is significantly in advance on their payments.
17. The customer had several mortgage loans relating to several residences, however this is not supported by customer's stated source of funds.
18. Multiple transfers between several related or unrelated customers without reasonable explanations.

CROSS BORDER TRANSACTIONS

1. Transactions where customers make frequent large overseas remittances within short periods of time.
2. Customer sends or receives large overseas remittances for economically unreasonable purposes.
3. Information concerning the originator of a wire transfer is not provided.
4. Transactions where customers frequently purchases or encash large amounts of traveler's or remittance cheques (including those denominated in foreign currencies).
5. Business relationships and transactions with natural and legal persons (including financial institutions and non-face to face customers), and those acting on their behalf, from countries for which this is called for by the Financial Action Task Force (FATF) or other higher risk countries as identified by the FIU.

Appendices 2

Examples of Suspicious Transaction Indicators –Foreign Exchange Dealers/Money Remitters

The detection of an indicator especially a combination of indicators should prompt the financial institution to increase monitoring and to take further actions to assess whether the transaction(s) should be reported to the FIU as suspicious.

CROSS BORDER TRANSACTIONS

1. Transactions where customers make frequent large overseas remittances within short periods of time.
2. Customer sends or receives large overseas remittances for economically unreasonable purposes.
3. Information concerning the originator of a wire transfer is incomplete or not provided fully
4. Transactions where customers frequently purchases or encash large amounts of traveler's or remittance cheques (including those denominated in foreign currencies).
5. Transactions with natural and legal persons (including financial institutions and non-face to face customers), and those acting on their behalf, from countries for which this is called for by the Financial Action Task Force (FATF) or other higher risk countries as identified by the FIU.
6. Customers who decline to provide information or evidence in conducting a transaction.
7. Customer attempts to conduct a transaction using documents (justification documents such as airline tickets) presented in a previous transaction.
8. Person conducting transaction at the counter using identification documents of another person. This includes any dealing with an agent where the identity of the ultimate beneficiary is undisclosed, contrary to normal procedure for the type of business concerned.
9. Customers transferring large sums of money to or from overseas locations with instructions for payments in cash.
10. Numerous wire transfers received by a customer but each transfer is below the reporting requirement in the remitting country.
11. Customer making payments for products/services to a third party and not the supplier.
12. Customer attempts to conduct transaction with a fictitious name
13. Customer submits copies of identification documents while refusing to present the originals without any rational reasons.
14. Customer documents which are suspected to be forged or false e.g. airline tickets, ID cards.

FOREIGN CURRENCY OR CASH TRANSACTIONS

1. Customer frequently purchases travelers cheques
2. Customers who appear to be acting together, simultaneously using separate tellers to conduct large cash transactions or foreign exchange transactions.
3. Customer converts large quantities of low denomination notes for those of higher denomination.
4. Large amount of cash presented without any reliable documentary evidence of its source.
5. Frequent exchange of cash into other currencies.

Appendices 3

Examples of Suspicious Transaction Indicators – Investment Advisers, Brokers, Dealers and Investment Fund

The detection of an indicator especially a combination of indicators should prompt the financial institution to increase monitoring and to take further actions to assess whether the transaction(s) should be reported to the FIU as suspicious.

OPENING OF INVESTMENT ACCOUNT

1. A customer who is reluctant to provide his/her details and for whom verification of identity proves unusually difficult.
2. A customer refuses to present the required identification documents or submits copies of identification documents while refusing to provide original identification documents for no rational reason.
3. Unusual discrepancies noted in the identification of the customer such as the customer's name; address or date of birth. Customer provides conflicting information or details about himself/herself and her investment needs.

INVESTMENT TRANSACTIONS

4. A customer purchases securities (e.g. stocks, bonds etc.) and the nature of such an investment is irregular given the customer's occupation/business details and other background information.
5. A customer makes a series of purchase of stocks, bonds, units, etc. using cash or cheque within a short period of time and is considered irrational in view of the customer's occupation, investment history and other factors.
6. Customer settles a large transaction using cash or small denomination notes and coins.
7. Customer transfers his investment to an apparently unrelated third party with no explanation.
8. Investment transactions involving accounts of corporations that are suspected of never having existed, especially in cases where during your contact with such corporations after their accounts were opened, you suspected errors or misleading information was provided at the initial account opening stage.
9. Early termination of an investment by a customer despite losses incurred as a result of the termination; especially where cash was used by the investor and/or the refund is paid to a third party.
10. Selling of securities by a customer for no rational reason or in circumstances that appear unusual.
11. Customer attempts to inflate the price of an investment held for gain.

Appendices 4

Examples of Suspicious Transaction Indicators –Insurance Businesses, Brokers and Agents

The detection of an indicator especially a combination of indicators should prompt the financial institution to increase monitoring and to take further actions to assess whether the transaction(s) should be reported to the FIU as suspicious.

ACCOUNT OPENING

1. Applicant is reluctant to provide the necessary identification information and documentation or provides minimal information.
2. Applicant provides conflicting information about his/her personal details and/or provides identification documents which you suspect to be fictitious.
3. Applicant appears to have insurance policies with several other institutions.
4. Applicant requests insurance policies in amounts which is considered beyond the customer's apparent means.
5. Application for a policy from a potential customer in a distant place where a comparable policy could be provided "closer to home."
6. Customer requests an insurance product that has no apparent purpose and is reluctant to provide the reason for his/her investment.
7. The applicant for an insurance policy requests to make a lump sum payment by a wire transfer or with foreign currency.
8. Applicant attempts to use a third party cheque to purchase/pay for a policy.
9. Applicant seeks an insurance policy with premiums that exceed the customer's apparent means.
10. Applicant accepts very unfavorable policy terms and conditions unrelated to his/her health or age.
11. Applicant requests to make a lump sum payment to purchase the insurance policy, when this would normally require installment payments.

DURING THE TERM AND END OF THE INSURANCE CONTRACT

12. Unusual instances of pre-payment of insurance premiums.
13. Customer pays large amount of premiums in cash or cheques which does not correspond to the customer's background
14. Customer changes from paying his/her premiums fortnightly or monthly to annually or in full.
15. The first (or the only) insurance premium is paid from a bank account outside of Fiji
16. Customer requests during the term of the insurance contract, that the ultimate beneficiary be replaced with another person who has no apparent connection with the customer/policy holder.
17. Customer cancels his/her policy early without a reasonable reason.
18. A customer on just having signed on his/her policy, immediately cancels his/her policy, especially at a loss, and requests that the payout be made to a third party.

Appendices 5

Examples of Suspicious Transaction Indicators –Accountants

The detection of an indicator especially a combination of indicators should prompt the financial institution to increase monitoring and to take further actions to assess whether the transaction(s) should be reported to the FIU as suspicious.

GENERAL

1. A customer fails or is unwilling to provide adequate identification information, or provides information that is misleading, vague, or difficult to verify.
2. Customer's transactions or proposed transactions do not correspond to the customer's economic background.
3. Customer alters the transaction after being asked for identity documents.
4. Customer refuses to identify a source for funds or provides information that is false, misleading, or substantially incorrect.

CUSTOMER ACCOUNT

5. A customer puts money in an accountant's account and uses this account to conduct transactions which could have been easily conducted through a bank or other type of account by the customer. This may include transfers to and from unrelated parties or large and rapid deposits and payments to suppliers or persons/entities in foreign countries.
6. Receipt of large sums of funds into the customer's account which is considered unreasonable in view of the customer's economic background.
7. Customer overpays the accountant by a substantial amount and seeks a refund from the accounting firm which is drawn on the firm's bank account.

TAX

8. Customer does not provide reasonable explanation for transactions.
9. Customer transactions with third parties in countries with a history of terrorism, drug trafficking or with weak regulatory framework.
10. Unreasonable use of offshore accounts by customer, trusts or companies to conduct his business.
11. Customer requests for two sets of accounts, one for taxation purposes and one for banks.
12. Customer conducts transactions through accountant that do not make commercial sense e.g. purchase of properties at inflated prices.

FINANCIAL SERVICES

13. A customer acting on behalf of a third person whom the accounting firm does not get to meet or is unable to contact or receive direct instructions from.
14. Customer is reluctant to provide adequate information when seeking financial advice.
15. Requests from customers to make settlements on their behalf which may appear unusual or unreasonable.

16. Customer requests accountants to facilitate unusual transactions such as early repayment of substantial loans or refinancing of loans with another institution shortly after getting loans in Fiji.
17. Customer requests the formation of complicated business structures which is considered unreasonable.
18. Wire transfers, deposits or payments to or from unrelated parties (foreign or domestic).

Appendices 6

Examples of Suspicious Transaction Indicators –Lawyers

The detection of an indicator especially a combination of indicators should prompt the financial institution to increase monitoring and to take further actions to assess whether the transaction(s) should be reported to the FIU as suspicious.

Management of Client Money, Securities or Other Assets

1. A customer requests that a lawyer holds in trust money on his/her behalf for no reasonable explanation such as for the provision of certain legal services or to conduct a particular transaction on behalf of the customer.
2. A customer seeks a lawyer's services to act on behalf of a third person whom the lawyer does not get to meet, contact or obtain instructions from.
3. A customer puts money in a lawyer's trust account and uses this account to conduct transactions which could have been easily conducted through a bank or other type of account.
4. Customer engages a lawyer to purchase a property or make other investments and deposits funds for this purpose into the lawyers trust account. The customer decides not to proceed with the proposed purchase or investment for no reasonable explanation and requests the lawyer to transfer the funds to an unrelated third party without providing reasonable explanation for the transfer.
5. Customer provides conflicting information or instructions to different members of the law firm.
6. Unexplained deposits made by overseas-based entities into a lawyer's trust account.
7. Multiple unexplained funds transfers to overseas beneficiaries;.

Purchase of real estate property

8. Funding for purchase of property received from third parties
9. Requests to act for multiple parties without meeting them.
10. Complex transactions in which multiple properties are bought, re-sold or exchanged;
11. Property is transferred to another individual soon after its acquisition.
12. Client buys multiple properties in a short period of time;
13. Funds received from or sent to a foreign country when there is no apparent connection between the country and the customer.
14. Unusual payment arrangement included in the terms of contract for sale or purchase of real estate.

Creation of companies

15. Attempts to disguise the real owner or parties to the transaction.
16. Involvement of high-risk countries.
17. Reluctance to disclose information, data and documents that are necessary to enable the execution of the transaction.
18. Complex company structures to disguise the identities of the ultimate natural persons that own or control the company.

Appendices 7

Examples of Suspicious Transaction Indicators – Real Estate Agents and Businesses

The detection of an indicator especially a combination of indicators should prompt the financial institution to increase monitoring and to take further actions to assess whether the transaction(s) should be reported to the FIU as suspicious.

1. A purchaser pays for a deposit on a property using large amount of cash with undisclosed source of fund.
2. A purchaser seals a deal on a property using cash.
3. The deposit on a property is paid by an unrelated third party.
4. A customer (seller) offers to pay unusually generous commission or fees.
5. A customer (property-owner) frequently changes his/her instruction to an agent on how to handle property rental payments.
6. A customer purchases a property without inspecting the property.
7. A purchaser uses a different name on the contract, agreements or deposit receipts etc.
8. A customer purchases the property in the name of a nominee other than his/her spouse e.g. in the name of a business associate or a relative.
9. A customer purchases many properties within a short period of time and does not seem to be particular of the location, condition etc. of each property.
10. The purchased property is immediately resold, and the resale entails a significant increase or decrease in the purchase price.
11. Cash used to make a significant deposit for the purchase of a property and the balance is financed by an unusual source – for example, a third party, private lender or offshore bank.
12. Complex transactions in which multiple properties are bought, re-sold or exchanged.
13. Funds received or sent to high risk-countries.
14. Customer deposits cash to buy a property but then pulls out from the transaction and requests a refund by cheque.
15. Introduction of unknown parties at a late stage of a transaction.
16. Customer uses forged and falsified documents.
17. The pattern of transactions changed since the business relationship was established.
18. Customer buys property in the name of a third party, relative or minor.

Appendices 8

Indicators or Red Flags for Tax Evasion & Other Tax Related Offences

The following indicators maybe linked to tax evasion and other tax related offences:

1. Deposits into personal accounts of what appears to be proceeds from business related activities.
2. Frequent/large transfers of business funds into personal account.
3. Use of family member accounts to deposit cash.
4. Use of cash to make deposits for loan accounts.
5. Frequent cash payments into loan accounts.
6. Diversification of business operations to evade taxes.
7. Significant remittance of funds between local and overseas individuals without any apparent established relationship.
8. Significant bank account activity which is not in line with customer's profile.
9. Ownership of many residential properties and vehicles that are not commensurate with the customer's profile.
10. Conducting several deposits below the reporting threshold of $10,000.00.
11. Numerous telegraphic transfers made into personal bank accounts.

Appendices 9

Indicators or Red Flags for Drug Trafficking and other Related Offences

The following indicators maybe linked to drug trafficking and other related offences:

Banks/Lending/Credit Institutions

1. Customer conducts a series of large deposits and withdrawals within a short period of time in cash or by cheque. The customer keeps making withdrawals until all funds deposited has been depleted.
2. Frequent and unusual cash deposits.
3. Acquisition of high value assets such as vehicles and property that do not match the customer profile.
4. Significant cash transactions that do not match daily business operations.
5. The stated occupation of the customer does not correspond to the level or type of transactions undertaken.(e.g. a student customer makes a series of large cash deposits and withdrawals at different locations).
6. Company accounts that are dominated by cash transactions rather than other monetary instruments normally associated with commercial businesses such as cheque transactions.
7. Customer makes irregular large loan repayments exceeding the required monthly/weekly repayment amount using cash or other negotiable instruments.
8. Customer makes large cash payments which clears off his/her loan balance well before the end of the loan term.
9. Large value term deposits for a customer, however, this is not supported by the customer's occupation or business activity.
10. Customer repays loan early, or is significantly in advance on their payments.
11. The customer had several mortgage loans relating to several residences, however this is not supported by customer's stated source of funds.
12. Multiple transfers between several related or unrelated customers without reasonable explanations.
13. Customer sends or receives large overseas remittances for economically unreasonable purposes.

Foreign Exchange Dealers

1. Frequent exchange of cash into other currencies.
2. Customer sends or receives large overseas remittances for economically unreasonable purposes.

Lawyers

1. Acquisition of high value assets such as vehicles and property that do not match the customer profile.

2. A customer requests that a lawyer holds in trust money on his/her behalf for no reasonable explanation such as for the provision of certain legal services or to conduct a particular transaction on behalf of the customer.
3. A customer seeks a lawyer's services to act on behalf of a third person whom the lawyer does not get to meet, contact or obtain instructions from.
4. A customer puts money in a lawyer's trust account and uses this account to conduct transactions which could have been easily conducted through a bank or other type of account.

Creation of companies

5. Attempts to disguise the real owner or parties to the transaction.
6. Complex company structures to disguise the identities of the ultimate natural persons that own or control the company.

Appendices 10

Indicators or Red Flags for Cybercrime/ Online Scams

The following indicators maybe linked to cybercrime/online scams:

1. The use of full names instead of nicknames and a language structure may not match how the supposed sender normally communicates.
2. Sudden internet banking transfers for large sums to a third party.
3. Third party immediately withdraws after a transfer and conducts outward remittances (frequently) to an unrelated party offshore.
4. Sudden change in payment instructions for no apparent reason.
5. Change in tone of email and/or frequent request for updates on when transfer will be made.
6. Customer received instructions to remit funds from a third party through social media or other internet-based messaging platform.

Appendices 11

Indicators or Red Flags for Fraud/Forgery

The following indicators maybe linked to fraud/forgery:

1. Use of unfamiliar business transacting methods which were not commensurate with nature of business.
2. Purchase of valuable assets and luxury items.
3. Stains or discolorations on the cheque possibly caused by erasures or alterations.
4. Use of money mules to remit funds offshore.
5. No apparent relationship established between sender and beneficiary of a remittance transaction.
6. Using fake documentation to open business accounts.
7. Set up of shell companies to facilitate credit card transactions.
8. Cheque presented at the bank for cashing contains multiple alterations to the details of the cheque.
9. Significant cash/cheque deposits or transfers of funds into a newly incorporated entity bank account which does not match the business profile.
10. A customer purchases a property without inspecting the property.

Appendices 12

Indicators or Red Flags for Human Trafficking

The following indicators maybe linked to human trafficking activities:

1. Common mobile number, address and employment reference being used to open multiple bank accounts in different names.
2. Customer makes deposits/withdrawals or otherwise generally operates an account accompanied by an escort, handler or translator (who may hold the customer's ID).
3. High and/or frequent expenditure at airports, ports, other transport hubs or overseas, inconsistent with customer's personal use or stated business activity.
4. Income received and immediately withdrawn in cash.
5. Newly-opened customer account appears to be controlled by a third party, including forms completed in different handwriting and/or the customer reads their address from a form.
6. Payments to logistics, airlines, coach companies, car rental or travel agents inconsistent with customer's personal use or stated business activity.
7. Relatively high or recurrent expenditure on items inconsistent with customer's personal use or stated business.
8. A business customer does not exhibit normal payroll expenditures (e.g., wages, payroll taxes, social security/superannuation contributions). Payroll costs can be non-existent or extremely low for the size of the customer's alleged operations, workforce and/or line of business.[10]
9. Substantial deductions to wages. To the extent a financial institution is able to observe, a customer with a business may deduct large amounts from the wages of its employees alleging extensive charges (e.g., housing and food costs), where the employees only receive a small fraction of their wages; this may occur before or after the payment of wages.
10. Cashing of payroll checks where the majority of the funds are kept by the employer or are deposited back into the employer's account. This activity may be detected by those financial institutions that have access to paystubs and other payroll records.
11. Frequent outbound wire transfers, with no business or apparent lawful purpose, directed to countries at higher risk for human trafficking or to countries that are inconsistent with the customer's expected activity.
12. Multiple, apparently unrelated, customers sending wire transfers to the same beneficiary. These wire senders may also use similar transactional information including but not limited to a common address and phone number. When questioned to the extent circumstances allow, the wire senders may have no apparent relation to the recipient of the funds or know the purpose of the wire transfers.
13. Transactions conducted by individuals, escorted by a third party (e.g., under the pretext of requiring an interpreter), to transfer funds (that may seem to be their salaries) to other countries.
14. Frequent payments to online escort services for advertising, including small posting fees to companies of online classifieds as well as more expensive, higher-end advertising and website hosting companies.
15. Frequent transactions, inconsistent with expected activity and/or line of business, carried out by a business customer in apparent efforts to provide sustenance to

[10]Egmont Group Human Trafficking White Paper 2020

individuals (e.g., payment for housing, lodging, regular vehicle rentals, purchases of large amounts of food).

16. Payments to employment or student recruitment agencies that are not licensed/registered or that have labor violations.

Customer Interaction Indicators: Behaviors observed while interacting with the public

17. A customer establishes an account or visits a branch to conduct transactions while always escorted by a third party (e.g., under the pretext of requiring an interpreter). Correspondingly, the third party escorting the customer may always have possession of the customer's identification document.
18. Common signer(s)/custodian(s) in apparently unrelated business and/or personal accounts. Similarly, common information (e.g., address, phone number, employment information) used to open multiple accounts in different names.
19. Accounts of foreign workers or students where the employer or employment agency serves as a custodian.
20. Unexplained/unjustified lifestyle incommensurate with employment or line of business. profits/deposits significantly greater than that of peers in similar professions/lines of business.
21. Deposits are largely received in cash where substantial cash receipts are inconsistent with the customer's line of business. Extensive use of cash to purchase assets and to conduct transactions.

Appendices 13

Indicators or Red Flags for Terrorist Financing

The following indicators maybe linked to terrorist financing activities:

Indicators linked to the financial transactions

1. The use of funds by the non-profit organization is not consistent with the purpose for which it was established.
2. The transaction is not economically justified considering the account holder's business or profession.
3. Transactions which are inconsistent with the account's normal activity.
4. Deposits were structured below the reporting requirements to avoid detection.
5. Multiple cash deposits and withdrawals with suspicious references.
6. Frequent domestic and international ATM activity.
7. No business rationale or economic justification for the transaction.
8. Unusual cash activity in foreign bank accounts.
9. Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country.
10. Use of multiple, foreign bank accounts.

Behavioral Indicators

11. The parties to the transaction (owner, beneficiary, etc.) are from countries known to support terrorist activities and organizations.
12. Use of false corporations, including shell-companies.
13. Inclusion of the individual in the United Nations 1267 Sanctions list.
14. Media reports that the account holder is linked to known terrorist organizations or is engaged in terrorist activities.
15. Beneficial owner of the account not properly identified.
16. Use of nominees, trusts, family member or third party accounts.
17. Use of false identification.
18. Abuse of non-profit organization.

Funds Transfers

19. A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves higher-risk locations.
20. Funds transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
21. Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.
22. Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
23. Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to higher-risk countries.

(Source: https://verafin.com/2015/05/58-red-flags-for-terrorist-financing/)

Appendices 14

Examples of Predicate Offences for Money Laundering

1. Tax evasion
2. Drug related offences
3. Fraud
4. Forgery
5. Corruption
6. Bribery
7. Terrorist Financing
8. Advanced Fee Fraud
9. Theft
10. Counterfeit of Currency
11. Exchange Control Breaches
12. Cybercrime related offences