ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING POLICY

It is a policy of Pacific Private Bank Ltd ("PPB") to take all reasonable steps necessary to identify, prohibit and prevent money laundering and any activity that facilitates money laundering and the funding of terrorist or criminal activities.

In this Policy "we", "us", "our" means PPB.

1. Policy Scope

The purpose of this Policy is to set the principles and define framework of PPB's processes, procedures and systems aimed to identify, prohibit and prevent activities of possible money laundering and financing of terrorism. The Policy also serves as a means of informing the Representatives of PPB of the applicable laws of Vanuatu preventing money laundering and financing of terrorism (Annexure 2). The Policy is further implemented in detail in PPB's Anti-Money Laundering and Counter- Terrorism Financing Program consisting of Part A and Part B.

PPB's AML/CTF Policy applies to all of its employees, officers and other representatives acting on behalf of PPB (hereinafter called Representatives).

The Representatives of PPB have at all times to be familiar with and comply with the up to date requirements set out in this Policy, other internal procedures of PPB and/or applicable laws of Vanuatu. It is a responsibility of Chief Compliance Officer to review the Policy periodically in order to ensure that it is up to date with the legal requirements and best practices. The Managing Director of PPB shall be responsible for making all the internal policies and procedures of PPB as well as amendments thereto available to all Representatives immediately after they have been adopted by relative governing body.

The Policy is in line with the national regulation of Vanuatu and further extends to applying and complying with International Standards on Combating Money Laundering and The Financing of Terrorism & Proliferation FATF Forty Recommendations and Special Recommendations on Terrorism Financing, the Wolfsberg Standards on AML Principles and best international banking practices on combating money laundering and terrorism financing.

2. Definitions

MONEY LAUNDERING

Money laundering generally is the process by which money earned from illegal means is "washed" through legitimate systems and enterprises in order for it to be cleaned and eventually returned to the criminal in the form of legitimate money.

There are three stages in the money laundering cycle generally known as:

(i) Placement – this is the entry of "dirty" money into legitimate institutions.

(ii) Layering – this is the most complex stage of the money laundering cycle and usually consists of multiple transactions designed to obscure the identity of the person and/or the audit trail of the source of the funds. It could involve multiple electronic transfers or even the use of traded products and/or services. The purpose of layering is to rapidly change assets into a different form and to hide or disguise the original source of the funds. Accordingly, the transactions can take place through multiple licensees, possibly even using various products – anything allowing for the swift transfer of ownership and the mechanisms that extend an audit trail or make it complicated.

(iii) Integration – during this stage, money is returned to the hands of the money launderer as legitimate funds and can be used for any purpose.

Source: United Nations Office on Drugs and Crime "The Money Laundering Cycle" at https://www.unodc.org/unodc/en/money-laundering/laundrycycle.html

Money laundering is defined as:

- the conversion or transfer of property, knowing that such property is derived from any criminal offence or from an act of participation in such criminal offence or offences for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such criminal offence or offences to evade the legal consequences of his actions;
- the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from a criminal offense or offenses or from an act of participation in such an offense or offenses.
- the acquisition, possession or use of property, knowing at the time of receipt that such property was derived from an offense or offenses or from an act of participation in such offense or offenses.

Further examples of money laundering schemes are set out in Annexure 1.

TERRORISM

FINANCING

Terrorism financing is defined in the United Nations International Convention for the Suppression of the Financing of Terrorism (1999) and is understood as activity by the person which by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

(a) An act which constitutes an offence as defined as terrorist act by the Counter terrorism and transnational organized crime act of Republic of Vanuatu; or

(b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing an act.

For an act to constitute the terrorism financing it shall not be necessary that the funds were actually used to carry out an offense referred to in paragraph 1, subparagraph (a) or (b).

There are two primary sources of financing for terrorist activities. The first involves getting financial support from countries, organizations or individuals. The other involves revenue-generating activities. These are explained in further detail below.

Financial Support

Terrorism could be sponsored by a country or government, although this is believed to have declined in recent years. State support may be replaced by support from other sources, such as individuals with sufficient financial means.

Revenue-Generating Activities

The revenue-generating activities of terrorist groups may resemble other criminal organizations. Kidnapping and extortion can serve a dual purpose of providing needed financial resources while furthering the main terrorist objective of intimidating the target population. In addition, terrorist groups may use smuggling, fraud, theft, robbery, and narcotics trafficking to generate funds.

Financing for terrorist groups may also include legitimately earned income, which might include collection of membership dues and subscriptions, sale of publications, speaking tours, cultural and social events, as well as solicitation and appeals within the community. This fundraising might be in the name of organizations with charitable or relief status, so that donors are led to believe they are giving to a legitimate cause.

Only a few non-profit organizations or supposedly charitable organizations have been implicated in terrorist financing. In these cases, the organizations may in fact have carried out some of the charitable or relief work. Members or donors may have had no idea that a portion of funds raised by the charity was being diverted to terrorist activities.

This type of legitimately earned financing might also include donations by terrorist group members of a portion of their personal earnings.

Laundering of Terrorist-Related Funds

Like criminal organizations, terrorists must find ways to launder or transfer illicit funds without drawing the attention of the authorities. For this reason, transactions related to terrorist financing may look a lot like those related to money laundering. Therefore, strong, comprehensive anti-money laundering regimes are essential to tracking terrorist financial activities.

Importance of Combating Terrorist Financing

Acts of terrorism pose a significant threat to the safety and security of people all around the world.

Business relationships with terrorist groups could expose the bank to significant reputational and operational risk, as well as legal repercussions. The risk is even more serious if the terrorist group is subsequently shown to have benefited from the lack of effective monitoring or willful blindness of a particular institution or intermediary that enabled them to carry out the terrorist activities.

The systems by which PPB detects transactions potentially related to terrorism closely resemble those designed to detect money laundering.

Should PPB become aware that a transaction or attempted transaction is related to the financing of terrorism or involves an individual or entity named as a terrorist pursuant to United Nations Security Council resolutions: the bank should immediately notify the VFIU and submit a suspicious transactions report, even if the bank declines the transaction as a result of its own due diligence.

Of note, money laundering schemes can also be utilised to fund terrorist groups.

PROLIFERATION FINANCING

Proliferation financing means the act of providing funds or financial service, which are used or will be used, in whole or in part:

(a) for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling of weapons or

(b) for the use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use good used for non- legitimate purposes), that contravenes any laws of Vanuatu.

Over the years, the global community recognized that weapons of mass destruction and their availability are detrimental to the security and sound economies of the world. Such weapons, whenever used, caused catastrophic and indiscriminative destruction to economies, infrastructures and wide spread loss of lives.

In order for terrorists and terrorist organisation to obtain such weapons of mass destruction, they should be able to have sufficient funds and have access to financial services to purchase such weapons. It is the responsibility of PPB to ensure that our business, services and delivery methods are not abused by terrorists and terrorist organisation in channeling the funds to the weapons sellers.

Similar to the terrorist financing methods, the terrorists and terrorist organisation may receive financial support from terrorist sympathizers and/or conduct revenue generating activities. The funds may be laundered through the formal financial system and used to purchase weapons.

Hence, PPB ensures that its AML&CTF program is strong, comprehensive and effective to detect and report proliferation financing to VFIU in accordance with legal acts.

3. Risk-based approach

As a financial services provider, PPB acknowledges that ML/TF risks exist which could potentially result in its services and products being utilised to facilitate money laundering or terrorist financing schemes. In addition to the regulatory risks of non-compliance with the legislation, these ML/TF risks may have an impact upon the business, including the reputation and License of PPB.

The risk of being exposed to money laundering and the financing of terrorism varies across customers, countries, products, services and over time. High risk situations demand stronger controls than lower risk situations. To manage and mitigate these risks, a risk- based approach shall be applied. The guiding principle is that resources shall be directed in accordance with priorities, so that the greatest risks receive the highest attention.

As specified in the AML & CTF Act, PPB's assessment of its ML/TF exposure must be risk-based. PPB has, and will continue to, assess and measure ML/TF risks based upon consideration of the risks posed by the following factors:

(a) its customer types;
(b) the types of designated services it provides;
(c) the methods by which it delivers designated services; (d) the foreign jurisdictions with which it deals; and
(d) the organisational structure; and
(e) the staff recruitment and retention.

4. The Anti-Money Laundering and Counter-Terrorism Financing Program

Pursuant to the AML & CTF Act, a Bank must have and comply with an AML & CTF Program. The AML & CTF Program adopted by PPB is divided into Part A (general requirements) and Part B (customer identification).

PPB has designed and will maintain its AML & CTF Program. The AML & CTF Program is applicable to all Representatives of PPB and documents the bank's policies, processes and procedures:

(a) to implement the transaction and activity reporting requirements,
(b) to implement customer due diligence requirements,
(c) to implement the record keeping requirements,

(d) to inform PPB's officers and employees of the laws of Vanuatu about money laundering and financing of terrorism, of the policies, processes, procedures and systems adopted by the entity to deal with money laundering and financing of terrorism,

(e) to train the entity's officers and employees to recognize and deal with money laundering and terrorism financing,

(f) on the role and responsibility of AML and ATF Compliance officer,

(g) on the establishment of an independent audit function which is able to test its AML&CTF processes, procedures and systems,

(h) on the adoption of systems by PPB to deal with money laundering and terrorism financing,

(i) on the staff screening, recruitment and retention program.

The primary purpose of Part A of the AML & CTF Program is to identify, mitigate and manage the risk that PPB may reasonably face (inadvertently or otherwise) by facilitating money laundering or terrorism financing through the provision of its designated services.

The primary purpose of Part B of the AML & CTF Program is to set out the applicable customer identification and verification procedures for customers of PPB.

The AML & CTF Program is risk-based and seeks to identify, mitigate and manage the possible ML/TF risks posed to PPB. A secondary purpose of the AML & CTF Program is to document the controls and systems that were implemented in order to address these ML/TF risks. Any weakness in the AML & CTF Program may impact adversely on the management of the ML/TF risks identified.

In particular, the AML & CTF Program documents the risks associated with the types of customers, the types of designated services, the delivery methods, and the foreign jurisdictions involved. Furthermore, the AML & CTF Program describes the employee due diligence procedures, the employee risk awareness and a training program, and finally the procedures for independent review and feedback.

ML/TF schemes can be difficult to identify and criminals can be ingenious in formulating different schemes in order to facilitate their money laundering or terrorist financing agendas. Accordingly, in order for the AML & CTF Program to be effective and so that it accomplishes its purpose of identifying, mitigating and managing ML/TF risk, it shall be regularly reviewed, and if necessary, amended.

Furthermore, the AML & CTF Program allows for any significant changes in ML/TF risks, including changes to the risks faced by PPB resulting from:

(i) the introduction of a designated service to the market;
(ii) the introduction of new methods of delivery for a designated service; or
(iii) the introduction of any new or developing technology to be used for the provision of designated services.

Where such changes are proposed and they result in a change in the ML/TF risks, PPB will implement controls to mitigate and manage the ML/TF risks, prior to adopting of such new designated services, delivery methods or technologies.

The AML & CTF Program, and any addendums to it, is subject to Board of Directors oversight and approval.

5. Customer due diligence procedures

Part B of the AML & CTF Program contains customer identification and verification procedures (commonly referred to as "Know your Customer" or "KYC" procedures), as well as customer approval and further ongoing monitoring procedures, which are risk-based, having regard to the ML/TF risks relevant to the provision of the services offered by PPB.

PPB carries out prescribed identification process each time before a person:

(a) opens an account with PPB, or

(b) engages any other services of PPB, or

(c) enters into business relationship with PPB, or

(d) conducts occasional transactions that exceeds the law prescribed thresholds of large cash transactions (not relevant due to no cash operations) or international currency transfers, whether conducted as a single transaction or by way of two or more transactions that appear to be linked.

Risk-based customer identification procedures include *inter alia* identifying politically exposed persons (PEP). PEP means a private individual who is or has been entrusted with prominent public functions; the term includes the immediate family members, or persons known to be close associates, of such persons. PPB understands that providing financial services to PEP might pose higher money laundering risks therefore customers identified as PEPs are required enhanced level of due diligence measures to be applied.

Well-designed procedures are aimed to mitigate and manage the potential ML/TF risks faced by PPB and ensure that the company is reasonably satisfied as to the true identity of its customers.

6. Correspondent banking

When establishing correspondent relationships with other financial institutions PPB requires that the relevant financial institution applies appropriate due diligence measures, verification and monitoring procedures of its clients.

After conducting relevant KYC procedures, the decision to establish correspondent relationships is within designated senior management officer of PPB.

PPB shall not enter into or continue a correspondent banking relationship with a shell bank. Shell bank means a credit institution, or an institution engaged in equivalent activities,

incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group.

Furthermore, appropriate measures shall be taken to ensure that PPB does not engage in or continue correspondent banking relationships with a bank that is known to permit its accounts to be used by a shell bank.

PPB does not allow a person with whom it carries out a cross border correspondent banking relationship to establish accounts in PPB for use by that person's customers.

7. Employee due diligence

PPB shall also implement comprehensive supervision procedures, ensuring that the identity and past history of prospective employees is verified. PPB recognises the potential risk as a result of staff turnover and has implemented procedures in order for new staff members (or existing staff members promoted with greater levels of AML & CTF responsibility) to be trained, monitored and subject to transactional limits. Comprehensive training in regards to the company's policies and procedures must be completed at the various stages of employment.

8. AML & CTF Awareness Training Programs

Employees shall periodically undergo training in AML & CTF laws and internal policy and procedures.

Employee training is carried out under the supervision of the Chief Compliance Officer or AML & CTF Compliance Officer. Training will initially occur upon commencement of employment with PPB, and thereafter ongoing training will occur periodically (at least annually).

PPB will also ensure that in case any third parties are employed to carry on certain functions of PPB, PPB will carry on Training Program on AML & CTF laws and internal policy and procedures for the relevant third parties.

The Training Program will take into consideration the size of the company, its customer base, its products and services offered and its resources, and will include the following:

(a) the AML & CTF Policy;
(b) the AML & CTF Program;
(c) the obligations of PPB under the AML & CTF Act and Rules and other applicable legal acts;
(d) the types of ML/TF risks PPB might face and the possible consequences of such risks;
(e) how to identify signs of ML/TF that arise during the course of the employees' duties;
(f) escalation procedures i.e. what to do once a ML/TF risk is identified;
(g) what the employee's role is in the firm's compliance efforts and how to perform them i.e. the processes and procedures relevant to each person's role;
(h) the record keeping and record retention policy; and
(i) the disciplinary consequences (including civil and criminal penalties) for non- compliance with the AML & CTF Act and supporting Rules.

9. Independent review/testing of the AML & CTF Program, processes, procedures and systems

A review of AML & CTF Program will be undertaken at least annually also in case of important changes of legal acts.

PPB shall establish (or outsource to the third party provider) an independent internal audit function to test its AML and CTF processes, procedures and systems. The review/testing will be undertaken either internally by a person independent from business units and bank's AML & CTF Compliance Officers - for instance internal auditor - or by an external service provider that will be retained to conduct such review.

The purposes of the review will be to:

(a) assess the effectiveness of the AML & CTF Program having specific regard to the ML/TF risk faced by PPB;

(b) assess whether AML & CTF Program complies with the AML & CTF Rules;

(c) assess whether AML & CTF Program has been effectively implemented; and

(d) assess whether PPB has complied with the AML & CTF Program.

The result of the review, including any report prepared, will be provided to the Board of Directors.

10. Record Keeping

PPB will retain all records relevant to its AML & CTF Program and policies including;

(a) the AML & CTF Program and all reviews and addendums to the same as well as record of adoption thereof;

(b) this AML & CTF Policy and all reviews and addendums to the same as well as record of adoption thereof;

(c) transactional records including records on originator and beneficiary information in currency transfers;

(d) CDD records: customer identification and verification records; record that indicates the kind of evidence that was obtained and either a copy of the evidence or information that enables a copy of it to be obtained; record of disclosure of any other customer's names that they may use; record of regular customer and transaction due diligence and the findings;

(e) Audits and compliance reviews;

(f) Suspicious matter reporting or any other report made under AML&CTF Act; (g) Reports relating to transactions which exceed threshold limits set out in the Law;

11. AML & CTF Compliance Officers

PPB has established compliance team to cover various compliance issues within PPB including but not limited to AML&CTF oversight.

PPB shall appoint dedicated person (-s) as the AML & CTF Compliance Officer (-s) in order to ensure the execution of the functions as required by the FTRA and AML/CTF Act. AML & CTF Compliance Officer (-s) are part of PPB's compliance team and report to the Chief Compliance Officer of PPB (who shall always be senior officer of PPB).

Chief Compliance Officer, on behalf of PPB's management and Board of Directors, has the overall responsibility to ensure that the relevant control systems, processes and routines work in an efficient manner and that the staff receives adequate training on AML/CTF topic.

The dedicated AML & CTF Compliance Officer's duties include adherence and monitoring compliance with the AML & CTF obligations, receiving and investigating reports of suspicious matters/activities, reporting suspicious activities, overseeing communication and ensuring that proper AML & CTF records are kept.

12. Ongoing Customer Due Diligence

Ongoing customer due diligence is an important component in mitigating and managing ML/TF risks (potential and identified).

PPB has set and implements procedures to adequately conduct ongoing customer due diligence:

(a) Customers are monitored on an ongoing basis in order to identify any suspicious activity;
(b) Representatives periodically review whether client's KYC information is up-to-date;

(c) Representatives review client's transactions, including trading and electronic fund transfers, based on a risk based approach manually in the context of other account activities in order to determine whether a transaction is suspicious or whether the transaction is structured to avoid reporting;

(d) the AML & CTF Compliance Officer is responsible for monitoring adherence to the AML & CTF Act, documents when and how it is carried out, and will report suspicious activities to the appropriate authorities;

(e) exception reports will be utilised to identify possible ML/TF risks and include monitoring transaction size, location, type, number and nature of the activity;

(f) employee guidelines, with examples of suspicious money laundering activities and lists of high-risk customers whose accounts may warrant further scrutiny, will be prepared; and

(g) the AML & CTF Compliance Officer will conduct an appropriate investigation before reporting a suspicious matter.

13. Suspicious Matter Reporting

Staff training and awareness programs will educate Representatives as to the potential indicators for forming a suspicion that a prospective or existing customer is seeking to use services offered by the company for money laundering or terrorist financing purposes, thereby triggering reporting obligations.

Suspicion is formed if a representative considers that an existing or prospective customer is attempting to use services offered by PPB for ML/TF purposes and any one of the following conditions is met:

(a) the Representative suspects on reasonable grounds that the customer is not the person they claim to be;

(b) the Representative suspects on reasonable grounds that the customers agent is not the person they claim to be;

(c) the Representative suspects on reasonable grounds that information collected by PPB concerning the provision (or prospective provision) of services:

(i) may be relevant to investigation of, or prosecution of a person or entity for an evasion, or an attempted evasion of taxation law;

(ii) may be relevant to investigation of, or prosecution of a person or entity for an evasion, or an attempted evasion, of a law of a State or Territory that deals with taxation; or

(iii) may be relevant to investigation of, or prosecution of a person or entity for, an offense against a law of Vanuatu; or

(d) the Representative suspects on reasonable grounds that the provision, or prospective provision, of the services is preparatory to the commission of an offence of financing of terrorism;

(e) the Representative suspects on reasonable grounds that information collected by PPB concerning the provision, or prospective provision of services may be relevant to the investigation of, or prosecution of a person or entity for an offence of financing of terrorism;

(f) the Representative suspects on reasonable grounds that the provision, or prospective provision, of the service is preparatory to the commission of an offence of money laundering;

(g) the Representative suspects on reasonable grounds that information collected by PPB concerning the provision, or prospective provision, of the service may be relevant to the investigation of, or prosecution of a person or entity for an offence of money laundering.

(h) Management approvals;

(i) Customer account/relationship records;

(j) Annual compliance reports and other management reports; (k) Training and compliance monitoring reports;

(k) Information relating to the effectiveness of training;

(l) Record of any enquiry relating to money laundering or the financing of terrorism made to the Director of VFIU;

(m) Record of a finding regarding intermediaries or third party introducers, correspondent banks.

All the records are to be retained at least for 6 years relatively after the completion of transaction, after the date when the report, finding was made, after the closure or termination of the account, service or business relationship.

AML & CTF Program and addendums, together with any documentation relevant to the reason for amendment, are also to be retained for 6 years after the AML & CTF Program and/or amendments cease to be in force.

14. Systems to re-assess risk

PPB will review all areas of its business to identify potential ML/TF risks that may not be covered in the procedures described above. The additional areas of ML/TF risks are in respect of new products, services, distribution channels and developing technologies. Additional procedures will be designed and will be implemented to identify, mitigate and manage potential ML/TF risk.

15. External authorities

PPB will co-operate with all external authorities, including VFIU. PPB will comply with any directions or notices received from such bodies and will actively search and retain records of any guidance issued or released in respect of perceived ML or TF risks.

16. Vanuatu Financial Intelligence Unit (VFIU) Feedback

The AML & CTF Compliance Officer, in conjunction with other representatives, will take all steps necessary to comply with any feedback, notices, orders, warrants etc. or to implement any directions issued by VFIU.

In particular, AML & CTF Compliance Officer will have due regard to any feedback provided by VFIU in respect of PPB' performance in managing its ML/TF risks. Any feedback must be shared with Chief Compliance Officer and will be incorporated into ongoing monitoring programs and the AML & CTF Program will be amended (where appropriate).

17. Privacy and secrecy

Customer information will be collected and retained in accordance with obligations under the legislation.

PPB must not disclose any information to any other person:

(a) that PPB, or the supervisory body or auditor of PPB or a person has formed a suspicion in relation to a transaction or an attempted transaction, or an activity or attempted activity; or
(b) that a report under AML&CTF Act is made to VFIU; or
(c) that information under the AML&CTF Act is given to VFIU; or
(d) any other information from which a person to whom the information is disclosed may reasonably be expected to infer any circumstances in paragraph (a)-(c).

The above does not apply if the disclosure is made to an authorized person as indicated in AML&CTF Act (Section 38 (2) (3) and (4)).

18. Protection of person and information in suspicious transaction and other reports

Subject to exceptions as per AML&CTF Act (Section 40A (2) etc.) a person must not disclose any information that identifies or is likely to identify any person who has:

(a) handled a transaction in respect of which a suspicious transaction or activity report or any other report or information is made under the Act;

(b) prepared a suspicious transaction or activity report or other report or information under the Act;

(c) given a suspicious transaction or activity report or other report or information under the Act.

A person is not liable to any civil or criminal action or other proceeding or damages for or in respect of an act done or omitted to be done in good faith in the exercise or performance, or purported exercise or performance of a power, function or duty conferred to him by the AML& CTF Act.

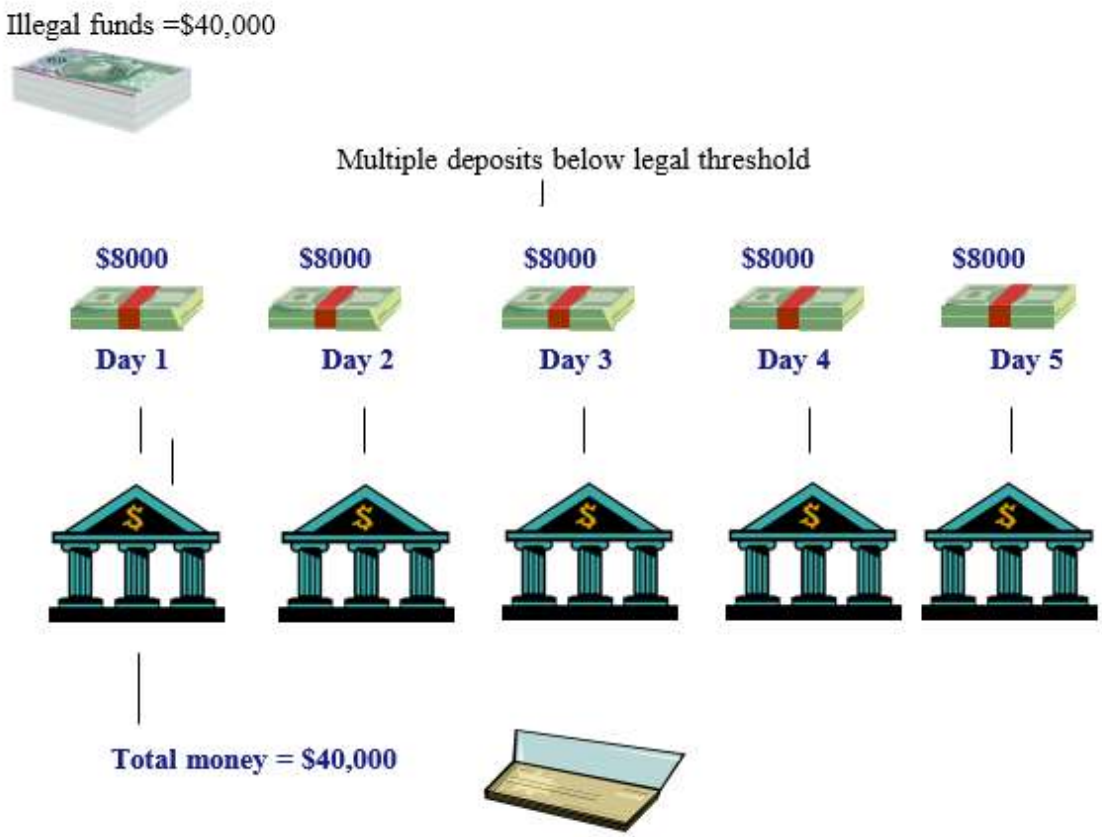
ANNEXURE 1

Money Laundering Schemes

Structuring deposits – also known as smurfing

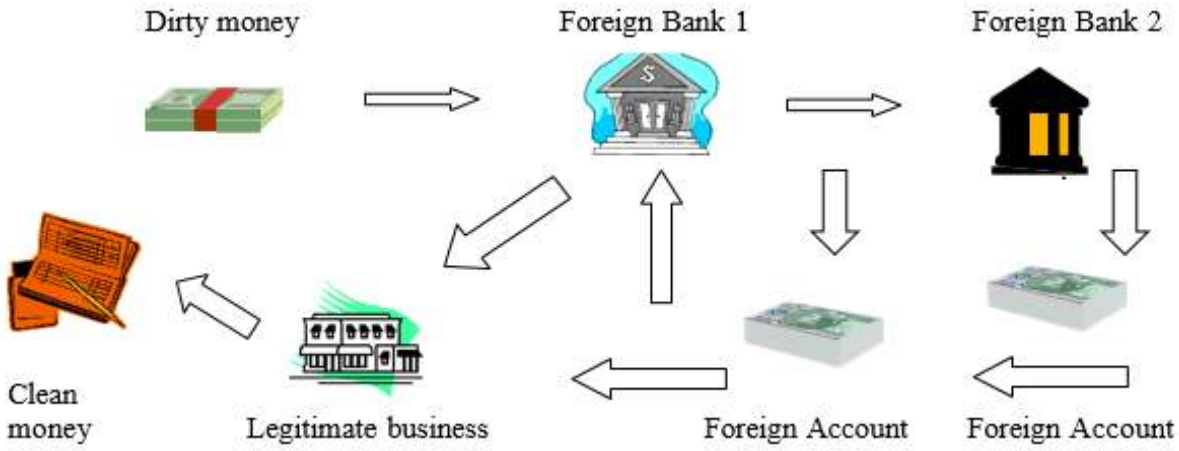
This method is designed to break up a large transaction into multiple smaller transactions in order to by-pass financial institution's reporting requirements. The reporting is referred to as "threshold reporting". In Vanuatu, the AML & CTF Act prescribes the threshold amount at VT 1,000,000.

Deposit transactions exceeding this threshold must be reported to VFIU. The money is deposited into one or more financial institutions by one person or a number of people.



Overseas banks

Money launderers often send money through various "offshore accounts" in countries that have bank secrecy laws, meaning that for all intents and purposes, these countries allow anonymous banking. A complex scheme can involve hundreds of bank transfers to and from foreign banks. According to the International Monetary Fund, "major offshore centers" include the Bahamas, Bahrain, the Cayman Islands, Hong Kong, Antilles, Panama and Singapore.

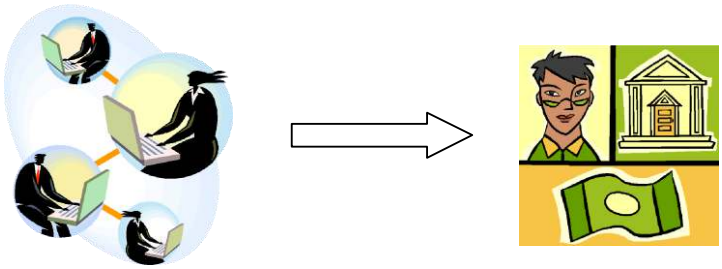


Alternative and Underground banking

Underground banking or alternative remittance systems are used in some parts of Asia because it leaves no audit trail. Money is not placed in traditional deposit taking institutions, such as banks, but is instead transmitted through underground banking systems such as fie chen in China[2]. Typically, the system involves the deposit of money in one country in exchange for a "cit" or "chop" (code). Money is paid in another country upon presentation of the chit. Alternative and underground banking systems are based on trust and family or social structures.

Electronic money transfers

The electronic transfer of money is a desirable money laundering technique given the fast movement of funds from one person or place to another.



Trusts

Trusts can be complicated structures involving a number of trustees and beneficiaries. It is possible to create a number of layers through the use of trusts, thereby obscuring or making difficult the identity of the underlying controller of the trust.

Gateway Intermediaries

The use of gateway intermediaries, such as lawyers and accountants is also attractive to money launderers. Money can be placed in holding accounts such as trust accounts which are in the name of the intermediary. The identity of the true owner of the funds is obscured and monies can be utilized for the purchase of assets such as real property. Those assets may then be sold to other persons and the sale proceeds received by the money launderer then become legitimate funds in the hands of the money launderer.

ANNEXURE 2

Legal Background of the Anti-Money Laundering and Counter-Terrorism Financing Act no. 13 of 2014 (AML & CTF Act)

Vanuatu is a member of the Asia/Pacific Group on Money Laundering (APG), a Financial Action Task Force (FATF)-style regional body. The Vanuatu Financial Intelligence Unit is the body charged with investigation into financial crime; it works closely with the Vanuatu Police Force.

The Financial Transaction Reporting Act (FTRA or FTR Act) of 2000 established the Vanuatu Financial Intelligence Unit (VFIU or FIU) within the State Law Office. Under the Anti-Money Laundering and Counter-Terrorism Financing Act No. 13 of 2014 with all its later amendments, the VFIU plays a role in ensuring compliance by the financial services sector with financial reporting obligations.

The purpose of the AML and CTF Act is to bring Vanuatu's anti-money laundering and counter-terrorist financing laws in line with the best international standard practice to combat money laundering and terrorism financing.

The AML and CTF Act also seeks to bring the Vanuatu legislation in line with the international standards set out by the Financial Action Task Force on Money Laundering ("FATF").

The Vanuatu Financial Intelligence Unit (VFIU) plays a role in ensuring compliance by the financial services sector with financial reporting obligations. Other anti-money laundering Regulators are the Public Prosecutors Office, the Reserve Bank of Vanuatu, the Vanuatu Financial Services Commission, and the Vanuatu Police Force.

Pursuant to the legislation, VFIU's has extensive powers. Several from those include the following:

(a) to compel the production of information or documents;
(b) to enter into premises under a monitoring warrant;
(c) to require an external audit or AML and CTF risk assessment;
(d) to provide remedial direction;
(e) to accept enforceable undertakings etc.

AML and CTF Act & Rules

The main legal acts regulating AML&CTF in Vanuatu are Anti-Money Laundering and Counter-Terrorism Financing Act No. 13 of 2014 and its accompanying Anti-Money Laundering and Counter-Terrorism Financing Regulation Order No. 153 of 2015 together with all their later amendments (hereinafter referred as the Rules).

It is responsibility of General Counsel and Chief Compliance Officer or its dedicated employee to update all employees of any changes in these acts via e-mail and during dedicated trainings.