TRANSACTION REPORTING AUTHORITY

ANTI-MONEY LAUNDERING GUIDELINE NO 1 OF 4

BACKGROUND

1. Introduction

The *Money Laundering and Proceeds of Crime Act 2000* was introduced to help detect and deter money laundering. Financial institutions and cash dealers are required by the Act to report suspicious transactions and establish record-keeping and compliance regimes. The Act also established a Transactions Reporting Authority (TRA) and by order dated 5 July 2001 the Attorney-General, with the approval of Cabinet, appointed the National Reserve Bank of Tonga (NRBT) as the TRA.

In terms of Section 11(1)(f) of the *Money Laundering and Proceeds of Crime Act 2000* the TRA may issue Guidelines to financial institutions. Guideline No 1 has been prepared to provide background information about money laundering and terrorist financing, including their international nature. It also provides an outline of the Tongan legislative requirements for a compliance regime, record keeping, client identification and sending reports to the TRA. In addition, it offers an overview of the TRA's mandate and responsibilities.

For more information about money laundering and reporting and other requirements under the Act, see the guidelines in this series:

* **Guideline 1 :Background** explains money laundering and its international nature. It also provides an outline of the legislative requirements as well as an overview of TRA's mandate and responsibilities.
* **Guideline 2 : Suspicious Transactions** explains how to report a suspicious transaction. It also provides guidance on how to identify a suspicious transaction, including general and industry-specific indicators that may help when conducting or evaluating transactions.
* **Guideline 3 : Customer Due Diligence** explains the requirement for financial institutions and cash dealers to identify their clients
* **Guideline 4 : Implementation of Compliance Regimes** explains the requirement for financial institutions and cash dealers to implement a regime to ensure compliance with their obligations under the *Money Laundering and Proceeds of Crime Act 2000*.

Throughout these guidelines, several references are provided to additional information that may be available on various Web sites. The TRA is not responsible for the accuracy or reliability of the information contained on these web sites.

2. What is Money Laundering?

The United Nations defines money laundering as any act or attempted act to disguise the source of money or assets derived from criminal activity. Essentially, money laundering is the process whereby "dirty" money-produced through criminal activity- is transformed into "clean" money, the criminal origin of which is difficult to trace.

There are three recognized stages in the money laundering process.

Placement involves placing the proceeds of crime into the financial system.

Layering involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the audit trail and the source and ownership of funds. This stage may involve transactions such as the buying and selling of stocks, commodities or property.

Integration involves placing the laundered proceeds back in the economy to create the perception of legitimacy.

Under Tongan law, a money laundering offence involves various acts committed with the intention to conceal or convert property or the proceeds of property (e.g. money) knowing or believing that these were derived from the commission of a serious offence. In this context, a serious offence means an offence that carries a maximum penalty that exceeds 12 months. It includes those relating to illegal drug trafficking, bribery, fraud, forgery, murder, robbery, counterfeit money, etc. The few exceptions are for offences that carry a lesser maximum gaol term or monetary penalties.

A money laundering offence may also extend to property or proceeds derived from illegal activities that took place outside Tonga.

3. Where does money laundering occur?

As money laundering is a necessary consequence of almost all profit generating crime, it can occur practically anywhere in the world. Generally, money launderers tend to seek out areas in which there is a low risk of detection due to weak or ineffective anti-money laundering programs.

4. How does money laundering affect business?

The integrity of the banking and financial services marketplace depends heavily on the perception that it functions within a framework of high legal, professional, and ethical standards. A reputation for integrity is one of the most valuable assets of a financial institution. If funds from criminal activity can be easily processed through a particular institution - either because its employees or directors have been bribed or because the institution ignores the criminal nature of such funds -the institution could be drawn into active complicity with criminals and become part of the criminal network itself. Evidence of such complicity will have a damaging effect on the attitudes of other financial institutions, and of regulatory authorities, as well as ordinary customers. In some countries concerns about weak anti-money laundering processes have lead to correspondent banks withdrawing facilities for clearance of cheques, telegraphic/wire transfers and processing of credit card transactions. This has not only impacted on the financial institution concerned but has affected a wide range of businesses that depend on the continuation of these payment channels for normal business operations.

As well as reputational risks in money laundering there are legal risks for the financial entities involved. There is heightened potential for law suits, adverse judgments, unenforceable contracts, fines and penalties generating losses, increased expenses for an institution, or even closure of such an institution. Legitimate customers may also be victims of a financial crime, lose money and sue the institution for reimbursement. There may be investigations, by banking or other law enforcement authorities resulting in increased costs, as well as fines and other penalties involved. Also, certain contracts may be unenforceable due to fraud on the part of the criminal customer.

5. What influence does money laundering have on economic development?

The International Monetary Fund (IMF) has cited inexplicable changes in money demand, prudential risks to bank soundness, contamination effects on legal financial transactions, and increased volatility of international capital flows and exchange rates due to unanticipated cross-border asset transfers as potential negative macroeconomic consequences of unchecked money laundering,

As with the damaged integrity of an individual financial institution, there is a dampening effect on foreign direct investment when a country's commercial and financial sectors are perceived to be subject to the control and influence of organised crime.

Money laundering proceeds can be utilized to control whole industries or sectors of the economy of certain countries. This increases the potential for monetary and economic instability due to the misallocation of resources from artificial distortions in asset and commodity prices. It also provides a vehicle for evading taxation, thus depriving the country of revenue.

6. Methods of Money Laundering

There are as many methods to launder money and the schemes being used are becoming increasingly sophisticated and complicated as technology advances. The following are some examples of common money laundering methods.

* *Nominees*

This is one of the most common methods of laundering and hiding assets. A launderer uses family members, friends or associates who are trusted within the community, and who will not attract attention, to conduct transactions on his or her behalf. The use of nominees facilitates allows the concealment of the source and ownership of the funds involved.

* *Structuring or smurfing*

Many inconspicuous individuals (commonly referred to as smurfs) deposit cash or buy bank drafts at various institutions, or one individual carries out transactions for amounts less than the amount that must be reported to the TRA, and the cash is subsequently transferred to a central account.

* *Asset purchases with bulk cash*

Individuals purchase big-ticket items such as cars, boats and real estate for cash. In many cases, launderers use the assets but distance themselves from them by having them registered in a friends or relatives name. The assets may also be resold to further launder the proceeds.

* *Exchange transactions*

Individuals often use proceeds of crime to buy foreign currency that can then be transferred to offshore bank accounts.

* *Currency smuggling*

Funds are moved across borders to disguise their source and ownership, and to avoid being exposed to the law and systems that record money entering into the financial system. Funds are smuggled in various ways (such as by mail, courier and body-packing) often to countries with strict bank secrecy laws.

* *Insurance products*

Illegally obtained funds may be used to purchase assets that are deliberately destroyed in order to allow the policyholder to receive "clean" claim money from an insurer

* *Gambling in casinos*

Individuals bring cash to a casino and buy gambling chips. After gaming and placing just a few bets, the gambler redeems the remainder of the chips and requests a casino cheque.

7. International Efforts to Combat Money Laundering

An important objective of money laundering activities is to remove the proceeds of crime from the jurisdiction in which they were obtained to help disguise their origins. This frequently involves the international movement of those proceeds, which is facilitated by the increasingly international character of business, financial and criminal activity. Although money laundering has become a large global phenomenon, jurisdictional boundaries have made international law enforcement difficult. International co-operation and co-ordination have become essential to the deterrence, detection and prosecution of money laundering, leading to the development of many international initiatives over the past decade to address this issue.

Perhaps the most well known of these initiatives is the Financial Action Task Force on Money Laundering (FATF), established by the G-7 countries in 1989. FATF is an intergovernmental body, comprising 31 countries and two regional organizations, whose purpose is to develop and promote policies to combat money laundering and terrorist financing. FATF has set out 40 recommendations that outline the basic framework for anti-money-laundering efforts and a further 9 recommendations relating to terrorist financing. These recommendations define international standards covering the criminal justice system and law enforcement, the financial system and its regulation, and international co-operation. More information about FATF and its recommendations can be found at http://www1.oecd.org/fatf/index.htm.

Other international anti-money-laundering initiatives include the following:

* Egmont Group of Financial Intelligence Units
* Asia Pacific Group on Money Laundering (APG)
* United Nations Single Convention on Narcotic Drugs
* United Nations Convention on Psychotropic Substances
* United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances

* United Nations Convention Against Transnational Organized Crime
* United Nations Convention against Corruption

For more information about:

Egmont Group refer to http://www.egmont.org/about_egmont.pdf
APG refer to http:// www.apgml.org/
United Nations Conventions refer to http://www.incb.org/e/conv/menu.htm.

For more information about money laundering, you can also refer to the following web sites:

* United Nations Office of Drug Control and Crime Prevention (http://www.odccp.org/money_laundering.html);
* Australian Transaction Reports Analysis Centre (http://www.austrac.gov.au/);
* International Money Laundering Information Network (http://www.imolin.org/);
* Moneylaundering.com (http://moneylaundering.com/)

8. Tonga's Legislation to Combat Money Laundering

The *Money Laundering and Proceeds of Crime Act 2000* has three key objectives:

* to implement specific measures to detect and deter money laundering and to facilitate investigation and prosecution of the related offences;
* to respond to the threat posed by organized crime by providing law enforcement officials with the information they need to deprive criminals of the proceeds of their criminal activities; and
* to support international efforts to fight multinational crime.

The specific measures include the following:

Record keeping and reporting. Financial institutions and cash dealers have to implement a compliance regime, keep certain records and establish client identities. They also have to report suspicious transactions to the TRA.

Suspicious Transactions. Financial institutions and cash dealers are required to report any transactions that give rise to suspicion within 3 days of forming the suspicion.

Creation of TRA. The TRA is responsible for collecting, analyzing and, in appropriate circumstances, disclosing information to law enforcement agencies for investigation. The TRA's mandate also includes enhancing public awareness and understanding of matters related to money laundering and providing training to financial institutions. The TRA also has responsibility for ensuring compliance with the compliance regime, reporting, record-keeping and client identification requirements.

In the process of conducting on-site examinations of licensed financial institutions for safety and soundness reasons the Reserve Bank will check compliance with AML requirements and attempt to ensure that the Tongan financial system is free from illegal money transfers. Over time, in its

TRA role, it will extend these on-site examinations to other financial institutions and cash dealers as provided for in the *Money Laundering and Proceeds of Crime Act 2000*

9. How to Contact the TRA

For further information on the TRA and its activities, and the guidelines, please contact

The Governor
National Reserve Bank of Tonga
Private Mail Bag No. 25
Nuku'alofa
Tonga

TRANSACTION REPORTING AUTHORITY

ANTI-MONEY LAUNDERING GUIDELINE NO 2 OF 4

SUSPICIOUS TRANSACTIONS

1. Introduction

The *Money Laundering and Proceeds of Crime Act 2000* was introduced to help detect and deter money laundering. Financial institutions and cash dealers are required by the Act to report suspicious transactions and establish record-keeping and compliance regimes. The Act also established a Transactions Reporting Authority (TRA) and by order dated 5 July 2001 the Attorney-General, with the approval of Cabinet, appointed the National Reserve Bank of Tonga (NRBT) as the TRA.

In terms of Section 11(1)(f) of the *Money Laundering and Proceeds of Crime Act 2000* the TRA may issue Guidelines to financial institutions. Guideline No 2 relates to suspicious activities.

A "financial institution" is defined in the *Money Laundering and Proceeds of Crime Act 2000* as any natural or legal person who carries on a business of:

(a) acceptance of deposits and other repayable funds from the public including for life insurance and investment related insurance;
(b) lending, including consumer credit, mortgage credit, factoring
(with or without recourse) and financing of commercial transactions;
(c) financial leasing;
(d) money transmission services;
(e) issuing and administering means of payment (such as credit cards, travellers' cheques and bankers' drafts);
(f) entering into guarantees and commitments;
(g) trading on its own account or on account of customers in money market instruments (such as cheques, bills, certificates of deposit), foreign exchange, financial futures and options, exchange and interest rate instruments, and transferable securities;
(h) underwriting share issues and participation in such issues;
(i) giving advice to undertakings on capital structure, industrial strategy and related questions, and advice and services relating to mergers and the purchase of undertakings;
(j) money-broking;
(k) portfolio management and advice;
(l) safekeeping and administration of securities;
(m) providing credit reference services; or
(n) providing safe custody services.

A "cash dealer is defined in the *Money Laundering and Proceeds of Crime Act 2000* as any natural or legal person who carries on a business of:

(a) an insurer, an insurance intermediary, a securities dealer or a futures broker;
(b) dealing in bullion, of issuing, selling or redeeming travellers' cheques, money orders or similar instruments, or of collecting holding and delivering cash as part of the business of providing payroll services;
(c) a gambling house, casino or lottery; or

(d) a trustee or manager of a unit trust.

2. Who must report Suspicious Transactions?

Any natural or legal person who carries on one or more of the businesses listed in 1 above must report suspicious transactions to the TRA in terms of Section 14(1) of the *Money Laundering and Proceeds of Crime Act 2000.*

3. What are suspicious transactions?

Suspicious transactions are transactions where there are reasonable grounds to suspect they relate to the commission of a serious offence.

A serious offence is defined broadly to include an offence against a provision of any law in Tonga or elsewhere that carries a maximum penalty which is greater than 12 months imprisonment. This includes most serious offences under Tongan law including drug trafficking, bribery, fraud, forgery, murder, robbery, counterfeiting, etc.

4. How to identify a suspicious transaction

A suspicious transaction may involve one or more factors that give rise to suspicion that the transaction is related to the commission of a money laundering offence.

The context in which the transaction occurs can be a significant factor in assessing suspicion. This will vary from one client to another. Transactions should be evaluated in terms of what is normal in Tonga, the financial institution's own business norms and what is known about the client.

Some of the factors that should be considered in assessing whether or not a transaction is suspicious are:

- the nature of, or unusual circumstances surrounding, the transaction;
- the known occupation or business background of the person conducting the transaction;
- attempts to use seemingly false identification in connection with any transaction, the use of aliases and a variety of similar but different addresses and an attempt to open or operate an account in a false name;
- admissions or statements of involvement in tax evasion or other criminal activities made to a financial institution or cash dealer or their employees or agents concerning a transaction;
- transactions involving known narcotic source or transit countries;
- transactions involving non-co-operative countries in the fight against money laundering and terrorist financing – see http://www1.oecd.org/fatf/NCCT/en.htm
- the behaviour of the person or persons conducting the transaction (e.g., unusual nervousness).

Examples of transactions that may give rise to suspicion are given in Attachment 1.

5. Obligation to report

Suspicious transactions regardless of amount must be reported. The requirement to report also extends to suspect transactions in forms other than cash; all transactions (such as telegraphic transfers, purchase of bank drafts or travellers cheques, etc.) are covered. The Act also encourages the reporting of a suspicious transaction, wherever possible, before it is carried out. A suspect transaction report can also be submitted on a transaction that was negotiated, but did not eventuate.

In terms of the *Money Laundering and Proceeds of Crime Act 2000* financial institutions and cash dealers are required to appoint a person to whom an employee is to report information relating to suspicious transactions.

Financial institutions and cash dealers must report suspicious transactions to the TRA as soon as possible but no later than 3 days after forming the suspicion.

Very severe penalties, including up to 2 years gaol, are provided in the *Money Laundering and Proceeds of Crime Act 2000* for failure to report suspicious transactions. There are also severe penalties for anyone who prejudices an investigation by informing ("tipping-off") another person that a suspicious transaction report is being, or has been, prepared. This does not mean that a financial institution or cash dealer should not seek to ascertain the source of funds or the precise nature of the transaction being undertaken or check whether an unusual transaction has a genuine commercial purpose.

6. What and where to report

Financial institutions and cash dealers must submit completed suspicious transaction reports in the format shown in Attachment 2 to:

The Governor
National Reserve Bank of Tonga
Private Mail Bag No. 25
Nuku'alofa
Tonga

7. Immunity

The Financial Institutions Act 2004 prohibits the disclosure of customer information other than limited circumstances. However, the *Money Laundering and Proceeds of Crime Act 2000* contains an overriding obligation to report information required by the Act regardless of the secrecy provisions imposed by any other law or otherwise.

In addition the *Money Laundering and Proceeds of Crime Act 2000* protects a financial institution or cash dealers or their officers, employees or other representatives, against any action, suit or proceeding in relation to the reporting process.

8. Further Information

For further information on the obligations to report suspicious transactions contact:
The Governor
National Reserve Bank of Tonga
Private Mail Bag No. 25
Nuku'alofa
Tonga

ATTACHMENT 1

EXAMPLE LIST OF TYPICAL SUSPICIOUS TRANSACTIONS

The following may give rise to suspicion in the absence of rational explanation in the light of customers' occupations, business details and other factors.

DEPOSITORY INSITUTIONS

Cash Transactions

1. Transactions where large deposits and withdrawals (including trading in securities, remittances and exchanges; the same hereinafter) are made in cash (including foreign currencies; the same hereinafter) or by cheque.

2. Transactions that are made frequently in short periods of time and accompanied by large deposits and withdrawals made in cash or by cheque.

3. Transactions where large amounts of small-denomination coins or bills (including foreign currencies) are deposited or exchanged.

4. Transactions involving large cash deposits into night safe facilities or rapid increases of amount.

Opening of New Accounts

5. Transactions involving customers who are suspected of having attempted to open accounts in fictitious names or in the names of other persons (including cases where accounts failed to be opened due to the absence of identifications or any other reason).

   Particularly, cases where customers act in the following ways with regard to their personal identification when opening their accounts:

   a. Cases where customers refuse to present their personal identification documents (including cases where customers desire to establish their identity through means other than their personal identification documents without any rational reasons).

   b. Cases where customers submit copies of their personal identification documents while refusing to present the originals.

   c. Cases where customers provide doubtful or unclear information.

   d. Cases where customers take procedure to open accounts in the names of other persons (including cases where bank officials in the personal identification process find that the customers taking procedures to open accounts are different from the persons whose names are to be used for the accounts)

6. Transactions involving accounts that are suspected of having been opened in fictitious names or in the names of other persons. Especially, cases where bank officials, during contact with customers after their accounts were opened, suspect faults in their

personal identification information (addresses, telephone numbers, etc.) that had been presented when opening the accounts.

7. Transactions involving accounts bearing the names of corporations that are suspected or never having existed. Especially, cases where bank officials, during contact with such corporations after their accounts were opened, suspect faults in their identification information (addresses, telephone numbers, etc.) that had been presented when opening the accounts.

8. Transactions involving customers who wish to have cash cards sent to destinations other than their addresses or refuse to have any bank notice sent to their addresses.

9. Transactions involving customers who have tried to open accounts by mail-order without success due to the absence of personal identification.

10. Transactions involving customers who attempt to open multiple accounts,.

11. Transactions involving customers who have been found to have multiple accounts.

12. Transactions involving customers who have no convincing reasons to make transactions at a particular branch. For example, such customers include those who, while being able to make transactions at branches close to their residence, are doing so at branches further away.

Transaction through Existing Accounts

13. Transaction involving accounts that have been used for large deposits and withdrawals during a short period of time after their opening and have then been closed or discontinued for any other transactions.

14. Transactions where large deposits and withdrawals are made frequently.

15. Transactions involving accounts that customers use for frequent remittances to a large number or people. Especially, cases where customers make large deposits into their accounts just before remittances.

16. Transactions involving accounts that customers use for receiving frequent remittances from a large number of people (especially, when customers make large remittances or withdrawals from their accounts just after receiving remittances),

17. Transactions involving accounts that have not been active for a long time and suddenly experiences large deposits and withdrawals.

18. Transactions that are unusual from the viewpoint of economic rationality. For example, cases where customers with large deposits refuse to invest them in higher-yield products.

Other Transactions

19. Transactions involving customers who jointly visit a financial institution and request different tellers to make large cash or foreign exchange deals.

20. Transactions involving customers who refuse to explain reasons or submit information when requested to verify the intended beneficiary and clear the suspicion regarding whether or not the customer is acting on its own behalf. These transactions include those that are made by representatives of customers and are expected to benefit other than the customers.

21. Transactions that are made by employees of financial institutions or their relatives to benefit parties that are unknown.

22. Transactions where employees of financial institutions are suspected of committing crimes

23. Transactions where deposits are made with forged or stolen money or securities and the customers are suspected of knowing that the money or securities are forged or stolen.

24. Transactions involving customers who emphasise the secrecy of the deals and customers who attempt to ask, force or bribe staff not to report deals to authorities.

25. Transactions that are identified as unusual by staff based on their knowledge and previous experience, and transactions involving customers whose attitudes or actions are identified as unusual by staff based on their knowledge and previous experience.

BUSINESSES INVOLVED IN TRADING BONDS AND OTHER SECURITIES

26. Transactions where customers bring in large amounts of bonds and/or other securities to sell them for cash.

27. Transactions where customers settle trading in bonds and/or other securities with cheques drawn by, or remittances from third parties

28. Transactions where customers attempt to buy large amounts of bonds for cash or cheques and then request to receive bond certificates while refusing to use depositary services without rational reasons.

BUSINESSES INVOLVED IN SAFE CUSTODY SERVICES

29. For cases involving the commencement of safekeeping deposit and trust transactions, refer to “Opening of New Accounts.” above

30. For cases involving the commencement of safety box use, refer to “Opening of New Accounts.” above.

31. Transactions where customers use safety box facilities frequently, unless they are found rational by bank officials in view of customers’ occupations, business details and other factors.

BUSINESSES INVOLVED IN MONEY TRANSMISSION SERVICES

32. Transactions in small amounts in an apparent effort to avoid triggering identification or reporting requirements.

33. Transactions where customers transfer large sums of money to overseas locations with instructions to the foreign entity for payment in cash.

34. Transactions where customers receive large sums of money from an overseas location via electronic funds transfer that include instructions for payment in cash.

35. Transactions where customers makes frequent or large electronic funds transfers for persons who have no account relationship with the institution.

36. Transactions where customers receive electronic funds transfers and immediately make a payment to a third party which is inconsistent with or outside the normal course of business for the client.

37. Transactions where customers instruct the financial institution to transfer funds abroad and to expect an equal incoming transfer.

38. Client shows unusual interest in electronic funds systems and questions limit of what amount can be transferred.

39. Transactions where customers send frequent wire transfers to foreign countries, but appear to have connection to destination country.

40. Transactions where sending entities having no apparent business connection with recipient.

41. Transactions where the size of electronic transfers is out-of-keeping with normal business transactions for that client.

42. Transaction which have no information about the beneficial owner or originator when the inclusion of this information would be expected.

43. Transactions where the stated occupation of the customer is not in keeping with the level or type of activity (for example a student or an unemployed individual who receives or sends large numbers of electronic transfers).

44. Transactions involving customers who are based in jurisdictions, which do not cooperate with international anti-money laundering efforts. ("Non-cooperative countries and territories (NCCTs)") or are shipping illegal drugs.

45. Transactions involving customers introduced by parties (including corporations) based in NCCTs or jurisdictions, which are shipping illegal drugs.

BUSINESSES WHO PROVIDE LOANS/FINANCIAL LEASES

46. Transactions involving customers who repay a problem loan unexpectedly.

47. Transactions involving customers who have loans to or from offshore companies that are outside the ordinary course of business of the client.

48. Transactions involving customers who offer large deposits or some other form of incentive in return for favourable treatment on loan request.

49. Transactions involving customers who seek to borrow against assets held by another financial institution or a third party, when the origin of the assets is not known.

50. Transactions involving customers who seem unconcerned with terms of credit or costs associated with completion of a loan transaction.

51. Transactions involving customers who apply for loans on the strength of a financial statement reflecting major investments in or income from businesses incorporated in countries known for highly secretive banking and corporate law and the application is outside the ordinary course of business for the client.

BUSINESSES INVOLVED IN FOREIGN EXCHANGE TRANSACTIONS

52. Transactions where the customer requests a foreign exchange rate that exceeds the posted rate.

53. Transactions where the customer wants to pay transaction fees that exceed the posted fees.

54. Transactions where the customer wants a cheque issued in the same currency to replace the one being cashed.

55. Transactions with counter parties in locations that are unusual for the client.

56. Transaction where the customer instructs that funds are to be picked up by a third party on behalf of the payee.

57. Transactions where the customer makes large purchases of travellers cheques not consistent with known travel plans.

58. Transactions where a large amount of foreign currency is exchanged to another foreign currency.

TRANSACTION REPORTING AUTHORITY

ANTI-MONEY LAUNDERING GUIDELINE NO 3 OF 4

CUSTOMER DUE DILIGENCE

1. Introduction

The *Money Laundering and Proceeds of Crime Act 2000* was introduced to help detect and deter money laundering. Financial institutions and cash dealers are required by the Act to report suspicious transactions and establish record-keeping and compliance regimes. The Act also established a Transactions Reporting Authority (TRA) and by order dated 5 July 2001 the Attorney-General, with the approval of Cabinet, appointed the National Reserve Bank of Tonga (NRBT) as the TRA

The *Money Laundering and Proceeds of Crime Act 2000* places an obligation on a financial institution to take reasonable measures to satisfy itself as to the true identity of any person seeking to enter into a business relationship with it (Section 12). This is an important element in the process of detecting and deterring money laundering. Financial institutions should also recognise that customer due diligence policies are an important element in overall risk management. Without adequate customer due diligence, financial institutions can be subject to reputational, operational, legal and concentration risks, which can result in significant financial cost.

A "financial institution" is defined in the *Money Laundering and Proceeds of Crime Act 2000* as any natural or legal person who carries on a business of :

(a) acceptance of deposits and other repayable funds from the public including for life insurance and investment related insurance;
(b) lending, including consumer credit, mortgage credit, factoring
(with or without recourse) and financing of commercial transactions;
(c) financial leasing;
(d) money transmission services;
(e) issuing and administering means of payment (such as credit cards, travellers' cheques and bankers' drafts);
(f) entering into guarantees and commitments;
(g) trading on its own account or on account of customers in money market instruments (such as cheques, bills, certificates of deposit), foreign exchange, financial futures and options, exchange and interest rate instruments, and transferable securities;
(h) underwriting share issues and participation in such issues;
(i) giving advice to undertakings on capital structure, industrial strategy and related questions, and advice and services relating to mergers and the purchase of undertakings;
(j) money-broking;
(k) portfolio management and advice;
(l) safekeeping and administration of securities;
(m) providing credit reference services; or

(n) providing safe custody services.

A "cash dealer is defined in the *Money Laundering and Proceeds of Crime Act 2000* as any natural or legal person who carries on a business of:

(a) an insurer, an insurance intermediary, a securities dealer or a futures broker;
(b) dealing in bullion, of issuing, selling or redeeming travellers' cheques, money orders or similar instruments, or of collecting holding and delivering cash as part of the business of providing payroll services;
(c) a gambling house, casino or lottery; or
(d) a trustee or manager of a unit trust.

In terms of Section 11(1)(f) of the *Money Laundering and Proceeds of Crime Act 2000* the TRA may issue Guidelines to financial institutions. Guideline No 3 relates to customer due diligence. It is based on principles outlined by the Basel Committee on Banking Supervision paper, "*Customer due diligence for banks*" issued in October 2001.

2. Definition of applicant

For the purposes of this guideline an applicant includes:

- The person or entity that seeks to establish or maintains an account with the financial institution or cash dealer ;
- The person or entity on whose behalf an account is to be established or maintained (i.e. beneficial owners);
- The beneficiaries of transactions conducted by financial institutions or cash dealers; and
- Any person or entity connected with a transaction who can pose a significant reputational or other risk to the financial institution or cash dealer.

3. When is identity verification required?

A financial institution or cash dealer should take reasonable steps to satisfy itself as to the true identity of any one seeking to enter into a business relationship or carry out a transaction or series of transactions.

Identity verification is required when an applicant is seeking to open a new account with a financial institution or cash dealer or simply undertaking a one-off transaction. Financial institutions and cash dealers should establish a systematic procedure for identifying new customers.

Where there is an existing business relationship further verification is not required if the applicant has already produced satisfactory evidence of identity. That said, financial institutions and cash dealers should ensure that records remain up-to-date and relevant, by undertaking regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place or when there is a material change in the way the account is operated.

In some exceptional circumstances, financial institutions cash dealers may rely on the procedures undertaken by other financial institutions or cash dealers when business is being referred. However, a financial institution or cash dealers should not rely on introducers that are subject to weaker standards than those governing its own procedures or that are unwilling to share copies of due diligence documentation. The following criteria should be met:

- The introducer must comply with minimum customer due diligence practices identified in this guideline;
- The customer due diligence procedures of the introducer should be as rigorous as those which the financial institution would have conducted itself for the customer;
- The financial institution or cash dealer must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer;
- The financial institution or cash dealer must reach agreement with the introducer that it will be permitted to verify the due diligence undertaken by the introducer at any stage; and
- All relevant identification data and other documentation pertaining to the customer's identity should be immediately submitted by the introducer to the financial institution or cash dealer, who must carefully review the documentation provided. Such information must be available for review by the Transaction Reporting Authority. In addition, financial institutions and cash dealers should conduct periodic reviews to ensure that an introducer that it relies on continues to conform to the criteria set out above.

While the transfer of an account in the applicant’s name in another financial institution or cash dealer subject to these guidelines may appear to provide some comfort, financial institutions and cash dealers should consider the possibility that the previous account manager may have asked for the account to be closed because of a concern about dubious activities. Enhanced rather than lesser due diligence procedures are appropriate in these circumstances.

In the absence of satisfactory identification an account should not be opened or a transaction conducted.

Financial institutions or cash dealers should include originator information and related messages on funds transfers that should remain with the transfer throughout the payment chain. Originator information should include name, address, and account number (when being transferred from an account). Financial institutions or cash dealers should give enhanced scrutiny to inward funds transfers that do not contain originator information. Should problems of verification arise that cannot be resolved, the financial institution or cash dealer should return the monies to the source from which they were received. It may also be appropriate, if the financial institution or cash dealer has reasonable grounds to suspect that the funds may be derived from illegal activities, for it to prepare a Suspicious Transaction Report and submit this report to the Transactions Reporting Authority.

As an exception to the above, transaction identifiers may be accepted where the originating bank is known to have adopted international best practice standards in AML/CFT. For transactions with high risk countries and remitters with unknown standards originator information must be obtained.

Very severe penalties, including up to 2 years gaol, are provided in the *Money Laundering and Proceeds of Crime Act 2000* for failure to establish the true identity of any applicant seeking to enter into a business relationship or undertake a transaction.

4. What are "reasonable measures"?

What is "reasonable" will depend on the circumstances. Obviously some types of customer are likely to pose a higher than average risk to a financial institution.

Financial institutions or cash dealers should develop clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk. It may help to develop a risk classification system which would act as a trigger for increased due diligence at commencement of customer relationship including identification as well as ongoing monitoring measures.

The *Money Laundering and Proceeds of Crime Act 2000* requires that specific consideration should be given to whether the applicant is based or incorporated in a country that has appropriate anti-money laundering measures (see list of non-compliant countries at http://www1.oecd.org/fatf/NCCT/en.htm) and the custom and practice in the relevant field of business.

Customer acceptance policies should also take into account factors such as the customers' background, occupation (e.g. Politically Exposed Persons – PEPs- see below), linked accounts, business activities or other risk indicators. For example, the policy may require only the most basic account-opening requirements for a working individual with a small account balance. On the other hand, quite extensive due diligence would be essential for an individual with a high net worth or whose source of funds is unclear. A decision to enter into a business relationship with a higher risk customer, such as a PEP, should be taken exclusively at senior management level.

5. General Identity Requirements

Financial institutions or cash dealer should obtain all information necessary to establish to their full satisfaction the identity of each applicant and the purpose and intended nature of the business relationship. The extent and nature of the information depends on the type of applicant (personal, corporate, etc.) and the expected size of the account.

The best documents for verifying the identity of applicants are official records that contain a photograph of the holder (examples are identity cards, passports and drivers licences) and are most difficult to obtain illicitly and to counterfeit. In these days of growing identity fraud, though, it is inadvisable to rely on only one form of identification.

Special attention should be exercised in the case of non-resident customers and in no case should a financial institution or cash dealer short-circuit identity procedures just because the new customer is unable to be present for interview. A financial institution or cash dealer should always ask itself why the customer has chosen to open an account in Tonga.

Financial institutions or cash dealers should retain evidence of a person's identity for at least five years after the last transaction.

6. Specific Identification Issues

Personal customers

For personal customers, financial institutions and cash dealers need to obtain and maintain the following information:

- Name and/or names used;
- Permanent residential address;
- Date and place of birth;
- Name of employer or nature of self-employment/business;
- Specimen signature; and
- Source of funds.

Financial Institutions and cash dealers should verify the information against original documents of identity issued by an official authority. Where there is face-to-face contact, the appearance should be verified against an official document bearing a photograph. Any subsequent changes to the above information should also be recorded and verified.

Corporate customers

Where the applicant is a body corporate the financial institution or cash dealer should obtain:

- The certificate of incorporation;
- The latest annual return to the Registrar of Companies;
- Business licence;
- Details of ownership;
- Constitution;
- a financial statement of the business or a description of the customer's principal line of business; and
- a letter/resolution appointing authorised signatories

The original documents or certified copies should be produced for verification. If significant changes to the company structure or ownership occur subsequently, further checks should be made. Authorised signatories on the business account must fulfil the identification requirements for personal customers.

Financial institutions and cash dealers should be vigilant in preventing corporate business entities from being used by natural persons as a method of operating anonymous accounts. Personal asset holding vehicles, such as international companies, may make proper identification of customers or beneficial owners difficult. A financial institution or cash dealer should understand the structure of the company, determine the source of funds, and identify the beneficial owners and those who have control over the funds.

Financial institutions and cash dealers should exercise care in initiating business transactions with companies that have nominee shareholders or shares in bearer form. Satisfactory evidence

of the identity of beneficial owners of all such companies should be obtained. In the case of entities that have a significant proportion of capital in the form of bearer shares, extra vigilance is required. A financial institution or cash dealer may be completely unaware that the bearer shares have changed hands. Therefore, financial institutions or cash dealers should put in place satisfactory procedures to monitor identity of material beneficial owners.

Other business customers

For other business customers, financial institutions or cash dealers should obtain:

- evidence of their legal status, such as a partnership agreement, association documents or a business licence;
- a description of the customer's principal line of business; and
- a letter/resolution appointing authorised signatories

The original documents or certified copies should be produced for verification. If significant changes to the business structure or ownership occur subsequently, further checks should be made. Authorised signatories on the business account must fulfil the identification requirements for personal customers.

Trust, nominee and fiduciary accounts

Trust, nominee and fiduciary accounts can be used to circumvent customer identification procedures. It is essential that the true relationship is understood. Financial institutions or cash dealers should establish whether the applicant is taking the name of another customer, acting as a "front", or acting on behalf of another person as trustee, nominee or other intermediary. If so, a necessary precondition is receipt of satisfactory evidence of the identity of any intermediaries, and of the persons upon whose behalf they are acting, as well as details of the nature of the trust or other arrangements in place. Specifically, the identification of a trust should include documentation setting out the trustees, settlors/grantors and beneficiaries.

Client accounts opened by professional intermediaries

When a financial institution or cash dealer has knowledge or reason to believe that a client account opened by a professional intermediary is on behalf of a single client, that client must be identified.

Some financial institutions or cash dealers hold "pooled" accounts managed by professional intermediaries on behalf of entities such as mutual funds, pension funds and money funds. Financial institutions or cash dealers also hold pooled accounts managed by lawyers, accountants or stockbrokers that represent funds held on deposit or in escrow for a range of clients. Where funds held by the intermediary are not co-mingled at the financial institution or cash dealer, but where there are "sub-accounts" which can be attributable to each beneficial owner, all beneficial owners of the account held by the intermediary must be identified.

Where the funds are co-mingled, the financial institution or cash dealer should look through to the beneficial owners. There can be circumstances where the financial institution or cash dealer may not need to look beyond the intermediary, for example, when the intermediary is subject to

the same regulatory and money laundering legislation and procedures, and in particular is subject to the same due diligence standards in respect of its client base as the financial institution. Financial institutions or cash dealers should accept such accounts only on the condition that they are able to establish that the intermediary has engaged in a sound due diligence process and has the systems and controls to allocate the assets in the pooled accounts to the relevant beneficiaries. In assessing the due diligence process of the intermediary, the financial institution or cash dealer should apply the criteria set out in paragraph 4 of item 3 above, in respect of introduced business, in order to determine whether a professional intermediary can be relied upon.

Where the intermediary is not empowered to furnish the required information on beneficiaries to the financial institution or cash dealer, for example, lawyers bound by professional secrecy codes or when that intermediary is not subject to due diligence standards equivalent to those set out in this guideline or to the requirements of the *Money Laundering and Proceeds of Crime Act 2000* or anti-money laundering legislation in other jurisdictions, then the financial institution or cash dealer should not permit the intermediary to open an account.

Politically exposed persons

Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose a financial institution or cash dealer to significant reputational and/or legal risks. Such politically exposed persons ("PEPs") are individuals who are or have been entrusted with prominent public functions, including heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations and important political party officials.

Accepting and managing funds from or initiating transactions on behalf of corrupt PEPs will severely damage the financial institution's or cash dealer's own reputation and can undermine public confidence in the ethical standards of Tonga's financial system. In addition, a financial institution or cash dealer may be subject to costly information requests and seizure orders from law enforcement or judicial authorities (including international mutual assistance procedures in criminal matters) and could be liable to actions for damages by the state concerned or the victims of a regime. Under certain circumstances, a financial institution or cash dealer and/or its officers and employees themselves can be exposed to charges of money laundering, if they know or should have known that the funds stemmed from corruption or other serious crimes.

Financial Institutions or cash dealers should gather sufficient information from an applicant, and check publicly available information, in order to establish whether or not the applicant is a PEP. Financial institutions or cash dealers should investigate the source of funds before accepting a PEP. The decision to open an account for, or transact o behalf of, a PEP should be taken at senior management level.

Non-face-to-face customers

Financial institutions and cash dealers are on occasion asked to open accounts for applicants who do not present in person for interview. This has always been a frequent event in the case of non-resident customers, but it has increased significantly with the recent expansion of postal, telephone and electronic banking. Financial institutions or cash dealers should apply equally

effective customer identification procedures and on-going monitoring standards for non-face-to-face customers as for those available for interview.

A typical example of a non-face-to-face customer is one who wishes to conduct electronic banking via the Internet or similar technology. The impersonal and borderless nature of electronic banking combined with the speed of the transaction inevitably creates difficulty in customer identification and verification. As a basic policy, the Transaction Reporting Authority expects that financial institutions or cash dealers pro-actively assess various risks posed by emerging technologies and design customer identification procedures with due regard to such risks.

In accepting business from non-face-to-face customers:

- Financial institutions or cash dealers should apply equally effective customer identification procedures for non-face-to-face customers as for those available for interview; and
- There must be specific and adequate measures to mitigate the higher risk.

Examples of measures to mitigate risk include:

- Certification of documents presented;
- Requisition of additional documents to complement those which are required for face-to-face customers;
- Independent contact with the customer by the financial institution;
- Third party introduction, e.g. by an introducer subject to the criteria established in paragraph 4 of item 3 above; or
- Seeking verification of the source of funds for the initial deposit, including sighting documentary evidence confirming the source of the funds.

Correspondent banking

Correspondent accounts that merit particular care involve the provision of services in jurisdictions where the respondent financial institutions or cash dealers have no physical presence. However, if financial institutions or cash dealers fail to apply an appropriate level of due diligence to such accounts, they expose themselves to the range of risks identified earlier in this paper, and may find themselves holding and/or transmitting money linked to corruption, fraud or other illegal activity.

Financial institutions or cash dealers should gather sufficient information about their respondent banks to understand fully the nature of the respondent's business. Factors to consider include: information about the respondent bank's management, major business activities, where they are located and its money-laundering prevention and detection efforts; the purpose of the account; the identity of any third party entities that will use the correspondent banking services; and the condition of bank regulation and supervision in the respondent's country. Financial institutions and cash dealers should only establish correspondent relationships with foreign banks that are effectively supervised by the relevant authorities. For their part, respondent banks should have effective customer acceptance and due diligence policies.

In particular, financial institutions or cash dealers should refuse to enter into or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group (i.e. shell banks). Financial institutions or cash dealers should pay particular attention when continuing relationships with respondent banks located in jurisdictions that have poor know your customer standards or have been identified as being "non-cooperative" in the fight against anti-money laundering. Financial institutions or cash dealers should establish that their respondent banks have due diligence standards consistent with the principles outlined in this guideline, and employ enhanced due diligence procedures with respect to transactions carried out through the correspondent accounts.

Financial institutions or cash dealers should be particularly alert to the risk that correspondent accounts might be used directly by third parties to transact business on their own behalf (e.g. payable-through accounts). Such arrangements give rise to most of the same considerations applicable to introduced business and should be treated in accordance with the criteria set out in paragraph 4 of item 3 above.

7. On-going monitoring of accounts and transactions

On-going monitoring is an essential aspect of effective know-your-customer procedures. Financial institutions or cash dealers can only effectively control and reduce risk if they have an understanding of normal and reasonable account activity of their customers so that they have a means of identifying transactions which fall outside the regular pattern of an account's activity. Without such knowledge, financial institutions or cash dealers are likely to fail in their duty to report suspicious transactions where they are required to do so under the *Money Laundering and Proceeds of Crime Act 2000*. The extent of the monitoring needs to be risk-sensitive. For all accounts, financial institutions or cash dealers should have systems in place to detect unusual or suspicious patterns of activity. This can be done by establishing limits for a particular class or category of accounts. Particular attention should be paid to transactions that exceed $10,000 or more or total more than $25,000 in any 4 week period in terms of Section 13 of the Act. Certain types of transactions should alert financial institutions and cash dealers to the possibility that the customer is conducting unusual or suspicious activities. They may include transactions that do not appear to make economic or commercial sense, or that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer. Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being "washed" through the account.

There should be intensified monitoring for higher risk accounts as per item 6 above. For higher risk accounts:

- Financial institutions or cash dealers should ensure that they have adequate management information systems to provide managers and compliance officers with timely information needed to identify, analyse and effectively monitor higher risk customer accounts. For example, the types of reports could include reports of missing account opening documentation, transactions made through a customer account that are unusual, and aggregations of a customer's total relationship with the financial institution or cash dealer.

- Financial institutions or cash dealers should develop a clear policy and internal guidelines, procedures and controls and remain especially vigilant regarding business relationships with PEPs and high profile individuals or with persons and companies that are clearly related to or associated with them. As all PEPs may not be identified initially and since existing customers may subsequently acquire PEP status, regular reviews of at least the more important customers should be undertaken.

When an account has been opened, but problems of verification arise in the banking relationship that cannot be resolved, the financial institution or cash dealer should close the account and return the monies to the source from which they were received. It may also be appropriate, if the financial institution or cash dealer has reasonable grounds to suspect that the account may have been for illegal purposes, to prepare a Suspicious Transaction Report and submit this report to the Transactions Reporting Authority.

8. Further Information or Assistance

For further information on customer due diligence contact:

The Governor
National Reserve Bank of Tonga
Private Mail Bag No. 25
Nuku'alofa
Tonga

TRANSACTION REPORTING AUTHORITY

ANTI-MONEY LAUNDERING GUIDELINE NO 4 OF 4

COMPLIANCE REGIME

1. Introduction

The *Money Laundering and Proceeds of Crime Act 2000* was introduced to help detect and deter money laundering. Financial institutions and cash dealers are required by the Act to report suspicious transactions and establish record-keeping and compliance regimes. The Act also established a Transactions Reporting Authority (TRA) and by order dated 5 July 2001 the Attorney-General, with the approval of Cabinet, appointed the National Reserve Bank of Tonga (NRBT) as the TRA.

In terms of Section 11(1)(f) of the *Money Laundering and Proceeds of Crime Act 2000* the TRA may issue Guidelines to financial institutions. Guideline No 4 relates to compliance regime obligations.

2. Who has to Implement a Compliance Regime?

If you are a financial institution or cash dealer you have to implement a compliance regime to comply with your reporting, record-keeping, client identification and staff training requirements.

A "financial institution" is defined in the *Money Laundering and Proceeds of Crime Act 2000* as any natural or legal person who carries on a business of:

(a) acceptance of deposits and other repayable funds from the public including for life insurance and investment related insurance;
(b) lending, including consumer credit, mortgage credit, factoring
(with or without recourse) and financing of commercial transactions;
(c) financial leasing;
(d) money transmission services;
(e) issuing and administering means of payment (such as credit cards, travellers' cheques and bankers' drafts);
(f) entering into guarantees and commitments;
(g) trading on its own account or on account of customers in money market instruments (such as cheques, bills, certificates of deposit), foreign exchange, financial futures and options, exchange and interest rate instruments, and transferable securities;
(h) underwriting share issues and participation in such issues;
(i) giving advice to undertakings on capital structure, industrial strategy and related questions, and advice and services relating to mergers and the purchase of undertakings;
(j) money-broking;
(k) portfolio management and advice;
(l) safekeeping and administration of securities;
(m) providing credit reference services; or
(n) providing safe custody services.

A "cash dealer is defined in the *Money Laundering and Proceeds of Crime Act 2000* as any natural or legal person who carries on a business of:

(a) an insurer, an insurance intermediary, a securities dealer or a futures broker;
(b) dealing in bullion, of issuing, selling or redeeming travellers' cheques, money orders or similar instruments, or of collecting holding and delivering cash as part of the business of providing payroll services;
(c) a gambling house, casino or lottery; or
(d) a trustee or manager of a unit trust.

3. What is a Compliance Regime?

A compliance regime should include the following:

- the appointment of a compliance officer;
- the development and application of compliance policies and procedures which are approved by the board in the case of Tongan incorporated entities and appropriate senior management in the case of foreign entities;
- establishment and maintenance of a record of all transactions of more than $10,000 or any series of transactions occurring in any 4 week period totalling $25,000 or more(Section 13(1)(a) of the *Money Laundering and Proceeds of Crime Act 2000)*;
- establishment and maintenance of evidence of a persons identity (Section 13(1)(b) of the *Money Laundering and Proceeds of Crime Act 2000*);
- internal procedures to make employees aware of Tongan anti money laundering requirements and procedures and provide appropriate training in the recognition and handling of money laundering transactions; and
- independent review by internal or external audit of compliance on at least an annual basis.

These six elements are keys to any effective system of internal controls and are expanded upon in the following sections.

4. Compliance Officer

The individual appointed will be responsible for the implementation of the compliance regime. The compliance officer should have the authority and the resources necessary to discharge his or her responsibilities effectively and should report, on a regular basis, to the board of directors or senior management, or to the owner or chief operator.

All staff should be aware of the identity of the compliance officer and report suspicious transactions to them for forwarding, if thought appropriate, to the TRA.

The compliance officer is responsible for:

- ensuring that internal policies and procedures are up-to-date and adequate for the task of identifying and deterring money laundering;
- ensuring that all relevant staff have access to up-to-date lists of persons of interest supplied by the TRA or international bodies involved in anti-money laundering and combating the financing of terrorism;
- analysing reports of suspect money laundering from staff and reporting suspicious transactions to the TRA within 3 days of the suspicion being formed;

- keeping a record of suspect transactions reported by staff and the actions taken or reasons for not pursuing the matter;
- reviewing on a daily basis transactions in excess of $10,000 or any series of transactions totalling $25,000 or more in a four week period;
- identifying high risk accounts and ensuring that additional monitoring is applied;
- ensuring that identity and transaction records are maintained for the required period under Tongan law; and
- ensuring that all relevant staff are trained and undergo refresher courses in money laundering methods and prevention no less frequently than annually.

5. Compliance Policies and Procedures

An effective compliance regime includes policies and procedures that are communicated, understood and adhered to by all within the financial institution who deal with customers or any property owned or controlled on behalf of customers. This includes those who work in the areas relating to customer identification, record keeping, and processing of transactions. They need enough information to process and complete a transaction properly as well as identify customers and keep records as required.

They also need to know when an enhanced level of caution is required in dealing with transactions, such as those involving countries or territories that have not yet established adequate anti-money laundering regimes consistent with international standards or higher risk customers.

Compliance policies must also establish internal reporting and review arrangements for large and/or suspicious transactions.

6. Training

Employees, agents or other individuals authorized to act for a financial institution or cash dealer must be trained in recognition of money laundering techniques, the entity's compliance policies, and reporting and record-keeping obligations. This includes staff at the front line responsible for opening new accounts, on-going contact with customers, processing transactions as well as senior management. The training should also extend to others who have responsibilities under the compliance regime, such as information technology staff involved in designing and implementing electronic or manual internal controls, the compliance officer and internal auditors.

New staff and those who move into relevant areas should receive anti-money laundering training as part of their induction process. Regular refresher courses – no less frequently than annually – should be conducted for all relevant staff.

When assessing training needs, the following elements should be covered:

- *Requirements and related liabilities:* The training should give those who need it an understanding of the reporting, client identification and record-keeping requirements as well as penalties for not meeting those requirements. For more information about these see other guidelines.
- *Policies and procedures:* The training should make employees, agents, or others who act for a financial institution aware of the internal policies and procedures for deterring and detecting money laundering and terrorist financing that are associated with their jobs. It should also give each one a clear understanding of his or her responsibilities under these policies and procedures.

Employees should understand that an account may only be opened in the true name of the account holder and that they cannot disclose that they have made a Suspicious Transaction Report. They should also understand that no criminal or civil proceedings may be brought against them for making a report in good faith.

- *Background information on money laundering and terrorist financing:* Staff need to understand that the financial institution or cash dealer is vulnerable to abuse by criminals laundering the proceeds of crime or by terrorists financing their activities. Training should include examples of how the financial institution or cash dealer could be used to launder illicit funds or fund terrorist activity.

A financial institution or cash dealer should maintain a record of the training received by particularly staff members in relation to AML/CFT. Financial Institutions and cash dealers should also regularly assess the AML/CFT knowledge and ability of staff, particularly those in critical positions. These assessments should feed into documented system for managing corrective/disciplinary action.

7. Record-keeping

A financial institution or cash dealer is required to keep records for a period of at least 5 years from the date the relevant transaction was completed or upon which action was last taken in respect of:

- Transactions of $10,000 or more, or any series of transactions in a 4 week period totalling $25,000 or more or the equivalent in foreign cash carried out by it; and
- The records of the supporting evidence and methods used to verify identity comprising either a copy of the evidence or information that would allow a copy to be obtained e.g. a driver's licence number.

The following information must be kept for the purposes of the first dot point above:

- The name, address and occupation (or where appropriate the business or principal activity) of the person conducting the transaction or on whose behalf it is being conducted;
- The method used to establish identity;
- The nature and date of the transaction;
- The amount involved (and if relevant the currency);
- The type and identifying number of the account with the financial institution or cash dealer involved in the transaction;
- The name of the drawer and payee of any negotiable instrument involved along with the amount and date of the instrument, the number of the instrument (if any) and details of any endorsements;
- The name and address of the financial institution or cash dealer and the officer, employee or agent who prepared the record.

8. Independent Review

Another component of a comprehensive compliance regime is an independent review of compliance policies and procedures to test their effectiveness an annual basis. This will help evaluate the need to modify existing policies and procedures or to implement new ones.

Several factors could trigger the need for more frequent review, such as changes in legislation, non-compliance issues, new services or products or new regulatory requirements.

The review should be conducted by an internal or external auditor. It should include interviews, tests and samplings, such as the following:

- interviews with those handling transactions and with their supervisors to determine their knowledge of the legislative requirements and the financial institution's policies and procedures.
- evaluation of the financial institution's or cash dealer's own policies and procedures, including legal and regulatory requirements.
- a review of the processes for identifying and reporting suspicious transactions including the handling of these by the compliance officer.
- a sampling and review of large transactions including their assessment and recording.
- a sampling of electronic funds transfers and the recording of such transactions.
- a test of the record-keeping system for compliance with the legislation, regulations and guidelines.
- a test of the client identification procedures for compliance with the legislation, regulations and guidelines.

The scope and the results of the review should be documented. Any deficiencies should be identified and reported to senior management or the board of directors. This should also include a request for a response indicating corrective actions and a timeline for implementing such actions.

If a financial institution or cash dealer does not have an internal or external auditor, a self-review should be conducted by an individual who is independent of the reporting, record-keeping and compliance-monitoring functions. This could be an employee or an outside consultant. The objective of a self-review is the same as the objective of a review conducted by internal or external auditors.

9. Further information

For further information on implementing a compliance regime contact:

The Governor
National Reserve Bank of Tonga
Private Mail Bag No. 25
Nuku'alofa
Tonga