BEST PRACTICE GUIDELINES FOR FINANCIAL INSTITUTIONS

Mainstream Banking, Lending, Deposit Taking, Insurance, Retail Investment, Casinos, Lawyers, Real Estate Agents and Sharebrokers

Issued by the New Zealand Police Financial Intelligence Unit
New Zealand Police National Headquarters
180 Molesworth Street, P O Box 3017
Wellington, New Zealand
Tel: + 64 4 474 9499
Fax: + 64 4 498 7405

CONTENTS

FOREWORD

Welcome to the **BEST PRACTICE GUIDELINES FOR FINANCIAL INSTITUTIONS**, issued to provide guidance to financial institutions in relation to the FINANCIAL TRANSACTIONS REPORTING ACT 1996.

These guidelines have two main objectives.

First, to help financial institutions understand and comply with their obligations as required by the Financial Transactions Reporting Act 1996 and second, to explain money laundering methods, as well as assist with identifying suspicious transactions.

For the most part, the information provided in these guidelines has been sourced directly from the Financial Transactions Reporting Act 1996 and undoubtedly, internal procedures in most financial institutions will already be in place.

Suggestions, examples and information from other agencies and legislation have also been included to either enhance existing procedures within financial institutions or in some cases, assist with their creation.

As with the previous GUIDANCE NOTES FOR FINANCIAL INSTITUTIONS, these guidelines include a section on Suspicious Transaction Guidelines. This section has been divided into four parts, specifically, GENERAL MAINSTREAM BANKING AND INVESTMENT, LICENSED CASINOS, PRACTISING LAWYERS and REAL ESTATE AGENTS.

Certain other money laundering methods and techniques have also been included in the General Information section of these guidelines, which describes alternative remittance systems, cash couriers, locations of specific concern and politically exposed persons.

While these issues are not directly relevant to financial institutions, they have been included simply to provide knowledge of the existence of other avenues that may potentially be used to launder illegal funds.

Similarly, given the current global environment in relation to terrorism, a separate section on Terrorist Financing has also been incorporated. As far as the Financial Transactions Reporting Act 1996 is concerned, however,

obligations on financial institutions only extend to verifying customer identity, retaining records and reporting suspicious transactions.

As a result of pending changes to legislation in relation to New Zealand's compliance with international standards concerning money laundering and terrorist financing, these guidelines will be updated again, once the proposed legislation is finalised.

In the meantime, it should be remembered that the definitive source of information on the law must always be the statutes and regulations themselves. If in doubt, the statute should be referred to or legal advice sought.

INTRODUCTION

The basic purpose of money laundering is to convert funds or assets derived from crime into seemingly legitimate funds or assets derived from honest sources. It essentially turns *dirty* money into *clean* money.

Money laundering transactions are often deliberately complex to make it difficult to trace the money back to its origins. Then again, a relatively simple transaction, such as changing New Zealand dollars into Australian dollars, has the same effect.

We all know that profit is the motivation behind most crime. Experience worldwide has shown that organised crime is particularly lucrative and generates considerably large amounts of money.

Money laundering, by virtue of its ability to disguise and legitimise illegal proceeds, enables criminals to keep their profits. It also provides the incentive and resources to continue offending. By depriving criminals of the monetary benefits of their activities, the motivation to offend is likely to diminish.

Internationally, the most significant initiative against money laundering is the United Nations Convention against *Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988*, often referred to as the *UN Convention* or the *Vienna Convention*.

Along with other legislative measures, the UN Convention requires signatories to legislate against the laundering of proceeds of drug offences and to provide legal mechanisms for the seizure and confiscation of assets derived from such offences.

New Zealand is a signatory to the UN Convention.

Similarly, the *Financial Action Task Force (FATF) on Money Laundering*, established in 1989, was a response to widespread drug offending in many countries.

The FATF is an independent, inter-governmental organisation that develops and promotes both national and international policies to combat money laundering and terrorist financing. The key purpose of this group is to generate the necessary political drive to create legislative and regulatory reforms in these areas.

In 1990, the FATF published a report, later revised in 2003, that incorporated *Forty Recommendations* which focussed on much needed improvements in national legal systems to facilitate counter-measures to combat money laundering. These recommendations were also intended to strengthen international co-operation in relation to this issue.

In 1991, New Zealand became a member of the FATF.

The FATF have called upon all countries to take the necessary steps and effectively implement procedures, to bring national systems into compliance with the recommendations.

Here is a link to the FATF Forty Recommendations.

Following the September 11 terrorist attacks on the United States in 2001, *Nine Special Recommendations* were also devised, which, when combined with the *Forty Recommendations*, outline the basic framework to detect, prevent and suppress terrorist financing.

Here is a link to the FATF Nine Special Recommendations.

Reporting by financial institutions of suspicious transactions is one of the cornerstones of the FATF recommendations. Law enforcement agencies throughout the world acknowledge that the successful investigation of money laundering offences depends largely on information received from the financial community.

Financial institutions are not being asked or expected to assume the role of law enforcers of money laundering. A positive approach to legislative requirements, however, will greatly improve the efforts of those agencies responsible for enforcement.

Working together is the key.

Throughout the remainder of these guidelines, the Financial Transactions Reporting Act 1996 will be referred to as the FTRA96.

The Financial Intelligence Unit (FIU) is available to assist financial institutions with any problems or questions arising from the FTRA96.

Please don't hesitate to call on (04) 474 9499.

Detective Senior Sergeant Ashley Kai Fong
Officer in Charge

Financial Intelligence Unit (FIU)
New Zealand Police

THE LAW ON MONEY LAUNDERING

INTERPRETATIVE NOTES

This section summarises the law in relation to money laundering, in particular the Crimes Act 1961 and the FTRA96.

The ultimate source of information on the law, however, must always be the statutes and regulations themselves. When in doubt, the statute should be referred to or legal advice sought.

There are currently four Acts of Parliament which have direct relevance to money laundering:

1. Crimes Act 1961
2. Financial Transactions Reporting Act 1996
3. Proceeds of Crime Act 1991
4. Mutual Assistance in Criminal Matters Act 1992

Penalties for failing to comply with the requirements of this legislation are significant.

Crimes Act 1961

Under this legislation, a money laundering offence is committed by engaging directly in a financial transaction or transactions for the purpose of concealing money derived from crime or having possession of money derived from crime with the intent to launder it.

Being *reckless* as to whether or not the property is the proceeds of a serious offence is also a violation of the Crimes Act 1961. *Recklessness* is described in more detail in the Suspicious Transaction Guidelines section.

The main offence (engaging in a money laundering transaction) is punishable by seven years imprisonment and the second (possession) by five years.

The legislation provides a defence to a charge on money laundering to any person who engages in a money laundering transaction in good faith for law enforcement purposes.

Money laundering

Under this legislation, it is an offence to:

- Engage in a financial transaction *knowing* or *believing* that the property involved is derived from any serious crime or be *reckless* as to whether this is the case.

- Any serious crime means any offence punishable by five years imprisonment or more, for example, drug offences, robbery, theft, fraud and others.

- Assist any person to conduct a transaction *knowing* or *believing* that the property is derived from any serious crime or be *reckless* as to whether this is the case.

- A money laundering transaction includes dealing with any property or assisting any other person to deal with that property for the purpose of concealing it or enabling any other person to conceal it.

- Obtain or possess any property (including money), which is derived from any serious crime, with the intention of engaging in a money laundering transaction *knowing* or *believing* the money or property is derived from any serious crime or being *reckless* as to whether this is the case.

  - Property includes land and personal property, cash, cheques, drafts, letters of credit, shares and insurance policies.

Financial Transactions Reporting Act 1996

This legislation imposes obligations on financial institutions including:

- Verification of customer identity, for example, when new accounts are opened, certain transactions conducted or where money laundering is suspected.

- Retention of transaction records and customer verification details.

- Reporting suspicious transactions.

It also provides for protection of the identity of people making suspicious transaction reports and immunity from liability of any breach of secrecy or customer confidentiality.

Obligations on financial institutions to verify identity

- Failure to verify the identity of customers, where the FTRA96 stipulates, is an offence. Working examples are provided in the Customer Verification section of these guidelines.

Financial institutions to report suspicious transactions

- If a transaction is conducted or attempted through a financial institution, and it is suspected that the transaction involves money laundering or the proceeds of crime, it must be reported to the Commissioner of Police.

  - Unless it is urgent, in which case it can be reported orally, a Suspicious Transaction Report (STR) must be made in writing either on the form supplied by the Police (see Appendix A) or any form in use by the

institution, as long as it contains all the sections outlined in the Schedule to the FTRA96 (see Appendix C). The STR should be forwarded to the FIU at New Zealand Police National Headquarters in Wellington.

Suspicious transaction reports not to be disclosed

- Where such a transaction is conducted or attempted, it is an offence to inform that person or any other unauthorised person that the transaction has been reported or that reporting is being considered. It is an offence to reveal the existence of an STR or a money laundering investigation with intent to prejudice the investigation or gain any advantage (monetary or otherwise). This offence is known as *tipping off*, which is explained in more detail in the Offences section of these guidelines.

  - The existence or consideration of an STR may only be disclosed to certain people who are authorised to receive such information.

  - Any person making an STR is protected from civil, criminal or disciplinary action in respect of any information contained in the report, unless the information was disclosed in bad faith.

  - The identity of any person making a report will not be revealed except for law enforcement purposes or on the order of a court.

Obligation to keep transaction records

- Transaction records are to be kept in a form that will allow a transaction to be completely reconstructed at any time by the Commissioner of Police.

Obligation to keep verification records

- Verification records must be retained in order to establish how customer identification was carried out.

  - It is not uncommon in legal transactions for the transaction to be carried out through a trustee, nominee or via one of several people and there will usually be a valid reason for this. It may be useful to keep a record of why the transaction was conducted in this way.

All records are to be kept for not less than five years. After the expiry of this period, however, records must be destroyed unless there is a lawful reason for retaining them.

Liability of employers and principals

- Employers and principals are liable for any offences committed by their employees.

- Principals and employers are liable whether or not the employee acted with their knowledge or approval.

- Employers and principals are liable for any offences committed by any person acting as their agent.

  - This liability applies unless the agent acted without the express or implied authority of the principals.

  - Employers and principals have a defence to these measures if they can demonstrate that they implemented measures to ensure their employees complied with the FTRA96. Further information is provided in the Defences section of these guidelines.

Proceeds of Crime Act 1991

The Proceeds of Crime Act 1991 provides for the restraining of assets derived from serious crime and their eventual forfeiture to the Crown following conviction. It also provides for the imposition of Pecuniary Penalty Orders which necessitate Crown assessment of the benefits derived from the commission of an offence, and may be enforced as if they were debts due from the offender to the Crown.

Mutual Assistance in Criminal Matters Act 1992

This legislation implements New Zealand's international obligations to facilitate requests to and by New Zealand for assistance in criminal investigations and prosecutions, including money laundering investigations and asset forfeiture actions.

Main Points of the Money Laundering Offence

The main points of the law in relation to money laundering are outlined below:

- The offence provisions apply to any person involved in the money laundering process, including:

  - The person who committed the original serious offence, from which the property was derived.

  - A person who *knowingly* or *recklessly* launders the proceeds of the offence, even if they were not involved in the original offence.

  - Any person who assists in the laundering process by being in possession of the proceeds of a serious offence with the intent to launder them.

- Where any person is prosecuted for a money laundering offence, proof that the person *knew* or *believed* or was *reckless* as to the proceeds being from a particular serious offence is not necessary. It is sufficient that they *knew* or *believed* that the property was the proceeds of any serious offence or were *reckless* as to whether this was the case.

- A person charged with a money laundering offence can not claim that he/she *believed* that the property was the proceeds of a particular offence when in fact it was derived from a different offence. The fact that the property is the proceeds of any serious offence is sufficient, as described in the case study below:

Name	*Crown v Wallace & Others*
Judges	*Giles J*
Court	*High Court, Auckland*
File Number	*T 139-98*
Judgment Date	*27 August 1998*
Subject	*CRIMINAL LAW: Money laundering arose out of large scale manufacture and supply of drugs operation run by appellant's husband involving at least $1.3 million. Charge a representative count. Appellant first time offender and pleaded guilty.*
Judgment	*"In my view s257A has to be applied according to its plain words. … It reflects Parliamentary intention to impose a criminal sanction on any person who deals with criminal proceeds. There is no requirement in the first limb of the definition of "conceal" for the Crown to prove an intent to conceal. In order to attract liability an accused has merely to "convert" property, knowing or believing that all or part of the property is the proceeds of a serious offence. The mere expenditure or consumption of tainted money, with no ulterior motive of concealment or any intention to see the money again, is caught by the statutory definitions contained in the section. It leads inexorably to the conclusion that the intention of Parliament was to attract criminal liability to such conduct"*[1]*.*
Statutes	*Crimes Act 1961 (s257A(2)/Criminal Justice Act 1985 (s21A).*

- One defence to a charge of money laundering is if the person charged proves that they were acting in good faith for the purposes of:

  - The enforcement or intended enforcement of Section 243 (money laundering) or any other provision of the Crimes Act 1961 or of any other act relating to a serious offence.

  - The enforcement or intended enforcement of the Proceeds of Crime Act 1991.

It is important to distinguish between *knowledge*, *belief*, *recklessness* and *suspicion*, which are discussed in more detail in the Suspicious Transaction Guidelines section.

[1]Verdicts and Judgment of Williams J, *Trial by Judge Alone: Money Laundering*, 16 November 2004.

If an institution or employee *knows* or *believes* that money involved in a transaction is the proceeds of crime and they proceed with the transaction they must do so on good faith for law enforcement purposes to avoid possible prosecution.

Again, the ultimate source of information on the law must always be the statutes and regulations themselves. When in doubt, the statute should be referred to or legal advice sought.

TERMINOLOGY

Understanding the meaning of some of the terms used throughout both the Crimes Act 1961 and the FTRA96, as they apply to money laundering legislation, will help with interpretation.

CRIMES ACT 1961

CONCEAL means to conceal or disguise property, including converting it from one form to another, as well as concealing or disguising the nature, source, location, disposition, or ownership of property or of any interest in it.

DEAL WITH means to deal with property in any manner and by any means including disposing of property, whether by way of sale, purchase, gift, or otherwise, transferring possession, or bringing property into or removing it from New Zealand.

INTEREST means a legal or equitable estate or interest in property; or a right, power, or privilege over property.

MONEY LAUNDERING TRANSACTION means dealing with any property that is the proceeds of a serious offence, or assisting any other person directly or indirectly to deal with any property for the purpose of concealing it or enabling any other person to conceal it.

PROCEEDS are any property that is derived or realised, directly or indirectly, by any person from the commission of a serious offence.

PROPERTY means real or personal property of any description, whether situated in New Zealand or elsewhere and whether material or not and includes an interest in any real or personal property. In dealing with the proceeds of serious offences, financial institutions will mostly deal with the property of money.

SERIOUS OFFENCE means an offence punishable by imprisonment for five years or more, and includes any act, wherever it is committed, which if committed in New Zealand would constitute an offence punishable by imprisonment for five years or more.

For a full list of definitions, refer to Part 10, Section 243 of the Crimes Act 1961.

FINANCIAL TRANSACTIONS REPORTING ACT 1996

The following list includes only those terms likely to be most often encountered by institutions and staff. Some of the definitions have been summarised to assist with understanding.

CASH means any coin or paper money that is designated as legal tender in the country of issue. It includes bearer bonds, travellers' cheques, postal notes and money orders. This definition applies to all except Part 5, Sections 37 to 43 of the FTRA96, which deals with the carriage of money across New Zealand's borders.

FACILITY means any account or arrangement that is provided by a financial institution through which a facility holder may conduct two or more transactions. It also includes, without limiting the general definition, a life insurance policy, membership of a superannuation scheme and facilities for safe custody, including a safety deposit box. The placement by a lawyer of funds in a locked deeds box or deeds safe for safe custody is included in the meaning of facility.

FACILITY HOLDER means the person in whose name the facility is established and also, without limiting the general definition, any person to whom a facility is assigned and any person who is authorised to conduct transactions through a facility. A person becomes a facility holder when he/she is first able to conduct transactions through the facility.

FINANCIAL INSTITUTION is defined in Part 1, Section 3 of the FTRA96. It is wide ranging and contains one particular clause (k), which encompasses a wide range of businesses and financial activities. This section should be referred to where there is any doubt as to whether a particular business or activity is defined as a financial institution.

The following entities are included in the definition of financial institution under the FTRA96:

- Accountants (within specified limits)
- Anyone carrying on the business of banking in New Zealand
- Building societies
- Friendly societies or credit unions
- Lawyers (within specified limits)
- Licensed casinos
- Life insurance companies
- New Zealand Racing Board
- Real estate agents
- Registered banks
- Reserve Bank of New Zealand
- Sharebrokers
- Trustees or managers of superannuation schemes
- Trustees or managers of unit trusts

- "Any person whose business or a principal part of whose business consists of any of the following: (i) borrowing or lending or investing money; (ii) administering or managing funds on behalf of other persons; (iii) acting as trustee in respect of funds of other persons; (iv) dealing in life insurance policies and (v) providing financial services that involve the transfer or exchange of funds, including (without limitation) payment services, foreign exchange services, or risk management services (such as the provision of forward foreign exchange contracts); but not including the provision of financial services that consist solely of the provision of financial advice", as per Part 1, Section 3(k) of the FTRA96.

LAWYER means a practitioner within the meaning of the Law Practitioners Act 1982. Enrolment is quite different from holding a practising certificate. As such, a qualified barrister and solicitor duly admitted although not holding a practising certificate, operating a business and receiving money on deposit or for investment or settling real estate transactions, would be a lawyer and a *financial institution* for the purposes of the FTRA96.

OCCASIONAL TRANSACTION means any transaction that involves the deposit, withdrawal, exchange or transfer of cash, as defined, and which is either not conducted through a facility or is conducted through a facility, even though the person conducting the transaction is not the facility holder.

PRESCRIBED AMOUNT means a monetary figure set from time to time by regulations to the legislation. When the amount is exceeded in certain transactions it triggers various responsibilities. The amount currently set in New Zealand is NZ$9,999.99[2].

PRINCIPAL FACILITY HOLDER means the facility holder(s) whom the financial institution reasonably regards, for the time being, as being principally responsible for the administration of the facility.

SUSPICIOUS TRANSACTION GUIDELINE means any guideline for the time being in force pursuant to Part 3, Section 24 of the FTRA96.

SUSPICIOUS TRANSACTION REPORT (STR) means a report made to the Commissioner of Police as required by Part 3, Section 15 of the FTRA96, which covers the obligations of financial institutions to report suspicious transactions.

TRANSACTION means any deposit, withdrawal, exchange or transfer of funds (in any currency) whether in cash, cheque, payment order or other instrument including electronic or other non-physical means. It also means, but is not limited to, any payment made in satisfaction, in whole or part, of any contractual or other legal obligation. It does not include the placing of a bet, participation in any game of chance, for example, Lotto, Instant Kiwi, or New Zealand based prize competition or any transaction specifically exempted under the regulations to the legislation.

---

[2]Refer to the *Financial Transactions Reporting (Prescribed Amount) Regulations 1996* for further information.

For a full list of definitions, refer to Part 1, Section 2 of the FTRA96.

CUSTOMER VERIFICATION

VERIFICATION REQUIREMENTS

The FTRA96 imposes duties on financial institutions as to when identification is necessary.

There are four main components, which are briefly outlined below:

- Identity *must* be verified when people apply to become facility holders for the first time, have an existing facility assigned to them or become a signatory on an existing facility.
  - Verification must be obtained before any new facilities are opened or changes made, unless it is impracticable to do so at the time, in which case, it must be obtained as soon as possible thereafter.
  - Where there are three or more facility holders, the identity of all of them need not be verified. It is sufficient to identify the principal facility holder or holders only.
  - In relation to transferring superannuation schemes, verification is not required, provided all members of the facility transfer simultaneously.
- Identity *must* be verified when people conduct occasional transactions when the amount of cash involved in a transaction exceeds the prescribed amount of NZ$9,999.99 or the New Zealand equivalent of a foreign amount.
  - Verification must be obtained if a person or persons appear to conduct a series of occasional transactions, where the total cash involved exceeds the prescribed amount of NZ$9,999.99 and the financial institution suspects that the transactions are being *structured*[3].
  - Verification must be obtained before the transaction is conducted, unless it is impracticable to do so at the time, in which case, it must be obtained as soon as possible thereafter.
- Identity *must* be verified when people conduct occasional transactions on behalf of other people when the amount of cash exceeds the prescribed amount of NZ$9,999.99.

[3] *Structuring* (also known as *smurfing*) refers to a process where a number of people are employed by a money launderer to conduct a series of transactions, all below the prescribed amount. The objective is to avoid customer verification requirements for transactions over the prescribed amount.

- Verification of the person conducting the transaction must be obtained, as well as the person on whose behalf the transaction is being conducted, regardless of whether they are present or not.

- Verification must be obtained before the transaction is conducted, unless it is impracticable to do so at the time, in which case, it must be obtained as soon as possible thereafter.

- Where a facility holder conducts a transaction on behalf of a non-facility holder, verification is only required for the non-facility holder.

The abovementioned requirements do not apply where a transaction is conducted on behalf of a person and the financial institution, through which the transaction is being conducted, believes that the person is the beneficiary of a trust and does not have a vested interest in the trust. An example of this would be where the person conducting the transaction is a trustee of a discretionary trust where the beneficiaries are yet to be established.

► Identity *must* be verified when people conduct a transaction or transactions that are considered suspicious by the financial institution, regardless of whether or not the transaction involves cash.

- The financial institution must verify the identity of the person if there are *reasonable grounds* to suspect that a transaction or proposed transaction is relevant to either the investigation or prosecution of any person for money laundering or enforcement of the Proceeds of Crime Act 1991. The financial institution must verify the identity of that person as soon as practicable.

One of the most important aspects of preventing money laundering is identification. By knowing your customer, breaches of the financial transactions reporting act 1996 can easily be avoided.

PROCEDURES FOR VERIFYING IDENTITY

Where a financial institution is required by the FTRA96 to verify the identity of a person, the verification must be carried out by means of documentary or other evidence that is reasonably capable of establishing the identity of that person.

Perhaps the only exception to verification requirements is where a person has an account at two different institutions and wishes to conduct a transaction from one account to the other. In this case, the first institution may rely on the fact that the second institution would have verified the person's identity at the time the facility was opened there. The only condition is that the first institution must satisfy itself that the other facility exists.

The FTRA96 is deliberately silent on the exact documentation considered reasonably capable of proving a person's identity. Not everyone owns a

passport or some people, due to citizenship status, may be unable to obtain a passport immediately. Likewise, in some cases, people may simply have no need for one.

As a general rule, institutions are required to verify identity from a document or documents obtained from a reputable and identifiable source, such as New Zealand Government issued identification, or by way of reference from a reputable and identifiable party.

In any case, the following list provides examples of possible forms of identification:

- ATM/credit card from another financial institution, only if signature is verified
- drivers licence
- passport
- refer to standard procedures as implemented by the financial institution

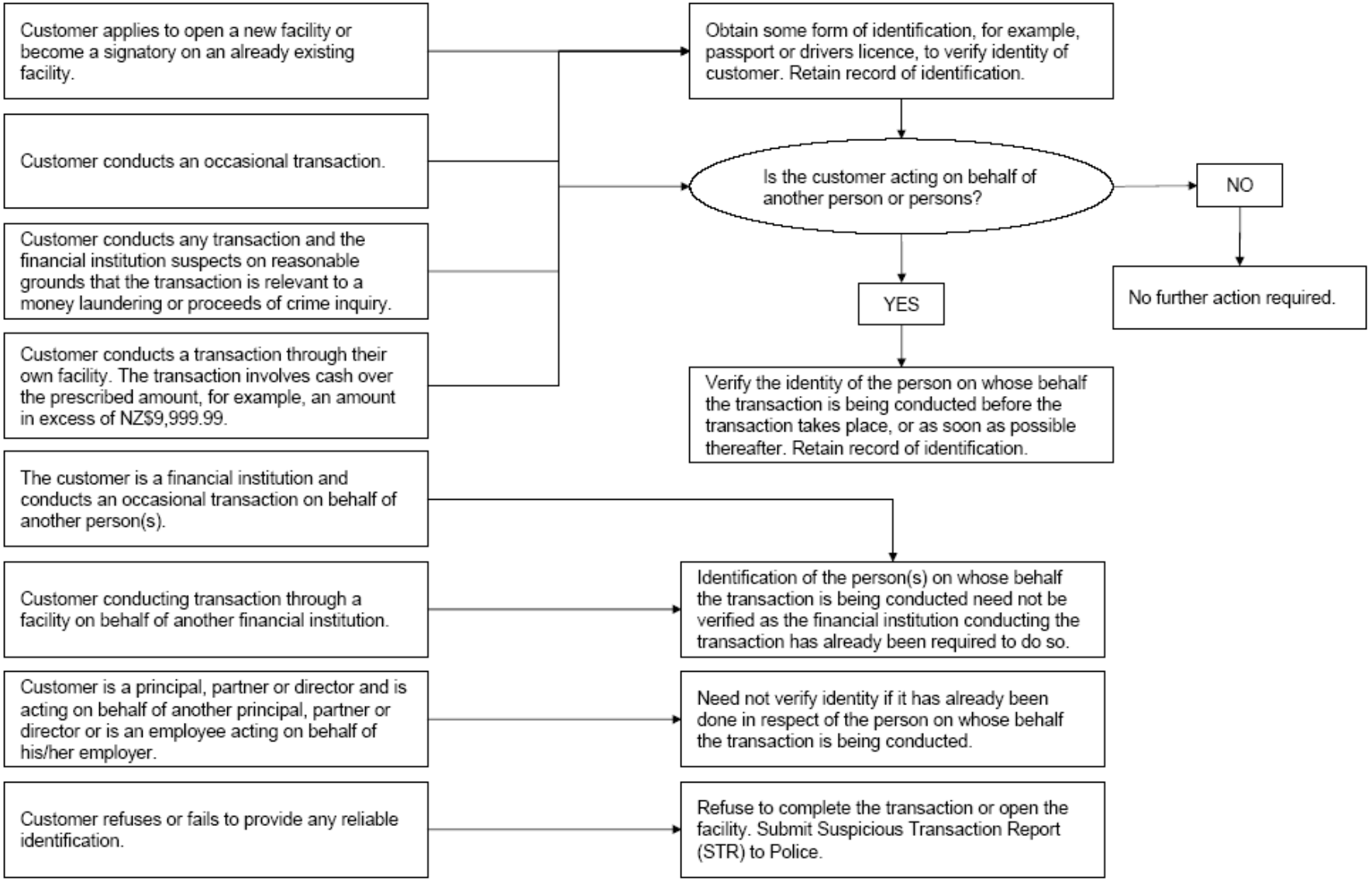
It is also advisable that secondary identification is taken. Certified photocopies or original utilities bills are also useful to verify addresses, for example, a telephone bill.

In a situation where there has been a significant time lapse between dealings with a particular customer, it may be sensible to renew the verification to ensure that the financial institution is dealing with the same person.

If a financial institution is unable to verify the customer or if the customer fails to provide any reliable identification, then the transaction must not be carried out and likewise, the account facility must not be opened. To do so would be a breach of the FTRA96.

It is recommended that only original or certified photocopies are accepted as appropriate forms of identification, for example, a photocopied passport endorsed by a justice of the peace.

SUMMARY OF CUSTOMER VERIFICATION FOR NEW ZEALAND FINANCIAL INSTITUTIONS



SUSPICIOUS TRANSACTION GUIDELINES

INTRODUCTION

The FTRA96 requires that suspicion of money laundering to be reported to the Police. Similarly, the Crimes Act 1961 prohibits the handling of funds for anyone suspected of laundering the proceeds of serious crime, except in specific circumstances, for example, to assist the Police with an investigation.

RECOGNISING MONEY LAUNDERING

In order for someone to commit a money laundering offence they must *know* or *believe* that the money involved in a transaction is the proceeds of crime. Note that the Crimes Act 1961 specifies that *belief* includes the concept of *recklessness*.

Recklessness means that a person involved in a financial transaction perceives a level of risk, however, continues with the transaction regardless.

Suspicion is not *knowledge* or *belief*. For that reason, if a transaction is carried out, even after a suspicion has been formed, the institution or employee is not committing any offence by being involved in it.

Likewise, where an institution or individual *knows* or *believes* that money involved in a transaction is the proceeds of crime, but continues with the transaction with the intention of reporting it, no allegation can be made later that the intent was to assist the money launderer.

Failure by financial institutions to comply with the law, that is, report suspicious transactions, may lead to prosecution. Furthermore, publicity in respect of assisting a money launderer may also irreparably damage personal and professional reputations.

With this in mind, it is essential to be vigilant to the possibility of money laundering, although, vigilance should not equate to paranoia. The law does not require anyone to play detective or presume all clients and prospective clients are money launderers unless the client can prove otherwise. **A common sense approach is vital**.

If suspicion is aroused in the normal course of business, it should not be ignored. Necessary steps should be taken to report any suspicions, according to appropriate procedures within the organisation.

It is essential, therefore, to have a basic understanding of how money laundering works, as well as possible indicators and techniques that may give rise to suspicion.

WHAT IS MONEY LAUNDERING?

Money laundering is the process by which criminals attempt to conceal the origins of their finances. If successful, it also allows them to maintain control

over those finances and ultimately provide an outwardly legitimate cover for their source of income.

In recent years, it has increasingly been recognised that an essential part of the *fight against crime* is to prevent criminals, wherever possible, from legitimising the proceeds of their activities by converting *dirty* money into *clean* money.

New money laundering methods are being devised constantly, some simple, some sophisticated. In a number of cases the amounts are relatively small, while others involve millions of dollars.

In most instances the money begins as cash, which, from a criminal perspective has the advantage of being anonymous. Unless marked or recorded in some way, it carries no indication of ownership or source and there is no question of its value.

SOURCES OF LAUNDERED MONEY

A high proportion of laundered money originates from drug trafficking, where cash is the normal medium of exchange. Cash is difficult to handle and move, however, in large amounts. In most business contexts, particularly in New Zealand, cash is rarely used and will generally attract attention if carried in sufficiently large amounts.

Drug trafficking and organised crime is big business. Some estimates have put the worldwide turnover in illegal drugs at over US$500 billion per annum, a figure which is comparable with the gross national product of many industrialised nations.

There are no official figures available in New Zealand to substantiate the amount of money generated by drug dealing and other crime, although, based on annual seizures and prosecutions, it is estimated to be in the hundreds of millions of dollars.

In addition to drug trafficking, substantial sums are laundered from crimes such as theft, robbery, burglary, fraud, receiving stolen goods, illegal prostitution, people smuggling, blackmail, extortion, racketeering and acts of terrorism.

THE THREE STAGES OF MONEY LAUNDERING

An effective money laundering operation normally follows three stages:

> ***Placement*** *introduces the illegitimate cash into the financial system.*
>
> ***Layering*** *involves undertaking multiple transactions to confuse the audit trail and separate the money from its origin.*
>
> ***Integration*** *introduces the laundered money into the legitimate economy, so that it appears to be normal business funds.*

If all three processes are successfully completed, the money will appear to have been legitimately obtained.

The main opportunity for identifying money laundering operations occurs at the *placement* and *layering* stages.

Both of these stages involve transactions that require contact between money launderers and financial institutions. This is particularly true at the *placement* stage.

Some simple examples of each of the three processes are outlined below.

Placement

The objective of *placement* is to move cash into the non-cash economy.

Methods of *placement* include, but are not limited to:

- Direct deposits of cash into a bank or other institution offering account services.
- Attempts to purchase insurance or investment products for cash, or to make part of the payment for them in cash.
- Cash purchase of high-value items such as gold, art, antiques, property, gambling chips or cars.
- Cash purchase of travellers' cheques, foreign currency, as well as telegraphic or wire transfers.

Layering

The objective of *layering* is to disguise the origin of the cash by carrying out many transactions between the *placement* of the cash and the final goal, which is *integration* of the illegitimate money into the legitimate economy.

Transactions of this kind may be revealed by their lack of normal commercial motive. If the only motive appears to be to carry out the transaction itself, and the result is likely to be uneconomic, there may be *reasonable grounds* for suspicion.

There is no standard *layering* procedure. The following example includes banks, insurance, foreign exchange and investment products and begins after the *placement* stage has been completed.

In the following scenario, the money is already in the form of a cheque:

> *The money launderer deposits the cheque into a bank account, opened using false identity. He/she then arranges for an associate to apply for an insurance policy. The premium for the policy, however, is paid by the money launderer through the associate.*

Shortly after having taken out the policy, the associate surrenders it, and the insurance company sends a refund cheque. This has the effect of transferring the money to another person in the form of a cheque from a respectable financial institution.

The associate then banks the cheque, possibly into his/her own account, and then withdraws the proceeds in a foreign currency once the cheque has been cleared and deposits the money into an account at another bank.

Over the next few weeks, the associate accumulates money in the bank account from other similar sources.

He/she then asks the bank to buy bonds from a securities house in another country. Bearer bonds are requested, so as to avoid registration.

The initial money launderer then applies for a loan from yet another bank on the security of the bearer bonds, which, with the consent of the associate, are transported to the bank from which the loan is requested.

This example demonstrates many different transactions and several breaks in the chain of ownership, all of which would make it difficult for an investigator to construct an audit trail.

Integration

The objective of *integration* is to assimilate the money into the legitimate economy in such a way that its criminal origins would never be suspected. The example below outlines a possible method of *integration*:

The money launderer locates a business that is trading well, but needs capital. He/she offers the business money in return for a share of the equity. As the business prospers, the money launderer puts in more funds, gradually buying out the original owners. Eventually he/she controls the business. In outward appearance it is a normal trading company. In reality its whole operation is based on criminal money.

RECOGNISING SUSPICIOUS TRANSACTIONS

It is difficult to define a *suspicious transaction*. As a general rule, however, a suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of customer.

WHAT IS A SUSPICIOUS TRANSACTION?

In the FTRA96, a suspicious transaction is referred to in the following terms:

Where any person conducts or seeks to conduct any transaction through a financial institution (whether or not the transaction or proposed transaction

involves cash) and the financial institution has *reasonable grounds* to suspect that the transaction or proposed transaction is or may be relevant to the:

- Investigation or prosecution of any person for a money laundering offence.
- Enforcement of the Proceeds of Crime Act 1991.

If a transaction is considered to be a suspicious transaction for the purposes of the financial transactions reporting act 1996, it must be reported to the Police.

POTENTIAL INDICATORS OF SUSPICIOUS TRANSACTIONS

As mentioned previously, the reporting by financial institutions of suspicious transactions is one of the cornerstones of the FATF Forty Recommendations and the successful investigation of money laundering offences depends largely on information received from the financial community.

As a normal part of daily business, financial institutions should be aware of indications that funds are being used for money laundering.

The next section provides examples of potentially suspicious or unusual activities. These examples have been broadly separated into the type of financial institution that is most likely to encounter a certain situation.

The section has been divided into four parts, specifically, **General Mainstream Banking and Investment**, **Licensed Casinos**, **Practising Lawyers** and **Real Estate Agents**, respectively.

Certain other money laundering methods and techniques have also been included in the General Information section of these guidelines. This information has been given simply to provide knowledge of the existence of other avenues that may potentially be taken to launder illegal funds. In most cases, however, they are not directly relevant to financial institutions.
Many of the situations described in these examples would be reasonably normal in some business contexts, whereas in others they would not. It is the *unusual* that should put financial institutions and their staff on alert.

It should be noted, however, that the existence of one of these activities alone may not necessarily mean that a transaction is suspicious. In this way, using a combination of common sense and intuition is advisable.

It is difficult to describe a suspicious transaction. As a general rule, it will often be one that does not make economic sense, or is inconsistent with a customer's business or personal activities.

GENERAL MAINSTREAM BANKING AND INVESTMENT

Examples of Suspicious Transactions

Account Transactions

Transactions conducted through accounts operated in the following circumstances may give reasonable grounds for suspicion:

- Customers who wish to maintain a number of trustee or client accounts that do not appear consistent with the type of business, including transactions involving nominee names.

- Customers who, for no apparent or logical reason, have numerous accounts and deposit cash to each of them in circumstances where the total credit, if or when combined together, would be a large amount.

- Customers who have active accounts with several financial institutions within the same locality, particularly when the institution is aware of a regular consolidation process from such accounts prior to a request for onward transmission of funds.

- Matching payments paid-out with credits paid-in by cash on the same or previous day.

- Payments in large third party cheques endorsed in favour of the customer.

- Customers who give conflicting information to different staff members.

- Large cash withdrawals from a previously inactive account, or from an account which has just received an unexpected large credit from abroad.

- Reluctance to use normal banking facilities, for example, avoiding high interest rate facilities for large balances.

- Large number of individuals making payments into the same account without adequate explanation.

- Customers who appear to be acting together, simultaneously using separate tellers to conduct large cash transactions or foreign exchange transactions.

- Company representatives who avoid contact with bank staff when opening accounts or making business transactions.

- Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client company and trust accounts.

A money launderer secures the co-operation of a trader whose takings are in cash. The trader banks criminal money along with normal takings and is paid a fee for each transaction.

Cash Transactions

Cash transactions involving the following types of activities may give reasonable grounds for suspicion:

- Company accounts that are dominated by cash transactions, for example, an absence of other monetary instruments normally associated with commercial businesses, such as cheques or credit cards.

- Frequent exchanges of cash into other currencies, where there appears to be no logical explanation for such activity.

- Transfers of large sums of money to or from overseas locations with instructions for payment in cash.

- Accounts operated by customers who refuse to provide appropriate identification or use misleading identification, or make it difficult to verify information. Bank accounts may be opened with forged documentation, which is difficult to detect.

- Several transactions conducted on the same day and at the same branch of a financial institution with a deliberate attempt to use different tellers.

- Cash deposits or withdrawals fall consistently just below occasional transaction thresholds. This practice is commonly referred to as *structuring* or *smurfing* and is often used to avoid threshold amounts that trigger identification requirements.

A drug dealer converts cash at a bureaux de change into larger denomination notes to reduce bulk. The money is then taken to another country where it is deposited into a bank account.

Complex and Unusually Large Transactions

Complex transactions often involve several different types of transactions or breaks in the chain of ownership of the funds. These types of transactions will normally have no apparent economic or obvious purpose. If it is suspected that a particular transaction is not legitimate, it should be reported and, as far as possible, the background and results be made available to assist the FIU if required.

Customer Characteristics

Unusual transactions that are out of character with known customer routines or behaviour may give reasonable grounds for suspicion:

- Stated occupation of an individual does not correspond with the type of transactions conducted.

- Unusual discrepancies in identification, such as, name, address or date of birth.

- Individuals involved in cash transactions who share addresses, particularly when the addresses are also business locations.

- Customers seemingly acting together simultaneously using separate tellers to conduct large cash transactions or foreign exchange transactions.

- Company representatives who avoid contact with bank staff when opening accounts or making business transactions.

- Funds generated by a business owned by individuals originating from the same country on the list of locations of specific concern[4] or involvement of several individuals originating from the same country on that list, acting on behalf of similar types of businesses. This also applies to individuals sending or receiving funds from locations of specific concern.

Deposits and Withdrawals

The following types of deposits and withdrawals may give reasonable grounds for suspicion:

- Inactive accounts that contain a minimal sum and then unexpectedly receive a deposit, or several deposits, followed by constant withdrawals that continue until the sum has been completely removed.

- Deposits that contain counterfeit notes or forged instruments, as well as cash that has an unusual appearance or smell.

- Large cash deposits using automatic teller machines (ATMs) or drop boxes to avoid direct contact with bank staff.

International Transactions

Off-shore international activity

The following types of off-shore international activity may give reasonable grounds for suspicion:

- Use of letters of credit and other methods of trade finance to move money between countries, where such trade is not consistent with the customer's usual business.

- Customers who make regular, large payments, including electronic transfers, that are unable to be clearly identified as genuine transactions to, or receive regular and large payments from, countries which are commonly associated with the production, processing or marketing of drugs; or tax haven countries.

- Build up of large balances, not consistent with the known turnover of customer's business, and subsequent transfer to accounts held overseas.

- Unexplained electronic fund transfers by customers on an *in-and-out* basis or without passing through an account.

[4]Refer to FATF Statement dated October 2008.

- Frequent cashing of travellers' cheques or foreign currency drafts, particularly if originating from overseas.

Wire Transfers

Wire transfers have long been considered one of the more popular and convenient means of transferring money across international borders. The speed and sheer volume in which wire transfers are carried out makes them an ideal mechanism for criminals to hide transactions.

Examples of potentially suspicious wire transfers include:

- Irregular and often small amounts transferred in an attempt to avoid identification or reporting requirements.

- Information concerning the originator is not provided.

- Multiple personal, business or non-profit organisation accounts are used to collect then channel funds to a small number of foreign recipients.

A business transfers criminal funds internationally with every appearance of legality, by acquiring false invoices from business partners abroad, or by using invoices from overseas subsidiaries.

Investment Related Transactions

The following types of investments may give reasonable grounds for suspicion:

- Purchase of securities to be held by the financial institution in safe custody, where this does not appear appropriate given the customer's apparent worth.

- Back-to-back deposit/loan transactions with subsidiaries or affiliates of overseas financial institutions in known drug trafficking areas.

- Requests by customers for investment management services (either foreign currency or securities) where the source of the funds is unclear or not consistent with customer's normal business activity or worth.

- Buying and selling a security for no discernible purpose or in circumstances that appear unusual.

An unemployed person receives and sends several wire transfers or makes daily maximum cash withdrawals at different locations over a wide geographic area.

Retail Investment Products

These examples have been structured around the basic processes within any investment business, for example, sales, dealing and settlements.

This list is not exhaustive and individual examples are not totally exclusive to any one type of industry or firm and should be read in their context and their applicability within the particular firm or business assessed.

Sales and dealing staff

New business

Compared to long-standing customers, new customers are more likely to be laundering money through an investment business by using one ore more accounts for a short period of time, as well as using false names and fictitious companies.

Investment may be undertaken directly with a New Zealand investment business or indirectly via an intermediary who doesn't ask too many awkward questions, especially in a jurisdiction where money laundering is not legislated against or where the rules are not rigorously enforced.

The following situations may give reasonable grounds for suspicion when presented individually or in conjunction with other circumstances. Additional inquiries may dispel, or confirm, such suspicions. Such transactions may include those that:

- Require customer identification, of a personal client, for whom verification of identity proves unusually difficult and who, for no apparent reason, is reluctant to provide details.

- Involve a corporate/trust client when there are difficulties and delays in obtaining copies of accounts or documents of incorporation, where these are required by the institution.

- Involve a client with no apparent reason for using the service, for example, clients with distant addresses who could find the same service closer to their home base.

- Are not normally conducted by the institution, however, the client insists on using the institution’s services when his/her needs could be more easily serviced elsewhere.

- Involve a new investor who is introduced by an overseas bank, affiliate or other investor, both of whom are based in countries where production of drugs or drug trafficking are prevalent, or the source of whose money is obscure.

- Involve an unknown counterparty.

Intermediaries

There are many clearly legitimate reasons for a client’s use of an intermediary. The use of intermediaries, however, does introduce further parties into the transaction, reducing its transparency and depending on the designation of the account, preserving anonymity. This is also a useful tactic which may be used by the money launderer to delay, obscure or avoid detection. Any

apparently unnecessary use of an intermediary in the transaction could give reason for suspicion.

Dealing patterns

The aim of the money launderer is to introduce as many layers as possible. This means that the money will come from a number of sources and pass through a number of different people or entities. Long-standing and apparently legitimate customer accounts may be used to launder money innocently, as a favour, or due to the exercise of undue pressure.

The following types of transactions may give reasonable grounds for suspicion:

- A large number of security transactions across a number of jurisdictions.
- Transactions not in keeping with the investor's normal activity, the financial markets in which the investor is active and the business that the investor operates.
- Buying and selling a security with no discernible purpose or in circumstances that appear unusual.
- Low grade securities purchased in an overseas jurisdiction then sold in New Zealand and high grade securities purchased with the proceeds.
- Bearer securities held outside a recognised custodial system.

Abnormal transactions

The following types of transactions may give reasonable grounds for suspicion:

- A number of transactions, carried out by the same counterparty, in small amounts of the same security, each purchased for cash and then sold in one transaction, the proceeds being credited to an account different from the original account.
- Any transaction in which the nature, size or frequency appears unusual. Early termination of packaged products, for example, at a loss due to front end loading, early cancellation, especially where cash had been tendered and/or the refund cheque is to a third party.
- Transfer of investments to apparently unrelated third parties with no explanation proffered.
- Transactions that are not in keeping with normal practice in the market to which they relate, for example, with reference to market size and frequency, or at off-market prices.

- Other transactions linked to the suspicious transaction, which could be designed to disguise money and divert it into other forms or other destinations or beneficiaries.

Settlements

Payment

Money launderers will often have substantial amounts of cash to dispose of and will use a variety of sources. Cash settlements through an independent financial consultant may not necessarily be suspicious, although, large or unusual settlements of securities, dealings or settlements in cash to a large securities house will usually provide good reason for further enquiry.

Examples of what may be unusual settlement payments include:

- A number of transactions, carried out by the same counterparty, in small amounts of the same security, each purchased for cash and then sold in one transaction.

- Large transaction settlements by cash.

- Payment by way of third party cheque or money transfers where there is a variation between the account holder, the signatory and the prospective investor.

- Purchases of shares through summary accounts held by banks with security houses. Such purchases show the bank and not the money launderer as the purchaser of the shares.

Delivery

Bearer securities, held outside a recognised custodial system, are portable and anonymous instruments, which may serve the purposes of the money launderer well. Presentation in settlement or as collateral may in some circumstances give reason for suspicion, as might settlement made by way of bearer securities from outside a recognised clearing system.

Disposition

As previously stated, the aim of money launderers is to take *dirty* money and turn it into *clean* money or to use it to finance further criminal activity, for example, more drug shipments. The aim of many criminals will be to remove the money from the country in which it originated so it can be passed on to other criminal elements where it is ultimately destined. The methods used will often be deliberately complex to make tracing the final beneficiaries difficult.

The following situations may give reasonable grounds for suspicion:

- Payment to a third party without any apparent connection with the investor.

- Settlement, either by registration or delivery, of securities to be made to an unverified third party.

- Abnormal settlement instructions including payment to apparently unconnected third parties.

Secured and Unsecured Lending

The following types of activities may give reason for suspicion:

- While it may be a source of relief to the lender when a customer, who has struggled with a loan or line of credit, suddenly repays in full, such an occurrence may, in some circumstances, be so unusual or unexpected that it may be considered suspicious.

- The early settlement of what appears to be a routine loan, however, may also lead to suspicion particularly if it involves cash. This is a classic money laundering technique that has been detected on numerous occasions overseas.

- A request to borrow against assets held by the financial institution or a third party such as another institution, where the origin of the assets is not known or the assets are inconsistent with the customer's standing.

- A request by a customer for the financial institution to provide or arrange finance where the source of the customer's financial contribution to a deal is unclear, particularly where property is involved.

Shell Companies

Shell or front companies can be purchased *off-the-shelf*. They consist of nothing more than the basic company documents, but can legally receive and pay out money. Money launderers use shell companies to give credence to bogus deals. Such entities may be more commonly referred to as *shelf companies* in New Zealand.

A money launderer may establish a company or companies in a country with an off-shore banking centre or tax haven. The company's articles of association allow it to conduct banking business, including foreign exchange. With the appropriate amount of capital it can actually register as a bank.

The company may then issue bearer shares, so that no-one will be able to identify the actual owner. Criminal money can then be deposited into the company, changed into other currencies and transferred abroad through regular channels.

The following case study outlines a relevant New Zealand situation:

> *In March 2001, an Auckland lawyer, operating his own practice, was approached by a client whom he knew only by his first name. To this day, the lawyer claims that this is the only information he knows about the person.*
>
> *Over a ten day period, the lawyer received four deposits of $100,000 from the person. Each time the lawyer received the money, he*

deposited it into his trust account held at a major bank in Auckland. The money was predominantly in $20 notes and the deposits were all made at the same branch. These deposits were recorded for credit against a company.

Three days after the last deposit was made, the lawyer wrote a trust account cheque to another lawyer's trust account. He then forwarded this cheque along with his client file to a second lawyer. The money was subsequently used to purchase real estate in Auckland. The cost of this real estate was just over $400,000.

Investigation into this matter revealed that the company was in fact a shelf company registered in Gibraltar. The identity of the person was also revealed. He had a history of drug offending.

It is not uncommon for an entity to be required quickly for the purpose of undertaking transactions, and the use of *shell* or *shelf* companies in most situations would not in itself be suspicious.

Again, it is the unusual which should give reason for suspicion. The use of a shelf company in a transaction where the use of such an entity appears unnecessary is, for example, somewhat suspicious.

One criminal organisation developed an empire of 500 shell companies for the purpose of creating paperwork as evidence of commercial activity, much of which was used for money laundering.

LICENSED CASINOS

Examples of Suspicious Transactions

Casino Transactions

Many of the following situations would be quite normal in some instances, where in others they may be unusual.

The following scenarios may give reasonable grounds for suspicion:

- Patrons wanting to exchange large quantities of low denomination notes for higher denominations. This type of activity is particularly suspicious if they do not seem to participate in any of the gaming activities or if they are known to staff to be involved in a business that would normally generate cheques or other instruments, rather than cash.

- Unusually large amounts of cash exchanged for chips made by a patron whose business is known by casino staff to normally generate cheques or other instruments, rather than cash.

- Frequent exchange of cash from other currencies to New Zealand dollars where there appears to be no logical reason for such activity.

- Patrons whose transactions contain counterfeit notes or forged instruments or whose cash has an unusual appearance or smell.

- Patrons conducting a number of separate transactions in an apparent attempt to avoid any of the requirements of the FTRA96, for example, a number of transactions under $9,999.99 to avoid customer identification requirements.

- A group of patrons who appear to be acting together and simultaneously, or within a short period of time, use separate cashiers to conduct large cash or foreign exchange transactions.

- Patrons purchasing large amounts of casino chips, do not gamble or do very little gambling and then attempt to cash the chips for a casino-issued cheque.

- Patrons buying-in with large amounts of cash at the tables or gaming machines, do not gamble and then cash out at the cashier's cage.

- Patrons making verbal statements as to their involvement in criminal activity.

- Patrons depositing cash, or making wire transfers, with no intention to wager.

- Patrons establishing and using cheque cashing facilities with no intention to wager.

A casino patron makes use of a gaming machine to exchange illicit notes by feeding the money into the machine and then cancelling the credit to obtain a casino cheque or other cash.

PRACTISING LAWYERS

Examples of Suspicious Transactions

Lawyers' Transactions

The following scenarios may give reasonable grounds for suspicion:

- A transaction is proposed, however, the client is not the person being dealt with. The client wants a lawyer to act on behalf of their niece or elderly relative, for example, who is unknown, not available for contact, and has not provided any instructions.

- A client requests a lawyer to hold a sum of money on the client's behalf, which is unrelated to any particular transaction or the provision of any legal services and where there is no other reasonable explanation for it being held by the lawyer.

- New client approaches a firm with a simple proposition. Once access has been gained to the firm's trust account, the proposal is radically changed or developed.

- Client uses lawyer's trust account for transactions that may be more appropriately conducted through a bank or other type of account.

- Client wants to deposit a sum of cash into a firm's trust account pending the proposed purchase of a house in New Zealand. The purchase never eventuates or falls through and the client requests a transfer of the funds to a third party without providing an adequate reason for the transfer.

- Payment to a lawyer by means of a cheque drawn on an account other than that of the client in circumstances where no sound reason is given for the third party making funds available.

- Clients or representatives providing conflicting information to different members of a law firm.

A client requests a number of trust accounts within a law firm, which are not consistent with his/her business or affairs, including transactions that involve nominees.

REAL ESTATE AGENTS

Examples of Suspicious Transactions

Real Estate Transactions

The following scenarios may give reasonable grounds for suspicion:

- Initial deposit is paid by purchaser with a large amount of cash.

- Initial deposit is paid with a cheque from a third party, for example, an associate or relative (other than a spouse).

- A purchaser uses a significant amount of cash to close a real estate deal.

- Property is purchased in the name of a nominee, for example, an associate or relative (other than a spouse).

- Purchaser refuses to put his/her name on any document associated with the property or uses a different name on contracts, agreements or deposit receipts etc.

- Client unsatisfactorily explains the last minute substitution of the purchasing party's name.

- Client purchases property without inspecting location.

A client purchases multiple properties within a short time period and appears to be indifferent regarding the location, condition and likely repair costs etc. of each property.

SUSPICION CHECKLIST

The following checklist outlines various warning signs that may indicate that a transaction is suspicious. It is not intended to be an exhaustive list. Not every unusual situation is automatically suspicious. Often there are innocent explanations for a person's behaviour.

For that reason, one single attribute may not necessarily give rise to suspicion, whereas when there are a number of indicators appearing together, further inquiry may be in order.

Similarly, many of the circumstances outlined below would be quite normal in some business situations. In others, however, they would be unusual and it is the unusual that should put financial institutions and their staff on alert.

As mentioned earlier, financial institutions are not expected to be detective agencies or take the stance that all clients are suspicious until shown otherwise. Some extra attention when faced with certain situations, however, may prove invaluable at a later time.

The following scenarios are not specific to any particular part of the financial sector and are intended only as a general guide.

Customer Transactions

Consider further inquiries when customers:

- Travel a great distance to use an institution's services, for no apparent or logical reason, when the equivalent is available much nearer to home.

- Insist on using an institution's services for transactions that are not within that particular institution's normal business and for which there are other firms with publicly acknowledged expertise.

- Are reluctant to co-operate with identity verification or provide false or misleading information or information that is difficult or expensive to verify.

Customer verification is a requirement of the financial transactions reporting act 1996. Reluctance to provide verification, however, is not necessarily suspicious in itself.

- Decline to provide information that in normal circumstances would make them eligible for credit, or for other banking services, that would be regarded as valuable.

- Wish to buy an insurance or investment product and are more interested in cancellation or surrender terms than long-term performance.

- Request a cancellation or surrender of a long-term investment shortly after arranging the contract, for no apparent or logical reason.

- Insist on entering into financial commitments that appear to be considerably beyond their means.

- Wish to invest significant amounts of money using cash, or top up payments using cash.

- Use a cheque drawn on an account, other than their own, in circumstances where there does not appear to be a logical reason why the person should be acting on another's behalf.

- Wish to make an investment that has no obvious purpose.

- Are happy to accept relatively uneconomic terms when, with a little effort, they could have a much better deal.

- Suddenly vary their pattern of insurance or investment, for example, ask for a lump sum contract when they have previously only invested in small, regular amounts.

- Ask for settlement to a third party where there appears to be no apparent reason for the investor to be acting on someone else's behalf and where it would appear simpler or more logical for payment to be made to the original investor.

Investment Transactions

Before entering into an investment transactions consider:

- Is the investor known personally? If not, what is known about him or her?

- Is the transaction in keeping with the investor's normal activity that is known to the financial sector business, the financial markets in which the investor is active and the investor's own business?

- Is the transaction in keeping with the normal practice in the market to which it relates, that is, with reference to market size and frequency?

- Is the role of any agent involved in the transaction unusual?

- Is the transaction to be settled in the normal manner?

- Are there any other transactions linked to the transaction in question that could be designed to disguise money and divert it into other forms or to other destinations or beneficiaries?

Employees/Agents And Money Laundering

The following is a very limited list of possible situations, which may lead to a belief that an employee or agent of a financial institution is involved with a money launderer to assist them in moving funds through that institution.

Money laundering involving employees and agents from financial institutions may include:

- Changes in employee characteristics, for example, lavish life styles or avoiding taking holidays.

- Changes in employee or agent performance, for example, the salesman selling products for cash has remarkable or unexpected increase in performance.

- Any dealing with an agent where the identity of the ultimate beneficiary or counterparty is undisclosed, contrary to normal procedure for the type of business concerned.

- Customers that always insist on dealing with the same employee, even for apparently routine business, may be money laundering. Customers may even cease trading with the institution for a period when the employee is away or change branches if the employee is transferred.

  In one case, the president of a bank facing serious problems agreed to provide money laundering services to a drug ring. He set up wire transfer arrangements for a number of businesses, using their borrowing arrangements with the institution. Under the president's guidance, no-one suspected anything irregular. The total scheme involved 17 banks, 21 businesses and 44 citizens. Eventually the emotional pressure was too much and he confessed, and US$53 million was recovered.

REPORTING MONEY LAUNDERING

When to Report

Transactions must be reported to the Police when any person conducts or seeks to conduct any transaction through a financial institution (whether or not the transaction or proposed transaction involves cash), and there are reasonable grounds to suspect that the transaction or proposed transaction is or may be relevant to the:

- Investigation or prosecution of any person for a money laundering offence.

- Enforcement of the Proceeds of Crime Act 1991.

An STR must be made as soon as practicable after a suspicion that a transaction involves money laundering or the proceeds of crime has been formed.

The financial institution should decide whether there are *reasonable grounds* for suspicion. Whether or not an STR should be made is also for the financial institution to decide. If there is doubt, advice from a supervisor, manager or the Police should be sought. Any internal instructions that organisations have in place regarding suspicious transaction reporting must be followed.

Important

No civil, criminal or disciplinary action can be taken by anybody for any breach of confidentiality or contract, unless information in an STR, in accordance with the provisions of the FTRA96, is disclosed to the Police in bad faith.

Acting in bad faith in making an STR may include, for example, submitting a report to the Police in an attempt to inconvenience someone.

If a report is made to the Police, or an institution is involved in a transaction that results in a report being made, the identity of anyone involved in the making of the report must not be revealed by the Police to anyone, except in very limited circumstances.

If the STR leads to court proceedings being brought against any person the identity of anyone involved in the making of the report can not be revealed unless the court orders otherwise.

Who to Report to

If a decision is made to complete an STR, the person directly involved in the transaction need not necessarily submit the report to the Police. Reports can be made to supervisors, managers or to people within the financial institution who are appointed to receive such reports. It is then the responsibility of that supervisor, manager or person so appointed to submit the report to the Police.

What to Report

Any STR made to the Police must, (as a minimum), contain all the information specified in the Schedule to the FTRA96, (see Appendix C). It must also contain a statement setting out the grounds on which the suspicion, that the transaction involved money laundering or the proceeds of crime, is based. It is important that as much relevant detail as possible is supplied in the report, for example, full names, addresses (business and residential), dates of birth and gender. Full names and addresses and full details of documents used for identification should be supplied where available. **Incomplete information is of limited value**.

Establishing the true identity or location of a person while armed with only one first name, a surname, a vague address, no date of birth and vague or non-existent identification details, is difficult and in many cases, impossible. This is particularly so if the person is not a New Zealand resident.

Provision of a physical description and/or a photograph, where available, will assist the Police considerably with identification, particularly if false details

have been provided at the time of a transaction. The standard Police STR form will assist in alerting institutions to the type of information that is preferred (see Appendix A).

How to Report

Unless urgent attention is required, reports must be made in writing to:

Commissioner of Police
C/- Financial Intelligence Unit (FIU)
New Zealand Police National Headquarters
P O Box 3017
Wellington

For standardisation purposes, the Police would prefer that the STR form supplied by the FIU is used. These forms are available free of charge from the FIU. It contains the information needed to develop the basis of an investigation and is tailored to suit Police databases. Use of this form, however, is not a requirement of the FTRA96. If an organisation has its own internal form for reports, that form may be used to report a suspicious transaction if it contains all the appropriate sections.

The FIU is authorised to receive reports on behalf of the Commissioner.

Reports should be mailed or faxed. They may be sent electronically (if agreement on the type of electronic transmission has first been reached with the FIU or Commissioner of Police).

The address, telephone and fax number of the FIU is on the STR form and on the first page of these guidance notes.

Oral Reporting

The FTRA96 requires reports be made to the Commissioner of Police in writing.

There is one exception, however, where the urgency of the situation requires a suspicious transaction report to be made orally to any member of the Police.

An oral report could be made when an institution's impression of a transaction has gone beyond *suspicion* and amounts more to *knowledge* or *belief* that the transaction involves the proceeds of crime.

> *An armed robbery of a lotto outlet where a large quantity of $5 and $10 notes were taken has occurred. The next morning a person appears at a bank branch wishing to change a large amount of $5 and $10 notes for $100 notes.*

In practice this means that if an institution thinks that a situation requires immediate Police attendance, they can make an oral report. Similarly, if it is considered that Police attendance is not required at the institution, but that the

Police should be made aware of a transaction as a matter of urgency, an oral report can and should be made.

If an institution feels that a situation warrants the immediate attendance of the Police the local District Police Station should be contacted.

In the case of bank branches and bureaux de change at airports, the airport Police should be contacted where possible.

If it is felt that immediate attendance by the Police is not required but the matter should be quickly brought to Police attention, the FIU may be contacted.

In each case that an oral report is made it is to be followed as soon as practicable by a written report to the FIU in the form normally used by the institution.

Auditors

Auditors are not financial institutions for the purposes of the FTRA96. This legislation does recognise, however, that auditors may in the course of their duties uncover transactions that they consider suspicious.

An auditor may report a transaction to any member of the Police, where in the course of carrying out the duties as an auditor, has *reasonable grounds* to suspect in relation to any transaction that:

- The transaction is or may be relevant to the investigation or prosecution of any person for a money laundering offence.

- The transaction is or may be relevant to the enforcement of the Proceeds of Crime Act 1991.

Reporting by an auditor is not required by the FTRA96, it is voluntary. There is no obligation to report to the Commissioner of Police. Voluntary reports may, however, be forwarded to New Zealand Police National Headquarters. This is the preferred option. The auditor may also report to any member of the Police.

The same protections against civil, criminal or disciplinary action provided for financial institutions are applicable to auditors.

If there is any doubt about whether or not to make a report, how to make one or whom to make it to, ask your supervisor, manager, head office, or the FIU at New Zealand Police National Headquarters.

OFFENCES

There are a number of offences, which can be committed by financial institutions and individuals, explained mainly in Part 3 of the FTRA96.

The penalties for breaches or non-compliance are quite severe. Financial institutions need to be familiar with the requirements of the legislation to avoid any possible breaches.

The legislation also contains provisions that make employers and principals of financial institutions vicariously liable for the actions of their employees and agents.

Suspicious Transaction Reporting

The following list outlines offences in relation to reporting suspicious transactions:

- Where any transaction is conducted or is attempted to be conducted through a financial institution and that institution is required to report the transaction to the Police, an offence is committed if the financial institution fails to report the transaction as soon as practicable after forming the suspicion.

- Where any financial institution commits an offence against the above, it is liable in the case of an individual for a fine of $20,000 and $100,000 in the case of a body corporate.

- When reporting a suspicious transaction, an offence is committed and a fine not exceeding $10,000 is liable, when a person:

  - Makes any statement which he/she knows is false or misleading in any way.

  - Omits from any statement, any matter or thing without which he/she knows that the statement is false or misleading in any way.

Customer Verification

The offences in relation to customer verification mirror the verification requirements explained in Part 2, Sections 6 to 11 of the FTRA96. These sections deal with failure to verify identity in the various circumstances where it is required.

Where any financial institution commits an offence against any of the provisions of Part 2, Section 13 of the FTRA96, it is liable in the case of an individual to a fine of $20,000 and $100,000 in the case of a body corporate.

Tipping Off

Part 3, Sections 20 and 22 of the FTRA96 are particularly important for financial institutions and their staff. The offences contained in them may, in some cases, be committed by employees as well as the institutions themselves.

These sections deal with what is commonly referred to as *tipping off*. A situation where an institution or employee alerts some unauthorised person to

the existence of an STR, the information in the report; or that the making of a report is contemplated.

The people who are permitted to deal with the information, and the circumstances under which they are permitted, are covered in Part 3, Section 20 of the FTRA96.

This section also deals with the supplying of false or misleading information in an STR. In the case of an individual, it is an offence punishable by six months imprisonment or a fine not exceeding $5,000. In the case of a body corporate, it is an offence punishable by a fine not exceeding $20,000 to knowingly contravene the provisions of Section 20.

Furthermore, Part 3, Section 22 of this legislation deals with the more serious situation of *tipping off* to gain some sort of advantage, pecuniary or otherwise, or to prejudice a money laundering investigation.

It is an offence punishable by two years imprisonment to tip off to gain an advantage or to prejudice a money laundering investigation.

- Where a financial institution has made, or is contemplating making, an STR that institution is not authorised to disclose the existence of the report, or that the making of a report is contemplated, to any person except:

  - The Commissioner of Police or any Police member authorised to receive such reports.

  - An officer, employee or agent of the financial institution, for any purpose connected with the performance of that person's duties.

  - A barrister or solicitor for the purpose of obtaining legal advice or representation in relation to the matter.

  - The Reserve Bank of New Zealand, for the purpose of assisting the RBNZ to carry out its functions under Part V of the Reserve Bank of New Zealand Act 1989.

- No officer, employee or agent of a financial institution to whom disclosure of information has been made, is permitted to disclose information to any person other than another officer, employee or agent of the financial institution for the purposes of performing the first mentioned person's duties or obtaining legal advice or representation in relation to the matter.

  - No barrister or solicitor to whom disclosure of information has been made is permitted to disclose that information to any person other than another barrister or solicitor for the purpose of giving legal advice or making representations in relation to the matter.

- Depending on the protection of identity of persons making suspicious transaction reports, nothing in Part 3, Section 20 of the FTRA96 prevents the disclosure of any information in connection with, or in the course of, proceedings before a court.

- Every person commits an offence that knowingly contravenes any of the provisions mentioned above and is liable, in the case of an individual, to imprisonment for six months or a fine of $5,000 or, in the case of a body corporate, to a fine of $20,000.

- Every person commits an offence who, for the purpose of obtaining, directly or indirectly, an advantage or pecuniary gain for him or herself or any other person, or with intent to prejudice any investigation into the commission or possible commission of a money laundering offence, contravenes any of the provisions above. A person who commits an offence against this section is liable for imprisonment for a term not exceeding two years.

- Every person commits an offence who, being an officer, employee or agent of a financial institution, and having become aware that any investigation into any transaction or proposed transaction that is the subject of an STR is being or may be conducted by the Police, and knowing that he/she is not authorised to disclose the information:

  - Either for the purpose of obtaining, directly or indirectly, an advantage or pecuniary gain for him or herself or any other person.

  - With intent to prejudice any investigation into the commission or possible commission of a money laundering offence, discloses that information to any other person.

  - A person who commits an offence against this section is liable for imprisonment for a term not exceeding two years.

Record Keeping

The offences in relation to record keeping mirror the record keeping requirements contained in Part 4, Sections 29 to 31 of the FTRA96. These sections deal with failure to keep records in the various circumstances where they are required.

Offences for failure to comply with record keeping requirements are contained in Part 4, Section 36.

Where any financial institution commits an offence against any of the record keeping provisions, it is liable in the case of an individual for a fine of $20,000 and in the case of a body corporate, $100,000.

Liability of Employers and Principals

The presence of vicarious liability makes it essential for principals and managers of institutions to be aware of the requirements of the legislation and

to ensure that their employees and agents are also. These requirements are covered in Part 6, Section 53 and 54 of the FTRA96.

- Employers and principals are liable for any acts done or omitted by employees whether or not the act or omission was done with the knowledge or approval of the employer or principal.

- Where any person is acting as the agent of another, then that other person is liable for any acts or omissions of the agent unless the acts or omissions were done by the agent without the authority, either express or implied, of the principal, either before or after the event.

- Where any body corporate is convicted of an offence against the FTRA96 or any regulations made under the legislation, every director or officer involved in the management of the body corporate is also guilty of the offence if it is proved that the act or omission that constituted the offence took place with the knowledge, authority, permission or consent of the director or manager.

PROTECTIONS

Protection of Persons Reporting Suspicious Transactions

- Where any information is disclosed by any person in any suspicious transaction report, as required by the reporting obligations under the FTRA96, no civil, criminal or disciplinary proceedings may rest against that person in respect of the disclosure, or any consequences that may follow, unless the information was disclosed in bad faith.

- Where any information is disclosed by an auditor, as required by the reporting obligations under the legislation, the same protections apply, unless the information was disclosed in bad faith.

- Part 3, Section 17 of the FTRA96 offers complete immunity for financial institutions and their staff for disclosure of information that might normally be covered by professional privilege, customer confidentiality or contractual requirements, unless the information was disclosed in bad faith.

Section 17 is not restrictive with regard to what information is covered; it extends to any information disclosed or supplied in a suspicious transaction report.

Immunity from Liability for Disclosure of Information

- Where any person does any act that, apart from the defence section of the Crimes Act 1961, would constitute a money laundering offence.

- In respect of the doing of that act, that person would have a defence to a charge under that section.

- That person discloses, to any member of the Police, any information relating to the money laundering transaction or suspected money laundering transaction.

- That information is disclosed, in good faith, for the purpose of or in connection with the enforcement or intended enforcement of the criminal law.

- That person is otherwise under an obligation to maintain secrecy in relation to, or not to disclose, that information, then, notwithstanding that the disclosure would otherwise constitute a breach of that obligation of secrecy or non-disclosure, the disclosure by that person, to that member of the Police, of that information is not a breach of that obligation of secrecy or non-disclosure or (where applicable) of any enactment by which that obligation is imposed.

Identity Protection when Reporting Suspicious Transactions

While offering similar protections as Part 3, Section 17 of the FTRA96, this section differs in a number of significant ways. It applies to any person, not just a financial institution or an employee, who finds him or herself confronted with a transaction in which they know or believe to be a money laundering transaction.

If they proceed with the transaction in circumstances which make the defence under Section 244 of the Crimes Act 1961 available and then report the transaction to the Police, they are entitled to similar protections as if they had made a suspicious transaction report under Section 15 of the FTRA96.

Any disclosure made under Part 3, Section 18 of the FTRA96, may be made to any member of Police and does not need to be in any particular form. This section applies to any information provided in an STR and also any information that, if disclosed, will, or is reasonably likely to, identify any person who has handled a transaction that has resulted in a suspicious transaction report.

- No member of the Police, having received such information, is permitted to disclose that information to anyone except for law enforcement purposes.

- If an STR results in court proceedings, none of the information covered by this section of the legislation can be disclosed, except on the order of the Judge or the person presiding at the proceedings.

The circumstances under which a Police Officer might disclose information are limited principally to matters involving offences of money laundering or the Proceeds of Crime Act 1991. Such disclosures would normally occur internally in the course of investigations. Protection of the identity of people lodging an STR will always be a priority in such investigations.

Legal Professional Privilege

The general principal concerning legal professional privilege is that lawyers are not required to disclose any privileged communication, as per Part 3, Section 15 of the FTRA96.

- For the purposes of Part 3, Section 19 of the legislation, a communication is a privileged communication only if it is:
  - A confidential communication, whether oral or written, passing between a lawyer and another lawyer (both of whom are acting in their professional capacity), a lawyer and his/her client, whether directly or through the agent of either.
  - Made or brought into existence for the purpose of obtaining or giving legal advice or assistance.
  - Not made or brought into existence for the purpose of committing or furthering the commission of some illegal or wrongful act.
- Where the information consists wholly or partly of, or relates wholly or partly to, the receipts, payments, income, expenditure, or financial transactions of a specified person (whether a lawyer, his/her client, or any other person), it shall not be a privileged communication if it is contained in, or comprises the whole or part of, any book, account, statement or other record prepared or kept by the lawyer in connection with a trust account of the lawyer within the meaning outlined in the Law Practitioners Act 1982.
- For the purposes of Section 19, references to a lawyer include a firm in which he/she is a partner or is held out to be a partner.

DEFENCES

There is a defence to a charge of money laundering contained in the Crimes Act 1961 and a number of defences in the FTRA96. The defences occur in the area of customer verification, suspicious transaction reporting and the liability of employers and principals.

Customer Verification

It is particularly important that staff members are aware of the requirements in relation to this part of the legislation.

Should a financial institution wish to take advantage of the defence provided by Section 14 of this legislation, it will need to demonstrate that it had internal procedures in place to ensure compliance and that staff were aware of, and trained, in those procedures.

This does not mean, however, that the staff member who failed to comply with the law has this defence.

- Where any charge is brought against a person or corporation under the customer verification requirements of the FTRA96, the defendant has a defence to the charge if it is proved that:
  - All reasonable steps were taken to ensure that the person or corporation complied with that part of the legislation.
  - In the circumstances of the particular case, the person or corporation could not reasonably have been expected to ensure compliance.
- Where any such charge is brought against a person or corporation, the court will consider a number of factors in determining whether or not the legislation was complied with, including the:
  - Nature of the financial institution and its business.
  - Existence and adequacy of any procedures established by the institution to ensure compliance, including staff training and audits to test the effectiveness of procedures.

Employers and Principals

It is important for employers and principals of organisations that are covered by the legislation, to ensure that staff members are aware of the requirements of the FTRA96, particularly in relation to procedures and compliance.

Without such measures in place, employers and principals may be held equally liable for any non-compliance by staff.

- Where any charge is brought against an employer or principal as a result of the actions of employees, the employer or principal has a defence if he/she proves that they performed whatever steps reasonably practicable to prevent such actions.

Privacy Act, Search Warrants, Contractual Obligations

There are a number of miscellaneous provisions in the FTRA96. These are briefly summarised below:

Application of the Privacy Act (S 28)

This section sets out, for the purposes of the Privacy Act 1993, what purposes information collected in suspicious transaction reports may be used by the Police. The use of such information is essentially confined to money laundering investigations, the enforcement of the Proceeds of Crime Act 1991 and the administration of the Mutual Assistance in Criminal Matters Act 1992.

Search warrants (S 44 to 51)

There is a specific provision in the FTRA96 for the Police to obtain a search warrant to search for and seize anything which is or may be evidence of an offence against this legislation. The sections set out the conditions, under which a search warrant might be used, the form the warrant is to take, powers conferred by the warrant, duties and responsibilities of persons executing

search warrants, how things seized are to be dealt with and specific provisions for dealing with things seized from lawyers' offices.

Non-compliance not excused by contractual obligations (S 55)
This section states that the provisions of the FTRA96 have effect despite anything to the contrary in any contract or agreement. Also that nothing in any contract or agreement excuses compliance with any of the provisions of this legislation.

GENERAL INFORMATION

Alternative Remittance Systems

Alternative remittance systems are best described as financial services, operating outside of traditional financial sectors. They allow funds to be moved from one geographic location to another, without any money actually moving. Also known as underground banking, these systems are often referred to as a money or value transfer service, hawala, hundi, fei-chien and the black market peso exchange.

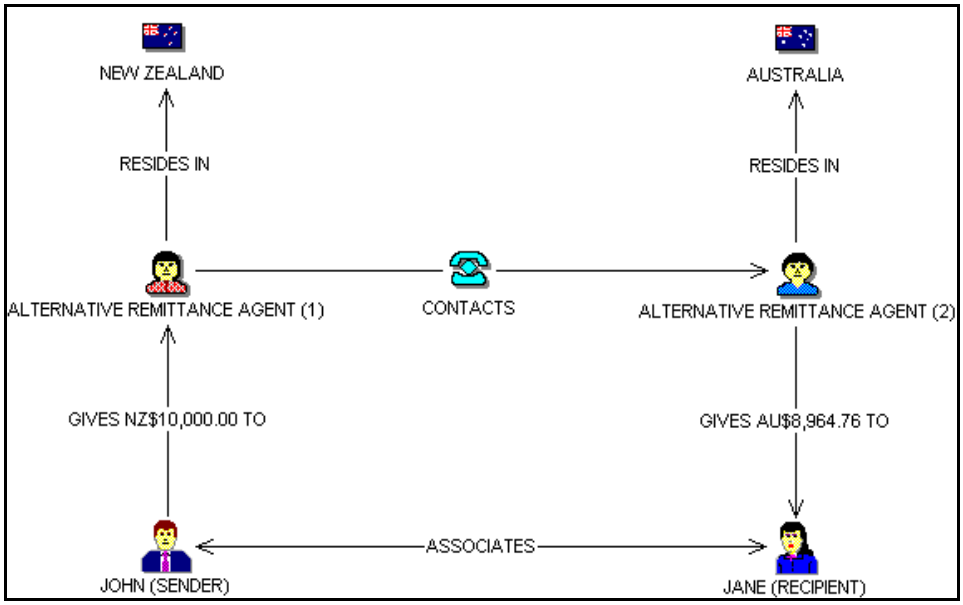
Essentially, alternative remittance systems allow for funds to be sent anonymously, accommodating money launderers and terrorist financiers by allowing them to send funds without having to provide identification. In some cases, few or no records are retained and in others, records are inaccessible to authorities. This makes it extremely difficult to trace funds after the transaction has taken place. **Running a remittance business in this way is in breach of the FTRA96**.

To bring New Zealand into line with international standards, alternative remittance agents will soon also need to be registered. Consequently, they will be required to demonstrate compliance with all FATF recommendations relevant to financial institutions.

Alternative remittance agents transfer money, usually across borders, without the physical or electronic transfer of funds. For a negotiated fee, an alternative remittance agent receives an amount of cash in one country and an alternative remittance agent in another country disperses an equivalent amount of cash, usually in local currency, to a recipient. This system relies almost entirely on the trust shared between the two remittance agents. The chart below outlines basic processes involved in alternative remittance systems:

> *In the following example, John (sender) lives in New Zealand and Jane (recipient) lives in Australia. John wants to send NZ$10,000 to Jane. John contacts alternative remittance agent (1) in New Zealand who contacts alternative remittance agent (2) in Australia. The agents negotiate a competitive conversion rate and commission. The agreed amount is then forwarded to Jane in the equivalent of Australian dollars, without the funds physically crossing the border.*

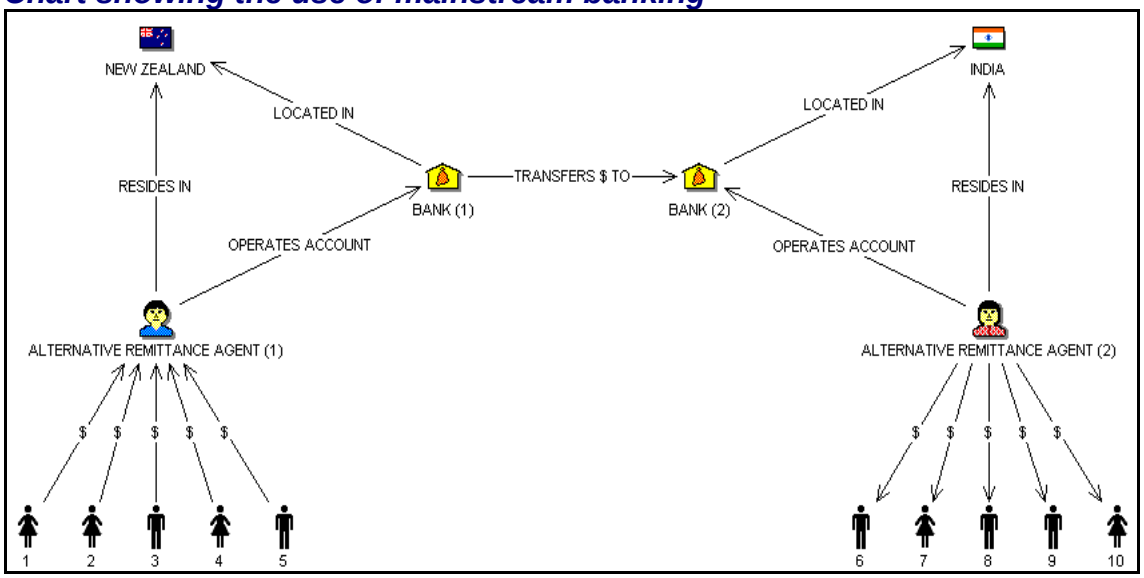
Chart showing process of alternative remittance systems



Alternative remittance agents may also utilise mainstream banking as demonstrated in the chart below:

In the following example, alternative remittance agent (1) is a New Zealand resident. He owns and operates a New Zealand bank account. He receives money from clients 1 to 5 wanting to transfer funds to India. One transfer is made to a bank account in India, which is owned and operated by alternative remittance agent (2). The funds are then distributed to recipients 6 to 10.

Chart showing the use of mainstream banking



In cases where mainstream banking is used by alternative remittance agents, customer due diligence will be advisable, once the legislation is revised, to ensure that financial institutions know who they are dealing with. Furthermore,

if an alternative remittance agent is not aware of their obligations under the FTRA96, they should not be dealt with.

Cash Couriers

Intelligence reporting, together with law enforcement indicates that cash smuggling is one of the major methods used by terrorists and money launderers to move money derived from and/or in support of their activities.

Indicators of cash couriering include:

- Use of co-ordinated, multi-jurisdictional couriering syndicates.
- Connections between cash couriers and trade-based money laundering.
- Major regional financial centres as destination points for the movement of cash through couriers.
- Connections between currency smuggling and currency counterfeiting.
- Connections between currency smuggling and casino operators.
- Use of cash couriers to support underground foreign exchange operations.

Locations of Specific Concern

Countries and territories that do not adhere to international standards consistent with the FATF Forty Recommendations to reduce the vulnerability of the financial system can be listed on the Non-Cooperative Countries and Territories (NCCT) list.

In addition, the FATF may from time to time issue statements concerning jurisdictions of concern.

At its February 2008 Plenary, the Financial Action Task Force issued a statement concerning Uzbekistan, Iran, Pakistan, Turkmenistan, Sao Tome and Principe and the Northern Part of Cyprus. Here is a link to the FATF Statement dated October 2008.

For the purpose of conducting due diligence, financial institutions are advised to note the risks arising from the deficiencies identified in the AML/CFT regimes of Uzbekistan and Iran. Financial institutions are also advised to note deficiencies of Pakistan's AML/CFT regime and to pay special attention to risks in transactions with financial institutions operating in the northern part of Cyprus.

The following list provides some examples of instances where further assessment may be required when transactions involve locations of specific concern:

- Foreign currency exchanges, immediately followed by wire transfers.

- Deposits, immediately followed by wire transfers.
- Large numbers of incoming or outgoing wire transfers to or from business accounts where there appears to be no logical purpose.
- Several accounts where funds are collected and forwarded to a small number of foreign beneficiaries, (individuals and businesses).
- Funds sent or received by international transfers.

Politically Exposed Persons

The FATF describes *politically exposed persons* as individuals who are or have previously been assigned prominent public functions in a particular country. If a politically exposed person becomes involved in any criminal activities, the financial discretion given to them often becomes a barrier in detecting or investigating their involvement in crime.

The following list has been taken directly from the FATF Forty Recommendations. In addition to performing normal due diligence processes, it is suggested that financial institutions take the following measures when dealing with politically exposed persons:

- Have appropriate risk management systems to determine whether the customer is a politically exposed person.
- Obtain senior management approval for establishing business relationships with such customers.
- Take reasonable measures to establish the source of wealth and source of funds.
- Conduct enhanced ongoing monitoring of the business relationship.

TERRORIST FINANCING

Financial Transactions Reporting Act 1996

In New Zealand, the FTRA96 imposes certain obligations on financial institutions, including:

- Verification of customer identity, for example, when new accounts are opened, certain transactions conducted or where money laundering or terrorist financing is suspected.
- Retention of transaction records and customer verification details.
- Reporting suspicious transactions.

Terrorism Suppression Act 2002

According to the Terrorism Suppression Act 2002, terrorism is broadly defined as certain types of acts that are:

> "…carried out for the purpose of advancing an ideological, political, or religious cause, and with the following intention: (a) to induce terror in a civilian population; or (b) to unduly compel or to force a government or an international organisation to do or abstain from doing any act"[5].

Terrorist Designations

Under the Terrorism Suppression Act 2002, the Prime Minister of New Zealand may designate an entity as a terrorist entity if there is good reason to suspect that the entity has knowingly carried out or participated in one or more terrorist acts.

Furthermore, after designating an entity as a terrorist entity, the Prime Minister may also designate other associated entities. Similarly, there must be good reason to suspect that the other entity is knowingly facilitating one or more terrorist acts, for example, by financing those acts fully or partially or acting on behalf of the designated terrorist entity.

The United Nations terrorist designation list registers individuals and organisations linked only to al-Qaeda and the Taliban. New Zealand's list is based on information received from the United Nations.

Here is a link to the New Zealand list of terrorist designations.

In contrast, the United States Treasury Office of Foreign Assets Control (OFAC), for example, registers all other entities suspected of having links to terrorism.

Here is a link to the OFAC list of terrorist designations.

Note that there are various other terrorist designation lists operating worldwide.

When to submit a Suspicious Property Report (SPR)

If a financial institution deals with an individual or organisation and there are *reasonable grounds* for suspicion in relation to a transaction and the individual or organisation is matched appropriately on New Zealand's terrorist designation list, a *Suspicious Property Report (SPR)* must be completed, pursuant to Section 43 of the Terrorism Suppression Act 2002 (see Appendix B).

Any SPR made to Police must, (as a minimum), contain all the information specified in the Schedule to the Terrorism Suppression Act 2002, (see Appendix D).

This report may be submitted to the FIU at New Zealand Police National Headquarters.

---

[5] *Terrorism Suppression Act 2002*, Part 1, Section 5(2a) and (2b), Terrorist act defined.

Essentially, if a match is found on New Zealand's terrorist designation list and as such, the financial institution involved submits a *Suspicious Property Report (SPR)*, they will be protected under the Terrorism Suppression Act 2002 from any civil action, particularly in relation to privacy issues.

When to submit a Suspicious Transaction Report (STR)

If a match is found on a list other than New Zealand's terrorist designation list, the financial institution involved must submit a *Suspicious Transaction Report (STR)*, pursuant to the FTRA96. Consequently, the financial institution will be protected under the FTRA96. This report should be forwarded to the FIU.

A financial institution must have reasonable grounds for suspicion in relation to a transaction before any decision is made to search for individuals or organisations on designated terrorist lists.

How to determine a match

Determining whether or not an appropriate match has been identified may be difficult to establish, particularly when searches are based solely on an individual's name. The New Zealand terrorist designation list registers personal identifiers such as:

- name
- title
- designation
- date of birth
- place of birth
- aliases
- nationality
- passport details
- addresses

Remember that all factors in relation to an individual should be taken into consideration before determining whether or not a match exists on a designation list.

Often it will be quite clear that the individual is not a person of interest, for example, if an elderly gentleman results in a name match, yet the date of birth on the terrorist designation lists corresponds with an individual in his early 20s, it is unlikely that this would be an appropriate match. In effect, there are no hard and fast rules apart from initiative and common sense.

The decision as to whether there are *reasonable grounds* for suspecting a match and submitting a report is a judgment for the financial institution or person concerned. If there is any doubt, the advice of a supervisor, manager or the Police should be sought.

This information is also demonstrated in the flowchart at the end of this section.

Dealing with Property

The Terrorist Suppression Act 2002 also covers the prohibition of dealing with the property of terrorists and associated entities. This includes all property derived or generated from terrorism.

An offence is committed when without lawful justification or reasonable excuse, a person deals with any property knowing that it is owned or controlled, directly or indirectly, by an entity designated under this legislation as a terrorist entity or as an associated entity.

An example of dealing with property with a reasonable excuse is when the act does no more than satisfy essential human needs of an individual designated under this legislation.

Funding Terrorism

Like any criminal organisation, terrorist groups need financial backing to achieve their objectives. A successful terrorist group must be able to develop and maintain an effective financial structure. This generally requires money laundering techniques and methods to ensure funding may be used to obtain resources needed to commit acts of terrorism.

The funds obtained by terrorists may take many different forms. In New Zealand, for example, under the Terrorism Suppression Act 2002, funds are defined as:

> "…(b) assets of every kind, whether tangible or intangible, moveable or immoveable, however acquired; and (b) includes legal documents or instruments (for example, bank credits, travellers' cheques, bank cheques, money orders, shares, securities, bonds, drafts, and letters of credit) in any form (for example, in electronic or digital form) evidencing title to, or an interest in, assets of any kind"[6].

This legislation also outlines four main issues concerning terrorist financing that are particularly relevant to financial institutions operating in New Zealand. These points are summarised below:

- It is a criminal offence for a person to directly or indirectly provide or collect funds intending that they be used, or knowing that they are to be used, fully or partially, to carry out any acts of terrorism.

- It should be noted that this does not include funds provided or collected for the purpose of advocating democratic government or the protection of human rights, for example, *Amnesty International*.

- In the event of prosecution, it is not necessary for the prosecutor to prove that the funds provided or collected were actually used, fully or partially, to carry out an act of terrorism.

[6] *Terrorism Suppression Act 2002*, Part 1, Section 4, Interpretation.

- Terrorist financing carries a penalty of imprisonment for a term not exceeding 14 years.

Detecting Terrorist Financing

In October 2001, the FATF agreed to provide special guidance for financial institutions to assist in the detection of techniques used for terrorist financing.

The subsequent document entitled *Guidance for Financial Institutions in Detecting Terrorist Financing* is intended as best practice guidelines and endeavours to ensure that terrorist funds are not inadvertently hidden or shifted. The expected result is that financial institutions will be better equipped to protect themselves from being used as a channel for this type of activity.

The information contained in the guidance notes complements and reinforces already existing requirements and obligations under the FTRA96. While many of the described indicators or characteristics apply specifically to potential terrorist financing most will apply to identifying suspicious transactions in general as discussed in the Suspicious Transaction Guidelines section.

In this way, it should be noted that the best practice guidelines do not replace or supersede any obligations under current legislation. Furthermore, implementation of any proposed measures should not be interpreted as necessarily protecting financial institutions from any legal action. In addition, it should not be interpreted as discouraging or prohibiting financial institutions from dealing with legitimate customers.

These guidance notes have, therefore, been developed solely to assist financial institutions in determining whether certain transactions merit further scrutiny to enable them to identify, report where appropriate, and ultimately avoid transactions involving funds that support or are associated with terrorist financing. Again, the information provided here is intended as best practice guidelines only.

Sources of Terrorist Funding

The following examples provide a brief overview of some possible sources of terrorist financing:

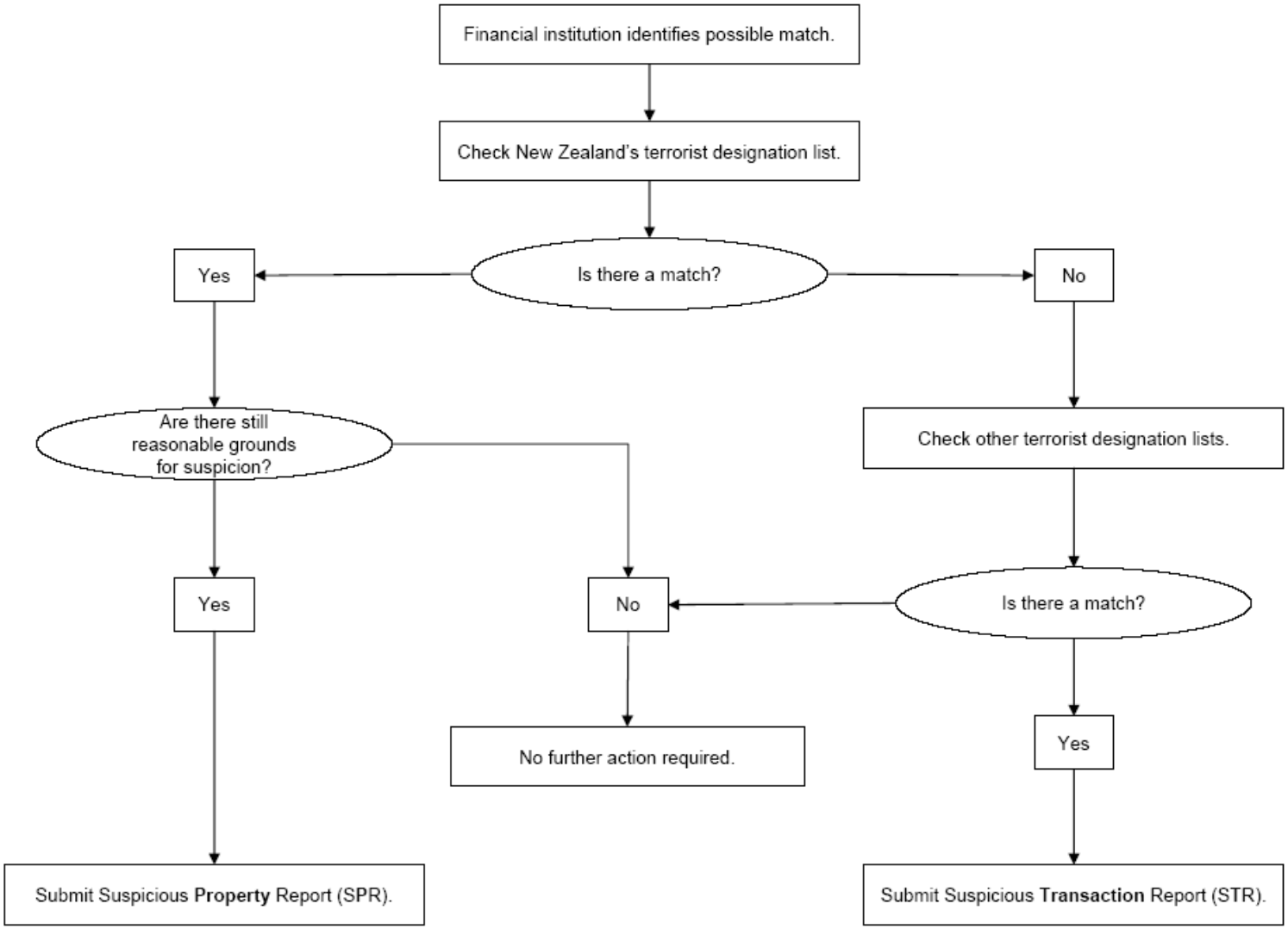
> ***Community fundraising*** *is often carried out in the name of organisations that are recognised as charitable or relief groups, specific fundraising methods may include door-to-door solicitation, publication sales, social events and appeals to wealthy community members. It is believed, for example, that Osama bin Laden contributed a significant amount of his personal fortune in support of the al-Qaeda terrorist network.*
>
> ***Revenue-generating crime*** *is described as income derived from unlawful activities. A terrorist group may financially support itself, for example, by kidnapping and receiving ransoms for hostages or extorting funds under the guise of protection money.*

> ***State-sponsored terrorism*** *is terrorism exercised by a government against its own citizens or in support of international terrorism.*

Experts generally agree that the money laundering methods used by terrorist organisations do not differ significantly from other criminal groups. There is some evidence, however, to suggest that certain techniques are exploited more often by terrorists, for example, the use of cash couriers and the purchase of monetary instruments such as bank cheques or money orders.

The information outlined in the Suspicious Transaction Guidelines section provides examples of suspicious transactions, which may be helpful when determining when further scrutiny may be required. This information applies to all criminal groups, including terrorist organisations.

SUGGESTED PROCESS FOR SUSPECTED MATCHES ON TERRORIST LISTS



APPENDIX A
SUSPICIOUS TRANSACTION REPORT (STR) FORM

SUSPICIOUS TRANSACTION REPORT
(Financial Transactions Reporting Act 1996)

PLEASE WRITE CLEARLY IN CAPITAL LETTERS

IDENTITY OF CUSTOMERS INVOLVED IN THE SUSPICIOUS TRANSACTION

CUSTOMER CONDUCTING TRANSACTION (IF KNOWN)

1 **Family name** ..... **Mr / Mrs / Ms / Miss** (please circle)

2 **First name(s)** .....

3 **Date of birth** .....

4 **Address (home)** .....

5 **Address (work)** .....

6 **Occupation/business** .....

IDENTIFICATION DETAILS (please attach copy of photograph if available)

Type of identification (e.g., drivers licence, passport etc.)	**Number**	**Issuer**
1	.....	.....
2	.....	.....
3	.....	.....

CUSTOMER ON WHOSE BEHALF TRANSACTION CONDUCTED (IF KNOWN)

1 **Family name** ..... **Mr / Mrs / Ms / Miss** (please circle)

2 **First name(s)** .....

3 **Date of birth** .....

4 **Address (home)** .....

5 **Address (work)** .....

6 **Occupation/business** .....

IDENTIFICATION DETAILS (please attach copy of photograph if available)

Type of identification (e.g., drivers licence, passport etc.)	**Number**	**Issuer**
1	.....	.....
2	.....	.....
3	.....	.....

DESCRIPTION (please attach copy of photograph if available)

Gender ..... **Ethnicity** ..... **Eye colour** ..... **Hair colour** .....

Hair style ..... **Height (cm)** ..... **Build** ..... **Age** .....

Clothing .....

Distinguishing features (e.g., tattoos, facial hair, accent etc.) .....

.....

TRANSACTION DETAILS

Transaction date ..... Transaction amount $ ..... Cash (Y / N) Currency .....

Nature of transaction (e.g., deposit, withdrawal, purchase, sale, foreign exchange, telegraphic transfer, EFTPOS etc.)

1 .....

2 .....

3 .....

Denominations (if applicable) .....

PLEASE RECORD DETAILS ON A SEPARATE SHEET FOR ANY FURTHER TRANSACTIONS

DETAILS OF FACILITIES HELD WITH FINANCIAL INSTITUTION

Account name .....

Date of birth .....

Account number .....

Type of account .....

Bank/branch .....

Signatories

1 .....

2 .....

Account holder .....

Date of birth .....

Occupation .....

Address .....

.....

Signatories addresses

1 .....

2 .....

GROUNDS FOR SUSPICION

Please give details regarding the nature of and circumstances surrounding the transaction and the reason for suspicion

.....

.....

.....

.....

.....

.....

.....

If insufficient space, please attached supplementary sheet and advise number of pages: ☐

FINANCIAL INSTITUTION DETAILS AND PLACE OF TRANSACTION

Institution type (e.g., bank, lawyer) .....

.....

Institution name .....

Branch name (include bank/branch number) .....

.....

Address .....

Tel ..... Fax .....

CONFIDENTIAL

Your identity will not be disclosed except for law enforcement purposes or by order of a Court, as indicated by Section 21 of the Financial Transactions Reporting Act 1996.

Details of staff member conducting transaction

Full name .....

Position .....

Signature .....

Date .....

Details of staff member making report

Full name .....

Position .....

Signature .....

Date .....

Tel ..... Fax .....

Please forward to: The Commissioner of Police, C/- Financial Intelligence Unit, New Zealand Police National Headquarters, P O Box 3017, Wellington

APPENDIX B
SUSPICIOUS PROPERTY REPORT (SPR) FORM

SUSPICIOUS PROPERTY REPORT

(Terrorism Suppression Act 2002)

PLEASE WRITE CLEARLY IN CAPITAL LETTERS

DETAILS OF DESIGNATED ENTITY

DESIGNATED INDIVIDUAL AS PER OFFICIAL LIST OF DESIGNATED ENTITIES

1 **Surname** ..... **Mr / Mrs / Ms / Miss** (please circle)

2 **First name(s)** .....

3 **Date of birth** .....

4 **Last known address** .....

DESIGNATED ORGANISATION AS PER OFFICIAL LIST OF DESIGNATED ENTITIES

1 **Organisation name** .....

2 **Last known address** .....

IDENTITY OF PEOPLE INVOLVED IN THE SUSPICIOUS TRANSACTION

To be completed by financial institutions in cases where the property in question is the subject of a transaction, or proposed transaction, involving a facility with the financial institution. In cases where a financial transaction is not involved, the section below headed SUSPICIOUS PROPERTY DETAILS should be completed.

PERSON CONDUCTING TRANSACTION

1 **Surname** ..... **Mr / Mrs / Ms / Miss** (please circle)

2 **First name(s)** .....

3 **Date of birth** .....

4 **Address (home)** .....

5 **Address (work)** .....

6 **Occupation/business** .....

IDENTIFICATION DETAILS (please attach copy of photograph if available)

Type of identification (e.g., drivers licence, passport etc.)	**Number**	**Issuer**
1	.....	.....
2	.....	.....

PERSON ON WHOSE BEHALF TRANSACTION CONDUCTED

1 **Surname** ..... **Mr / Mrs / Ms / Miss** (please circle)

2 **First name(s)** .....

3 **Date of birth** .....

4 **Address (home)** .....

5 **Address (work)** .....

6 **Occupation/business** .....

IDENTIFICATION DETAILS (please attach copy of photograph if available)

Type of identification (e.g., drivers licence, passport etc.)	**Number**	**Issuer**
1	.....	.....
2	.....	.....

DESCRIPTION (please attach copy of photograph if available)

Gender ..... **Ethnicity** ..... **Eye colour** ..... **Hair colour** .....

Hair style ..... **Height (cm)** ..... **Build** ..... **Age** .....

Clothing .....

Distinguishing features (e.g., tattoos, facial hair, accent etc.) .....

TRANSACTION DETAILS

Transaction date ..... Transaction amount $ ..... Cash (Y / N) Currency .....

Nature of transaction (e.g., deposit, withdrawal, purchase, sale, foreign exchange, telegraphic transfer, EFTPOS etc.)

.....

Denominations (if applicable) .....

PLEASE RECORD DETAILS ON A SEPARATE SHEET FOR ANY FURTHER TRANSACTIONS

DETAILS OF FACILITIES INVOLVED

To be completed in all cases where the property in question is the subject of a transaction, or proposed transaction, involving a facility with the financial institution, or if no transaction is involved, where the property is held in a facility.

Account name	**Account holder** .....
Account number	.....
Type of account	**Address** .....
Bank/branch	.....
Signatories	**Signatories addresses**
1	1 .....
2	2 .....

SUSPICIOUS PROPERTY DETAILS

To be completed in all cases not involving a financial transaction. In the case of reports involving a transaction, the section above headed IDENTITY OF PEOPLE INVOLVED IN THE SUSPICIOUS TRANSACTION should be completed by the financial institution concerned. Where the property in question is held in a facility, details of the facility must be provided in section above headed DETAILS OF FACILITIES INVOLVED.

1 **Property value** .....

2 **Property details** .....

OWNER OR CONTROLLER OF PROPERTY (IF NOT DESIGNATED ENTITY OR HOLDER OF FACILITY)

1 **Surname** ..... **Mr / Mrs / Ms / Miss** (please circle)

2 **First name(s)** .....

3 **Date of birth** .....

4 **Address (home)** .....

5 **Occupation/business** .....

GROUNDS FOR SUSPICION

Please give details regarding the nature and circumstances surrounding the transaction, or the possession/control of the property, as well as the reason for suspicion, for example, name match with designated entity. Please also note the date on which the suspicion was formed, as well as the supply date on the existence of the facility or other property being reported, initially brought to attention (to the best of knowledge).

.....

.....

.....

.....

.....

.....

.....

If insufficient space, please attached supplementary sheet and advise number of pages: ☐

Date suspicion formed .....

Supply date .....

FINANCIAL INSTITUTION DETAILS AND PLACE OF TRANSACTION

Institution type (e.g., bank, lawyer) .....

Institution name .....

Branch name (include bank/branch number) .....

Address .....

Telephone ..... Facsimile .....

CONFIDENTIAL

Your identity will not be disclosed except for law enforcement purposes or by order of a Court, as indicated by the Terrorism Suppression Act 2002.

Details of staff member conducting transaction

Full name .....

Position .....

Signature .....

Date .....

Details of staff member making report

Full name .....

Position .....

Signature .....

Date .....

Tel ..... Fax .....

PLEASE FORWARD TO

The Commissioner of Police
C/- Financial Intelligence Unit
New Zealand Police National Headquarters
P O Box 3017, Wellington
Tel 04 474 9499, Fax 04 498 7405

APPENDIX C
FINANCIAL TRANSACTIONS REPORTING ACT 1996 SCHEDULE

44 *Financial Transactions Reporting*
1996, No. 9

Section 15 (2) (b) SCHEDULE

DETAILS TO BE INCLUDED IN SUSPICIOUS TRANSACTION REPORTS

1. The name, address, date of birth, and occupation (or, where appropriate, business or principal activity) of each person conducting the transaction (if known to the person making the report).
2. The name, address, date of birth, and occupation (or, where appropriate, business or principal activity) of any person on whose behalf the transaction is conducted (if known to the person making the report).
3. Where a facility with a financial institution is involved in the transaction, —
   (a) The type and identifying number of the facility:
   (b) The name, address, date of birth, and occupation of the person in whose name the facility is operated:
   (c) The names of the signatories to the facility.
4. The nature of the transaction.
5. The amount involved in the transaction.
6. The type of currency involved in the transaction.
7. The date of the transaction.
8. If available, details of any documentary or other evidence held by the financial institution that is involved in the transaction and that may assist in establishing the identity of the person who conducted the transaction or the identity of any person on whose behalf the transaction was conducted.
9. If available, details of any documentary or other evidence held by the financial institution through which the transaction was conducted and that may assist in establishing the identity of the person who conducted the transaction or the identity of any person on whose behalf the transaction was conducted.
10. The name, position, phone number, and fax number of the person who prepared the report.
11. If applicable, the branch name, address, and telephone number of the financial institution which provided the facility involved in the transaction or the financial institution through which the transaction was conducted, as the case may be.

———————————

This Act is administered in the Ministry of Justice.

Wellington, New Zealand: Published under the authority of the
New Zealand Government — 1996
69701 — 96/N5

APPENDIX D
TERRORISM SUPPRESSION ACT 2002 SCHEDULE

Schedule 5 **Terrorism Suppression Act 2002**
2002 No 34

s 44(1)(a) **Schedule 5**

Details to be included in suspicious property reports

1. The name, and (if available) the last known address, of the designated entity concerned.

2. For property that came into the possession or immediate control of a financial institution through a transaction conducted or proposed to be conducted through the financial institution and involving a facility with the financial institution:

(a) the grounds on which the financial institution holds the suspicion referred to in section 43(2) and the date on which that suspicion was formed:

(b) (to the best of the knowledge of the financial institution) the date on which the financial institution became aware of the existence of the property, and (if readily available to the financial institution) the type of, and all other available identifying information about, the property:

(c) (if readily available electronically to the financial institution)—

(i) the nature of the transaction; and
(ii) the date of the transaction:

(d) the type and identifying number of the facility:

(e) the value of the property in the facility (if known to the person preparing the report for the financial institution):

(f) the name, address, date of birth (if applicable), and (if known to the person preparing the report for the financial institution) occupation (or, if appropriate, business or principal activity) of the person in whose name the facility is operated, and (if available to the person preparing the report for the financial institution) details of any documentary or other evidence held by the financial institution and used to establish the identity of that person:

(g) the names of the signatories to the facility and (if available to the person preparing the report for the financial institution) details of any documentary or other evidence held by the financial institution and used to establish the identity of the signatories to the facility:

(h) (if readily available electronically to the financial institution) the name, address, date of birth (if applicable), and occupation (or, if appropriate,

business or principal activity) of each person conducting the transaction and of any person on whose behalf the transaction is conducted:

(i) (if applicable) the branch name, address, and telephone number of the financial institution which provided the facility involved in the transaction or the financial institution through which the transaction was conducted, as the case may be.

3. For other property in the possession or immediate control of a financial institution or any other person—

(a) the grounds on which the financial institution or other person holds the suspicion referred to in section 43(2) and the date on which that suspicion was formed:

(b) (to the best of the knowledge of the financial institution or other person) the date on which the financial institution or other person became aware of the existence of the property, and (if readily available to the financial institution or other person) the type of, and all other available identifying information about, the property:

(c) the value of the property (if known to the financial institution or other person):

(d) (if available to the financial institution or other person) the name, address, date of birth (if applicable), and occupation (or, if appropriate, business or principal activity) of the person who owns the property (if it is not owned by the entity), and details of any documentary or other evidence held by the financial institution or other person and used to establish the identity of the person who owns the property:

(e) (if available to the financial institution or other person) the name, address, date of birth (if applicable), and occupation (or, if appropriate, business or principal activity) of the person who controls the property (if it is not controlled by the entity), and details of any documentary or other evidence held by the financial institution or other person and used to establish the identity of the person who controls the property.

4. If the report is made in relation to property controlled or possessed by a financial institution, the name, position, and phone and fax number of the person authorised by the financial institution to prepare and submit the report. In all other cases, the name, position (if relevant), and phone and fax numbers of the person who prepared the report.

_____

Legislative history

17/04/2001 Introduction (Bill 121-1)

03/05/2001	First reading and referral to Foreign Affairs, Defence and Trade Committee
22/03/2002	Reported from Foreign Affairs, Defence and Trade Committee (Bill 121-2)
08/10/2002	Second reading, committee of the whole House, third reading
17/10/2002	Royal assent

This Act is administered in the Ministry of Foreign Affairs and Trade and the Ministry of Justice.

Wellington, New Zealand: Published under the authority of the
New Zealand Government—2002

INDEX