

AML / CFT

Anti-money laundering and countering financing of terrorism

Internal Affairs AML / CFT Sector Risk Assessment

March 2011

INTERNAL AFFAIRS



Te Tari Taiwhenua

Table of contents

<u>Part 1: Executive summary</u>	5
<u>The scope of the SRA</u>	5
<u>Limitations</u>	5
<u>Overview of current findings</u>	5
<u>Abbreviated risk table</u>	6
<u>Part 2: Introduction</u>	7
<u>The Anti-Money Laundering and Countering Financing of Terrorism Act 2009</u>	7
<u>Purpose of the SRA</u>	7
<u>AML/CFT Supervisors</u>	7
<u>Structure</u>	8
<u>Other ML/TF assessments</u>	9
<u>Information sources</u>	10
<u>Methodology</u>	12
<u>Limitations</u>	13
<u>Money laundering and terrorist financing</u>	13
<u>Other relevant legislation</u>	14
<u>Part 3: Sector summary</u>	15
<u>Abbreviated risk table</u>	15
<u>Summary by sector</u>	15
<u>Part 4: Sector risks</u>	21
<u>Money remittance or transfer services (MR)</u>	21
<u>Trust and company service providers (TCSPs)</u>	25
<u>Casinos</u>	30
<u>Currency exchangers (CE)</u>	38
<u>Cash storage - safe deposit boxes</u>	42
<u>Cash transport</u>	45

<u>Non-bank non-deposit-taking lenders (NBNDTL)</u>	49
<u>Financial leasing</u>	52
<u>Non-bank credit cards</u>	55
<u>Factoring</u>	59
<u>Debt collection</u>	62
<u>Payroll remittance</u>	65
<u>Appendix A</u>	68
<u>Appendix B</u>	69
<u>Appendix C</u>	70



Contact details

Kate Reid
Manager
AML/CFT Unit, Department of Internal Affairs
kate.reid@dia.govt.nz
DDI: +64 4 4940674

Laura Blade
AML/CFT Lead Analyst
Intelligence Unit, Department of Internal Affairs
laura.blade@dia.govt.nz
DDI: +64 4 4940601

Part 1: Executive summary

This section provides a brief outline of the SRA and a summary of the risk ratings for the sub-sectors.

The scope of the SRA

1. This sector risk assessment (SRA) is a preliminary assessment by the AML/CFT supervisors to assess the risks of money laundering across the sector they will supervise. The Department of Internal Affairs will supervise casinos, money service businesses, payroll remittance, lending, financial leasing, safe deposit/cash storage and non-bank credit card providers for the purposes of the Anti-Money Laundering and Countering the Financing of Terrorism Act 2009 (the Act). Other AML/CFT supervisors (the Reserve Bank and the Securities Commission) have published similar risk assessments for the sectors they supervise.
2. This SRA will assist the AML/CFT supervisors in understanding the risks of money laundering in the sector. It will also benefit reporting entities as it will assist them to prepare for undertaking risk assessments in their businesses. Reporting entities are required by the Act to undertake a risk assessment prior to establishing an AML/CFT programme. This document provides guidance to reporting entities on areas of higher risk in their business.

Limitations

3. The assessments of each industry or sub-sector undertaken in this document are based on structural risk factors. For consistency when comparing sub-sectors we have not taken into account the adequacy or effectiveness of any controls at this stage as the supervisory arrangements provided for in the Act are yet to take effect.
4. There is limited information available on money laundering or terrorist financing risks in New Zealand. A national risk assessment undertaken by the New Zealand Police Financial Intelligence Unit (FIU) has only recently been published. This SRA draws significantly on risk assessments, guidance and reports from other jurisdictions and international organisations such as the Financial Action Taskforce (FATF).

Overview of current findings

5. The following assessments are a result of considering the internationally recognised structural risk factors of money laundering in the sub-sectors below. Those structural risk indicators include size and scale of the sector, cash intensity of business, amount of international business, customer base and indicators of potential money laundering activities.
6. The risk assessment model rates structural indicators as high, medium or low based on available data. Indicators of higher risk are cash intensive products and services along with certain types of customers.
7. The ratings in this SRA do not take into account risk mitigants that are in place in individual entities or across the sub-sectors. Only a relatively narrow set of AML/CFT requirements is currently in force across the sector. For most reporting entities the AML/CFT supervisors cannot test the effectiveness of existing controls. AML/CFT supervisors' powers are limited until the Act comes into force, probably in early 2013. For this reason controls have been noted where they exist, but not included in the risk rating process, in order to present consistent ratings that can be

compared across sectors.

8. There is little information or evidence to support a rating on terrorist financing in New Zealand at present.

Abbreviated risk table

Sector	Overall ML/FT risk
Money remittance	HIGH
Trust and Company Service Providers (TCSPs)	HIGH
Casinos	MEDIUM/HIGH
Currency exchange	MEDIUM
Safe Deposit Boxes	LOW/MEDIUM
Cash transport	LOW/MEDIUM
Non-bank non-deposit taking lenders (NBNDTLs)	LOW
Financial leasing	LOW
Non bank credit cards	LOW
Factoring	LOW
Debt collection	LOW
Payroll remittance	LOW

Part 2: Introduction

The Anti-Money Laundering and Countering Financing of Terrorism Act 2009

9. The Anti-Money Laundering and Countering the Financing of Terrorism Act 2009 (the Act) was passed in October 2009. The purposes of the Act are:
- To detect and deter money laundering and the financing of terrorism (ML/TF); and
 - To maintain and enhance New Zealand's international reputation by adopting, where appropriate in the New Zealand context, recommendations issued by the Financial Action Task Force (FATF); and
 - To contribute to public confidence in the financial system.
10. Under Section 131 of the Act, one of the functions of each AML/CFT (anti-money laundering and countering financing of terrorism) supervisor is to assess the level of risk of ML/TF across all of the reporting entities that it supervises. This has been undertaken in the form of the Sector Risk Assessment (SRA). Three SRAs have been produced – one for each of the three AML/CFT supervisors' sectors (see 'AML/CFT supervisors' below).

Purpose of the SRA

11. This SRA is the first assessment undertaken by the AML/CFT supervisor of the money laundering risks in the sector.
12. The SRA is intended to:
- Assist the supervisors in their understanding of particular ML/TF risks within their designated sector; and
 - Provide guidance to reporting entities on the specific risks relevant to their sector or sub-sector; and
 - Contribute to the New Zealand Police Financial Intelligence Unit (FIU) assessment of ML/TF risks in New Zealand financial institutions.

AML/CFT Supervisors

13. The relevant supervisors for the types of reporting entities are detailed in Section 130 of the Act. That section allows for AML/CFT supervisors to agree on the appropriate supervisor for a reporting entity where the products or services offered by that reporting entity may be covered by more than one AML/CFT supervisor. There is also provision for supervision of a group of reporting entities as a Designated Business Group by one or more than one AML/CFT supervisor.
14. A reporting entity can only have one supervisor. The national AML/CFT co-ordination committee can appoint an AML/CFT supervisor for a reporting entity in the absence of any agreement by the supervisors. The Act designates three AML/CFT supervisors and gives them and the FIU powers to carry out their AML/CFT functions.
15. The Reserve Bank is the relevant AML/CFT supervisor for:
- Registered banks
 - Non-bank deposit takers (NBDTs)
 - Life insurers.
16. The Securities Commission is the AML/CFT supervisor for:
- Issuers of securities
 - Trustee companies
 - Futures dealers

- Collective investment schemes
 - Brokers
 - Financial advisers.
17. The Department of Internal Affairs (the Department) is the AML/CFT supervisor for all reporting entities not covered by the Reserve Bank and Securities Commission. At present this includes:
- Casinos
 - Money service businesses (including currency exchange and money remittance/transfer)
 - Payroll remittance
 - Lending and other services (including non-bank non-deposit-taking lenders, debt collection and factoring)
 - Financial leasing
 - Cash transporters
 - Safe deposit/cash storage
 - Issuing and managing means of payment (including non-bank credit card providers).
18. Trust and Company Service Providers (TCSPs) (including Company Formation Agents (CFAs) and company services) are not currently included in the AML/CFT regime. However as noted in the Ministry of Justice AML/CFT Regulations and Codes of Practice Discussion document, recent media reports and international findings have highlighted the risk of TCSPs and proposals have been made to include them as reporting entities moving forward. Therefore, TCSPs have been included as part of the SRA.
19. For the purpose of this risk assessment, stored value card providers have not been considered independently. Stored value cards that are not subject to one of the proposed exemptions¹ are offered by registered banks and therefore come under the Reserve Bank's supervision.

Structure

20. There are 4 parts to this document.

Part 1: Executive Summary – provides a brief outline of the risk ratings for the sub-sectors.

Part 2: Introduction – introduces the relevant legislation and gives an overview of the risk assessment process, the methodology used in the assessment of the ML/TF risks in the sector and limitations with the current SRA.

Part 3: Sector summary – provides a summary of each sub-sector and the key risk areas.

Part 4: Sector risks – addresses each sub-sector in depth by highlighting the factors considered in the risk assessment of each sub-sector. In turn this is arranged into different sections:

- Overview - this provides some general comments on the sub-sector as a whole

¹ AML/CFT Codes of Practice and Regulations Discussion Document, August 2010

- Structural risks - drawing on international guidance, this section considers the areas of risk that relate to the nature and scale of the sub-sector and its operations
- Specific risks – again drawing on international guidance, this section details the major areas of risk of ML/TF in a sub-sector relevant to the business activities undertaken by reporting entities in that sub-sector.

Other ML/TF assessments

Mutual evaluation report of New Zealand

21. The FATF and the Asia-Pacific Group on Money Laundering (APG) completed a Mutual Evaluation Report on New Zealand in October 2009 which described some deficiencies with AML/CFT requirements in New Zealand at that time. These included gaps in law and regulation, limited Customer Due Diligence (CDD), insufficient beneficial ownership information availability and vulnerabilities with the New Zealand Companies registration process.
22. The Act, along with Regulations and Codes of Practice yet to be introduced, aim to address vulnerabilities identified by the FATF.
23. Sector specific vulnerabilities identified in FATF publications have been considered under the risks for each sector.

The risk-based regime – three levels of risk assessment

24. The regime introduced under the AML/CFT Act enables AML/CFT activities to be based on risk. The purpose of this is to minimise compliance costs and ensure that resources are targeted towards high-risk, high-priority areas.
25. The Act provides for risk assessment at three levels:

National Risk Assessment

26. The FIU has undertaken a National Risk Assessment (NRA) pursuant to section 142(k) of the Act. The NRA's primary audience is relevant government agencies including the AML/CFT supervisors. It gives an overview of AML/CFT issues affecting New Zealand from a law enforcement perspective. Information from government organisations, both domestic and international, contributed to this assessment. Further information will be available from the AML/CFT supervisors and reporting entities for future national risk assessments.
27. The NRA acknowledges the information gaps in the data available to assess ML/TF. The FIU intends to develop and maintain valid and reliable indicators of ML/TF and publish Quarterly Typology Reports. The reports, along with other available intelligence, will inform the AML/CFT supervisors and sectors of trends. Future SRAs will benefit from this information.

Sector Risk Assessment

28. SRAs have been produced by the respective sector AML/CFT supervisors. Future SRAs will draw on a variety of sources, including risk assessments carried out by the FIU and reporting entities. Ongoing SRA work will be conducted by the AML/

CFT supervisors in order to fully understand the ML/TF risks within their sectors and to inform reporting entities on risk indicators, trends and emerging issues. SRAs may be revised regularly or on an ad-hoc basis, depending on the rate of change in ML/TF risk affecting a sector.

Reporting Entity Risk Assessments

29. Section 58 of the Act requires all reporting entities to undertake an assessment of the risk of ML/TF in their business. The risk assessment must consider the nature, size and complexity of its business, products and services including delivery methods, its customers and any countries it has dealings with as a part of its business. One of the factors that reporting entities must have regard to in developing their risk assessments is guidance material on risk assessment produced by an AML/CFT Supervisor or the Commissioner of Police. This SRA forms part of the guidance material issued by an AML/CFT Supervisor. AML/CFT supervisors are preparing further guidance on the process of carrying out a reporting entity risk assessment.



30. The following diagram outlines the inter-relationship of the risk assessment processes:

Information sources

31. The SRA has drawn together information from a number of sources. Currently there is little comprehensive or precise data available to fully assess the ML/TF risks across all products, services or areas in each sector. As a result, the SRAs drew heavily on overseas based experience and findings from similar jurisdictions with AML/CFT requirements, such as the Australian Transaction Reports and Analysis Centre (AUSTRAC). This is combined with observations from multi-national organisations that New Zealand is a member of including the FATF and APG, as well as the Wolfsberg Group, Interpol, and the International Monetary Fund where applicable.
32. This information is supplemented by local information, particularly data received from entities that responded to various surveys and/or interviews by AML/CFT supervisors. Consideration has been given to other data sources available to the AML/CFT supervisors including summary Suspicious Transaction Report (STR) data and information provided by the FIU, as well as industry expertise, knowledge and experience from internal and external resources relevant to the sector.

33. The Department consulted with approximately 31% of all reporting entities. This was done via either:
- Interviews with a sample of reporting entities in each sector,
 - Questionnaires sent to the remainder of the reporting entities in each sector

Table 1 outlines the response rates for each sector:

Sector	Total number of identified reporting entities	Number of respondents	Response rate
Money remittance	46	5 ²	13%
TCSPs	49	9	18%
Casinos	6	5	83%
Currency exchange	34	7 ³	21%
Safe Deposit Boxes	5	4	80%
Cash transport	7	4	57%
NBNDTLs	190	17	9%
Financial leasing	26	9	35%
Non bank credit cards	9	5	55%
Debt collection	65	20	31%
Factoring	27	3	11%
Payroll remittance	15	6	40%

² It should be noted that one of the respondents accounts for approximately 85% of all 840 agents identified

³ It should be noted that one of the respondents accounts for approximately 90% of all 1215 agents identified

Methodology

34. The AML/CFT supervisors have drawn upon international guidance in preparation of the SRAs. This assessment follows an international model for AML/CFT risk assessments developed by the World Bank and the APG.
35. The model assesses a series of factors to indicate the nature and scale of possible ML/TF in New Zealand. These include:
 - Size of the sub-sector or industry, including value of transactions;
 - Turnover volume;
 - High cash intensive products and services;
 - Frequency of international transactions;
 - Higher risk customer types; and
 - Indicators of potential ML activities – including the number of Suspicious Transaction Reports currently recorded from each sub-sector under the Financial Transaction Reporting Act 1996 requirements, any prosecutions or convictions that indicate ML.
36. Each risk indicator is assessed as LOW, MEDIUM or HIGH based on current information and understanding of the ML/TF risk in the sector.
37. Following the assessment of the structural risks, the assessment model then considers a basic overview of any high level AML/CFT regulatory requirements and the current supervision environment. Potential high level considerations include:
 - AML/CFT Regulations/Guidelines/enforcement mechanisms;
 - AML/CFT on-site inspections and off-site monitoring;
 - Resources committed to AML/CFT supervisory authorities;
 - Market entry/control (including fit and proper requirements); and
 - Monitoring of transactions and adequacy of STR reporting.
38. Because the Act is not fully in force, the policies, procedures and controls that may manage or mitigate the risks in the sectors' reporting entities have not been assessed. Because we are not considering the effectiveness of reporting entities' controls in the risk rating process, we have made no judgements whether the risks in the sector are adequately managed or mitigated. Individual entities may have systems and controls in their business that adequately address some or all of the risks discussed in the risk assessment. This SRA assesses the risk across the sector and not at the individual reporting entity level. Entities that have already developed expertise and knowledge in ML/TF will find that knowledge beneficial when interpreting the ML/TF risks to their business.
39. Specific areas of risk within the sector are also identified and assessed in the SRA. Products and services offered by businesses in a sector that are susceptible to ML/TF are evaluated as well as determining whether any delivery channels or customer types were likely to be more at risk of money laundering. This SRA does not necessarily identify or comment on all financial activities undertaken by entities within the sector.
40. Given the limitations of available information and the early stage of the implementation of the AML/CFT requirements of the Act, it is likely that this first SRA will differ in scope from subsequent assessments. It is intended that this assessment will be the foundation of more detailed and informative assessments in years to come. The AML/CFT supervisors anticipate that SRAs will be revised as further information and data becomes available from reporting entities, the FIU and overseas.

41. It is anticipated that reporting entities may determine how ML/TF risks will be assessed in their business using a different approach to the SRA methodology.

Limitations

42. This SRA has been produced prior to full implementation of the Act with inevitable limitations on the risk assessment process. The following limitations to the SRA process were identified:
- information on money laundering in New Zealand is limited, with some reliance on international typologies and guidance to identify risks;
 - reporting entities have various degrees of understanding of AML/CFT legislation, procedures or the ML/TF risks in their business, therefore the perception of risks may not be fully developed in some responses to surveys;
 - insufficient availability of detailed data and information to inform some risk areas;
 - variable quality of data across some of the sectors with more qualitative sources used;
 - the limited scope of current legislative requirements; and
 - STR data reporting currently only allows for quantitative analysis.
 - incomplete database of all reporting entities supervised by the Department (although it is believed that the large majority of reporting entities have been identified),
 - limited corporate knowledge of some sectors within the Department
 - resource and time constraints also restricted the Department's ability to engage with more reporting entities in the sector; and
 - some reporting entities were unwilling to provide information to the Department to inform the SRA.
43. The majority of these limitations will be addressed with the development of the AML/CFT regime and increased engagement with reporting entities. The SRA will evolve as the quality of the information improves. AML/CFT supervisors expect that when the statutory obligations come into force and reporting entities are supervised for compliance with these obligations, more and better information on the AML/CFT risks facing the sectors will emerge. Subsequent risk assessments should contain a better balance of quantitative and qualitative information.

Money Laundering and Terrorist Financing

44. This assessment focuses on the risk of money laundering in the sector as there is limited information on terrorist financing in New Zealand for the AML/CFT supervisors to comment on.
45. Money laundering is concerned with concealing the origins of funds or assets. Funds are generated through illegal operations, such as drug manufacture and supply, and launderers attempt to hide its origin through a number of often complex transactions. There are generally 3 stages to money laundering:
- Placement – involving the introduction of illicit funds into the financial system
 - Layering – the numerous transactions designed to confuse any tracing of funds to its original source
 - Integration – legitimising the funds through ordinary financial activity.
46. With money laundering, the criminal activity has already taken place. With terrorist financing, the focus is on preventing the criminal activity from occurring. The characteristics of terrorist financing can make it difficult to identify. These include the low value of transactions and that funding can come from legitimate as well as

illicit sources. Where illicit funds are being used, the methods employed to monitor money laundering may also be applicable for terrorist financing as the movement of those funds often relies on similar methods to money laundering.

47. There have been no convictions for terrorist related offences in New Zealand since the introduction of the Terrorism Suppression Act in 2002. The FIU and the 2009 Mutual Evaluation Report indicate that there is little evidence to suggest terrorist financing is occurring in New Zealand and consider the risk of terrorist financing to be low. The FIU is better placed to provide information on terrorist financing indicators and activities at present.

Other Relevant Legislation

Financial Transactions Reporting Act 1996 (FTRA)

48. The FTRA contains the AML/CFT requirements that will be in place for financial institutions and casinos until the Act fully commences. The FTRA currently applies to most entities that are the subject of this risk assessment.
49. The purpose of the FTRA is to facilitate the prevention, detection, and investigation of money laundering in New Zealand. This is assisted by requiring financial institutions to meet certain obligations in relation to financial transactions. This includes the verification of identity, STRs and record keeping.

The Financial Service Providers (Registration and Dispute Resolution) Act 2008

50. The objectives of the Financial Service Providers (Registration and Dispute Resolution) Act 2008 are to identify financial service providers, to allow for more effective monitoring and evaluation of financial service providers, to assist supervision of reporting entities with AML/CFT obligations and to improve consumer redress in the financial sector.
51. Financial service providers were required to be registered by December 2010.

The Private Security Personnel and Private Investigators (PSPPI) Act 2010

52. The purpose of the PSPPI Act is to minimise the risks within the security sector and ensure the competency of those operating in the sector. The PSPPI Act introduces a new licensing regime to replace the current Private Investigators and Security Guards Act 1974 Registrar.
53. Cash transport companies will be required to be compliant with the PSPPI Act from 1 April 2011. Under the PSPPI Act all persons and companies guarding any real or personal property (including cash) belonging to another are required to be licensed or certified. Employers, including self employed persons, must hold a licence and employees must hold a Certificate of Approval. This process will include checks relating to applicants' criminal history, mental health, experience, competence and skills.

Part 3: Sector Summary

Abbreviated Risk Table

Sector	Overall ML/FT risk
Money remittance	HIGH
TCSPs	HIGH
Casinos	MEDIUM/HIGH
Currency exchange	MEDIUM
Safe Deposit Boxes	LOW/MEDIUM
Cash transport	LOW/MEDIUM
NBNDTLs	LOW
Financial leasing	LOW
Non bank credit cards	LOW
Factoring	LOW
Debt collection	LOW
Payroll remittance	LOW

Table 1. Overall ratings of risk by sector as determined by the SRA methodology (Structural Risk Indicators x Control Measures)

Summary by Sector

Money remittance (MR)

Overall risk rating – **HIGH**

54. MR poses the greatest risk of all the sectors assessed. MR services can be used at all stages of the money laundering process. Remittance services allow customers to enter money into the financial system (Placement), obscure the trail of dirty money through the transfer (Layering) and re-enter the market via the recipient financial system (Integration).
55. The MR sector in New Zealand is a large industry transferring millions of dollars in hundreds of thousands of transactions to over 200 countries, some of which can be considered high risk⁴. The lack of CDD measures and availability of online and mobile transfer services allow customers to maintain a level of anonymity and avoid detection through structuring techniques and the use of money mules or employees.
56. Information from New Zealand government agencies and FATF also suggests money laundering is being conducted by operators of MR businesses using their available remittance services to transfer illicit funds overseas. This may include collusion between operators and customers and presents a significant money laundering risk for the Department.
57. Informal or 'underground' remittance systems also present a high risk due to the lack of understanding of these services operating in New Zealand. While informal remittance is also used for legitimate purposes, the benefits of launderers using informal systems exceed those of registered MR companies by ensuring an added

⁴ Countries with inadequate AML/CFT controls

level of anonymity for the customer.

58. Although some companies have established AML/CFT procedure, there seems to be a lack of understanding and training in the detection of suspicious transactions and/or ML/TF methods for some reporting entities frontline staff.

Trust and Company Service Providers (TCSPs)

Overall risk rating – **HIGH**

59. Although TCSPs are not currently included in the AML/CFT regime they have been considered as part of the SRA due to the higher risk identified in recent media reports and international findings. The FATF Mutual Evaluation report noted significant vulnerabilities in the areas of CDD and services offered in the TCSP sector. 'The degree of complicity of the TCSPs in facilitating money laundering varies significantly with some unknowingly assisting in illicit activities and others having a greater knowledge of the illegal activities of their clients'.⁵
60. Company Formation Agents (CFAs) are considered higher risk due to the ability of money launderers to use CFAs to exploit the New Zealand Company Registration process. The use of nominee directors and shareholders, shell companies, limited partnerships and trusts create complex structures that can give the appearance of a legitimate purpose whilst making it difficult to establish beneficial ownership. While the CFA may not handle financial transactions itself, the lack of due diligence by CFAs makes it extremely easy for criminals to use these structures to shift money between entities whilst maintaining the anonymity of the client.
61. Other services provided by TCSPs, including virtual and registered offices and specialised financial services, can be used to add another layer of legitimacy and conceal beneficial ownership to facilitate money laundering.
62. The lack of current controls in the TCSP sector combined with the anonymity services can offer money launderers contribute to the overall HIGH risk rating.

Casinos

Overall risk rating – **MEDIUM/HIGH**

63. The casino sector is a complex environment when considering risk factors. Casinos are a cash intensive business there are many money laundering techniques that can be employed based on the diverse range of financial services offered. Conversely, there is already a level of regulatory scrutiny and AML control in casinos that mitigates the risk to some extent.
64. SkyCity Auckland can be considered higher risk predominantly due to its size (for the 2008/2009 financial year gaming gross revenue was NZD\$336.1 million compared to NZD\$36.7 million for Hamilton⁶). The sheer volume and size of transactions within SkyCity Auckland would suggest it is easier for criminals to maintain a level of anonymity and harder for casino staff to be fully aware of what is happening in the casino.

⁵ FATF-GAFI *The misuse of corporate vehicles including Trust and Company Service Providers*, 13 October 2006, pg

5

⁶ SkyCity Entertainment Group FY09 Full Year Result presentation, page 30, 16 August 2009

65. Junkets⁷ are considered high risk primarily due to the ease at which money is introduced to the New Zealand markets. Licensing processes for junkets are an area of particular concern. Careful consideration will need to be given to the controls and CDD requirements developed as part of the AML/CFT regime.
66. The other main concern is the difficulty in distinguishing suspected money launderers using illicit funds from ordinary patrons using legitimate funds. Many of the money laundering methodologies identified (cancel credits, currency exchange, redeeming winnings for casino cheques and use of prepaid credit cards) are the same behaviours seen in an innocent patron using legitimate funds. This may be more problematic in SkyCity Auckland where the size of the venue and volume of transactions may mean it is harder to 'know your customer'. These concerns may be somewhat mitigated by enhanced CDD requirements and lower reporting thresholds under the AML/CFT Act and Regulations.
67. Casino chips are not defined as 'currency' in either the AML/CFT Act or by New Zealand Customs Service. This poses a potential risk as they are not required to be declared on arrival to or departure from New Zealand and may be excluded from legislative and regulatory considerations regarding currency.

Currency Exchange (CE)

Overall risk rating – **MEDIUM**

68. Money laundering in the CE sector can only be seen as relevant in the 'Placement' stage of money laundering. In order to be successfully laundered funds need to be layered and then integrated back into the financial system.
69. The use of foreign exchange and prepaid currency cards present the highest risk for CE services. The accessibility and anonymity associated with these products make them an attractive placement tool for launderers. Bank drafts and travellers cheques can be considered lower risk; this is primarily due to the low number and value processed in New Zealand.
70. Identity fraud/false identification may pose potential risks for the CE sector. This is because of inadequate identity requirements currently in place in the currency exchange sector.
71. The use of refining⁸ and structuring techniques by way of in-store or online currency exchange services is assessed as low risk, due largely to the low limits on services and the fact that the currency will still require 'Layering' and 'Integration' to disguise illicit funds.
72. Current controls in the CE sector are considered adequate in some areas. However, consideration needs to be given to identity processes and more robust transaction monitoring and reporting.

⁷ Entering New Zealand for a limited period of time with the primary purpose of gambling in a casino where:

1. the arrangements are made, at least in part, by a junket organiser; and
2. all, or a substantial part, of the costs of transportation, food, and accommodation for the person entering New Zealand is paid by or on behalf of the holder of a casino licence.

⁸ Exchanging low denomination for high denomination currency.

Safe Deposit Boxes

Overall risk rating – **LOW/MEDIUM**

73. Safe deposit boxes are viewed as a tool to store cash whilst implementing the three stages of money laundering (Placement, Layering and Integration). The heightened risk rating is primarily due to the inability of vault employees to obtain information relating to the contents of the boxes and customers having unlimited access to facilities.
74. The ability to obtain a safe deposit box using fraudulent identification also adds another element of risk to the cash storage sector. This can be attributed to inadequate identity processes currently in place.
75. Although there are limited controls to overcome the privacy requirements in the safe deposit box sector, consideration should be given to improving current identity verification processes and access monitoring capabilities.

Cash Transport

Overall risk rating – **LOW/MEDIUM**

76. The cash transport sector in New Zealand is varied with companies offering a selection of services. The use of cash transport services can allow customers to enter money into the financial system via the cash collection service (Placement), obscure the trail of dirty money through the transfer (Layering) and re-enter the financial system through the bank deposit or delivery service (Integration).
77. The quantities of cash held and transported by cash transport companies vary depending on their insurance levels, capacity and individual client contracts. The high volumes of cash being transported and in some cases, an inability to establish source of funds make this sector vulnerable to money laundering. Clients can easily combine illicit funds with genuine takings in order to disguise their origin and increase their legitimacy.
78. A lack of CDD also presents a significant risk to the cash transport sector. Some reporting entities only conduct basic credit checks on new clients, which do not include any checks on directors and shareholders or company office checks.

Non-bank non-deposit-taking lenders (NBNDTLs)

Overall risk rating – **LOW**

79. NBNDTL are considered low risk for the Department in regards to money laundering. Identity fraud and structuring methodologies are possible however the low loan limits, general customer type and complexity of transactions makes these loan services potentially undesirable for money launderers.
80. The main area of concern in NBNDTLs is the ability to launder money by investing or being the provider of funds for loan companies. The Department currently has limited information regarding the source of funds used for lending and information provided by the sector indicates there is little due diligence conducted on investors. Further research will need to be carried out in order to fully understand funding in the NBNDTL sector.

Financial leasing

Overall risk rating – **LOW**

81. Money launderers may consider the use of financial leases as a means to legitimise money by making lease repayments using illicit funds. Interview responses suggest the current application process may not carry the desired level of anonymity required by money launderers; however some companies may provide services to shell companies or Limited Partnerships⁹ and the use of these corporate vehicles could enable beneficial owners to remain anonymous. Robust CDD checks on directors and shareholders of clients would be required to mitigate these risks.
82. Although financial leasing can be considered a way of purchasing valuable assets (a known money laundering typology) the complexity of lease agreements and the long term nature of financial leases may make them too complicated and time consuming for money launderers.

Non-bank credit cards

Overall risk rating – **LOW**

83. Non-bank credit cards (including charge cards) pose similar money laundering risks to credit cards issued by registered banks. The non-bank credit card sector is made up of open loop cards (global or domestic cards accepted at multiple outlets) and closed loop cards (accepted by specific New Zealand retailers that issue the cards).
84. CDD measures in the non-bank credit sector are considered inadequate in some cases. Applications using fraudulent identification are also a possible risk. Online services offer customers a level of anonymity and the acceptance of one form of identification make the application process vulnerable to potential money laundering activities.
85. Money launderers can structure or refine payments using illicit funds to avoid detection; this would be the most common form of money laundering using non-bank credit cards and presents the highest risk. Non-bank credit cards can also be used to transfer funds overseas via open loop global card networks, cash withdrawal options and the purchase of valuable assets. Robust transaction reporting capabilities to identify these risks are being used by some reporting entities.
86. Merchants also present a potential risk in regards to money laundering as they can use their own facilities to launder illicit funds. This method is difficult to detect and may involve collusion between customers and merchants.
87. Although non-bank credit cards can be considered a way of laundering money, the diverse range of card options available in New Zealand indicate this is more of a risk for global open loop cards and in most cases these companies have established AML/CFT procedure and robust transaction monitoring and reporting capabilities to mitigate the risks highlighted above.

⁹ Limited Partnerships are a form of partnership involving General Partners, (who are liable for all the debts and liabilities of the partnership) and Limited Partners (who are liable to the extent of their capital contribution to the partnership). A Limited Partnership is formed by registration in New Zealand http://www.business.govt.nz/companies/learn-about/other-entities/limited-partnerships/faqs/copy_of_introduction.

Factoring

Overall risk rating – **LOW**

88. Although factoring companies are able to conduct due diligence on their clients they are reliant on the CDD conducted by the client in regards to the debtor. This makes the identification of money laundering activity difficult.
89. Money laundering in the factoring sector would require some level of collusion between the client, factor and debtor in order to legitimise illicit funds. This may include the issuing of fraudulent invoices or organised fraudulent money flows between the client and factor or client and debtor.
90. The low transaction numbers and lack of high risk customers and transactions in the sector justify the low risk rating.

Debt collection

Overall risk rating – **LOW**

91. Debt collection poses the lowest risk to the Department. Debt collectors are unable to conduct adequate CDD on debtors and there is a lack of international evidence to suggest money laundering is occurring in the debt collection sector.
92. Debt collectors are reliant on the information provided by clients in relation to debtors. Money laundering in the debt collection sector would require some level of collusion between the client and debtor in order to legitimise illicit funds. The ability to identify these activities is limited as debt collectors do not conduct CDD on debtors. At present, there is no evidence to suggest this is occurring in the debt collection sector in New Zealand.

Payroll remittance

Overall risk rating – **LOW**

93. The Department's supervision of payroll remittance extends only to those companies that make payroll payments on behalf of their clients, not those that simply offer payroll administration services.
94. The use of 'ghost' or 'phantom' employees is a possible method to conduct money laundering transactions. However the requirement to supply an Inland Revenue Department (IRD) number for employees makes it more difficult to maintain anonymity therefore decreasing the attractiveness of this option as a method to launder money.
95. The low transaction and payment numbers and the lack of international evidence to suggest money laundering is occurring in the payroll remittance sector, justify the low risk rating.

Part 4: Sector risks

Money remittance or transfer services (MR)

Overview

96. The MR sector in New Zealand is diverse. Money can be remitted overseas through a variety of sources including the transfer facilities of banks, dedicated money transfer operators or non-bank institutions like credit unions, microfinance institutions and CE businesses. The Department is responsible for the supervision of dedicated money transfer operators and CE businesses.
97. The MR sector can be divided into two categories, traditional remittance systems which are often large organisations with numerous sub-agents and alternative or 'informal value transfer systems' (examples include 'hawala' and 'hundi'¹⁰). For the purpose of the SRA, traditional MR systems have been considered however the use of informal systems has been highlighted as a possibility under Industry Risks (see page 24).
98. MR services are used in all stages of the money laundering process (Placement, Layering and Integration). MR allows customers to enter money into the financial system (Placement), obscure the trail of dirty money through the transfer (Layering) and re-enter the financial system through recipient financial system (Integration).
99. The risks specific to the MR sector have been addressed below.
100. The overall risk assessment rating for MR is **HIGH**.

Structural risks

Size of sub-sector: volume of money flow and number of transactions

101. The exact number of reporting entities is still being determined, however there are approximately 820 identified agents offering MR services outside of New Zealand registered banks.
102. The total number of MR transactions can be split into inbound and outbound¹¹ transactions. The number of outbound transactions is estimated at 400,000 and inbounds 170,000 per year.
103. The estimated total value of transactions within a year is approximately \$150 - \$200 million. This includes both inbound and outbound transactions. These estimates are based on averages over the responses from interviews and questionnaires.

Proportion of cash intensive products and services

104. The majority of MR business is cash intensive. Most MR services operate by accepting cash at an agent location which is then electronically transferred to the recipient location for the receiver to pick up in cash also. The use of agent locations

¹⁰ Hawala and Hundi are alternative remittance systems that operate outside of traditional banking or financial channels.

¹¹ Inbound transactions are those transfers received by MR agents in New Zealand. Outbound transactions are those transfers sent overseas by MR agents in New Zealand.

is the most common form of money transfer.

105. Services are offered in over 100 currencies, however outbound transfers made using agent locations can only be facilitated using New Zealand currency.
106. Some reporting entities also offer online and/or mobile services. This service allows customers to conduct a money order transfer using their Visa or MasterCard via the internet or mobile phones.

Proportion of international transactions

107. The majority of MR transactions are international. Remittance services available in New Zealand are offered to over 200 countries worldwide.

Proportion of high risk customers (e.g. Politically Exposed Persons (PEPs), non-resident customers, private banking customers, trusts, bearer share holders etc)

108. The lack of information collected on customers using MR services makes the assessment of high risk customers difficult.
109. Remittance services are offered to over 200 countries worldwide. Some of these are considered higher risk due to their poor AML/CFT measures, including Latvia, Lithuania, Estonia, Cyprus, Azerbaijan, Vanuatu, Panama, Brazil, India and Seychelles.
110. Services are also offered to non-resident customers who are also considered high risk. This is due to their potential association with high risk countries and the difficulty of obtaining information relating to non-residents by law enforcement agencies.

Indicators of potential ML/TF activities

111. Five percent (1251 out of 25,219) of all STRs submitted for the period 2004-2008 were related to money remittance services. Recorded STRs for MR increased 55% between 2004 to 2007.
112. New Zealand government agencies have a current interest in MR companies with potential links to drug offending and organised crime.

Control measures

AML/CFT Regulations/Guidelines/Enforcement mechanisms in place

113. Currently the FTRA contains the main legislative requirements in relation to AML. This legislation imposes certain obligations on financial institutions in relation to the conduct of financial transactions including identity verification and reporting.
114. Some of the identified reporting entities offering MR services have established AML/CFT policy, procedure and training. This includes Know Your Customer (KYC) and CDD processes.

AML/CFT on-site inspections and off-site monitoring – supervisory compliance ratings

115. Currently MR agents are not actively regulated for AML/CFT purposes in New Zealand. There is no compliance/audit regime established and no on-site inspections or off-site monitoring.

Resources committed to AML/CFT by supervisory authorities (budget and number of staff)

116. At present, the Department's designated sector is not required to comply with their obligations under the AML/CFT Act, and consequently there is no compliance monitoring. There is currently five full time staff dedicated to implementing the Department's AML/CFT supervisory function. Enforcement officers will be recruited in preparation for the commencement of the AML/CFT Act and Regulations and the compliance monitoring programme.

Market entry/control (including fit and proper)

117. MR companies are required to be registered under the Financial Service Providers (Registration and Dispute Resolution) Act 2008. All MR providers will be required to be registered by December 2010.

Monitoring of transactions and adequacy of STR reporting

118. 1251 STRs were submitted for the period 2004 – 2008 relating to MR.

119. Some MR companies indicated they have adequate reporting systems to meet AML/CFT requirements.

Industry risks

120. **The structuring or refining of transfers/remittances under reporting thresholds to avoid detection.** Possible risk areas include:

- Numerous transactions under NZD\$9,999.99 to one recipient account,
- Numerous transaction under NZD\$9,999.99 to numerous accounts in a range of recipient countries,

The FATF/APG Mutual Evaluation noted the CDD threshold (NZD\$9,999.99) for wire transfer is too high.

- The use of numerous agent locations to conduct transactions,
- Some companies offer remittance services to countries with little or no AML controls and/or countries considered 'high risk' for terrorist activity,

The FATF/APG Mutual Evaluation noted there is no requirement for financial institutions to give special attention to transactions from or to high risk countries which do not sufficiently apply the FATF recommendations.

- Sub-agents operate on a commission based system and therefore are less likely to reject/report potentially suspicious activity,
- There are no set limits on the maximum amount customers can remit in one transaction,
- Use of online services to increase anonymity, this includes the use of credit cards which could be stolen or obtained using fraudulent identification ,
- Inadequate CDD measures.

The FATF/APG Mutual Evaluation noted there was no legal requirement for all wire transfers to be accompanied by full originator information.

121. **The use of money mules or employees to conduct MR transactions.** Risk areas include:
- Some reporting entities offer one off internet transactions which do not require identification,
 - Money laundering is difficult to detect if the 'mule' or employee does not have criminal links or is unknown to authorities,
 - Mules or employees are offered remuneration for services so are less likely to reject/report potentially suspicious activity,
 - Mules or employees are usually recruited using spam or email scams and often conduct money laundering transactions unknowingly.
122. **The use of fraudulent documents to exploit MR services.** Risk areas include:
- Most companies proof of identity process requires only one form of identification and in most cases accept a New Zealand Driver Licence which is considered insufficient to verify identity,
 - Fraudulent/false foreign passports are more problematic to identify,
 - The use of online services to increase anonymity, this includes the use of credit cards which could be stolen or obtained using fraudulent identification.
123. **Obtaining ownership over a MR company or sub-agent to exploit MR services.** Risk areas include:
- Money laundering via ownership of MR companies is difficult for law enforcement agencies to detect as it can involve collusion with customers and transactions are tailored to avoid detection,
The FATF/APG Mutual Evaluation noted there is no system in place to monitor Money or Value Transfer Service (MVTs) providers and ensure their compliance with FATF recommendations.
 - The use of false identification and fictitious names for customers,
 - Frequent transactions under reporting thresholds to avoid detection,
 - Turnover of the MR provider is unusually higher than comparable companies or agents,
 - MR provider has known organised crime connections,
 - Suspicious transactions performed on the bank account of the MR provider.
The FATF/APG Mutual Evaluation noted MVTs providers are not required to maintain a list of their agents and make that list available to the competent authorities.
124. **The use of the Informal Remittance Systems (IRSs) e.g. hawala or hundi.** Risk areas include:
- Money laundering is difficult for law enforcement agencies to detect,
 - IRSs are not fully understood in New Zealand,
 - IRSs offer cheaper rates and faster delivery than legitimate remittance services,
 - IRSs are an anonymous service that rely on established connections in order to keep anonymity,
 - IRSs are often unregistered companies established with the intention of avoiding legal and regulatory responsibilities,
 - Inadequate CDD,
 - Poor record keeping,
 - No registration requirement and no professional body oversight,
 - Ethnic operators may have linkages to, or sympathy for, groups supporting terrorist activity.
The FATF/APG Mutual Evaluation noted authorities have not taken sufficient action to identify informal remittance channels.

Trust and company service providers (TCSPs)

Overview

125. Although TCSPs are not currently covered by the AML/CFT Act, they have been proposed for inclusion as reporting entities under the AML/CFT regulations¹².
126. TCSPs include all persons or businesses that provide any of the following services¹³:
- a. acting as a formation agent of legal persons,
 - b. acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons,
 - c. providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement,
 - d. acting as (or arranging for another person to act as) a trustee of an express trust,
 - e. acting as (or arranging for another person to act as) a nominee shareholder for another person.
127. TCSPs can provide a number of services including:
- Trust services – services to domestic and international customers wanting to establish a trust in New Zealand. This may include assistance in the formation and maintenance of family, charitable, trading and foreign trusts.
 - Company formation agents (CFAs) – services to assist in the formation and maintenance of a New Zealand registered company.
 - Limited Partnerships services – services to assist in the formation and maintenance of a Limited Partnership or an Overseas Limited Partnership¹⁴.
 - Office services – which may include registered address, virtual and/or serviced offices and phone/mail forwarding services.
128. Recent media reports have implicated New Zealand companies formed via CFAs in attempts to bribe foreign officials and transport munitions between North Korea and Iran. This highlighted risk relating to TCSPs provides evidence to support inclusion of TCSPs as reporting entities.
129. The overall risk assessment rating for TCSPs is **HIGH**.

Structural risks

Size of sub-sector: volume of money flow and number of transactions

130. There are approximately 95 companies noted as offering TCSP services. The majority of reporting entities in the TCSP sector offer more than one service. The table below outlines the breakdown of services offered by TCSP sector reporting entities.

¹² Lawyers and Accountants may also offer TCSP services however are not currently included under the AML/CFT Act. This risk assessment covers all those TCSPs excluding legal or accountancy firms.

¹³ FATF-GAFI *The misuse of corporate vehicles including Trust and Company Service Providers*, 13 October 2006, pg 23

¹⁴ An Overseas Limited Partnership is a partnership that has been formed in a country other than New Zealand but because it is engaged in business activities in New Zealand it must register as an Overseas Limited Partnership. http://www.business.govt.nz/companies/learn-about/other-entities/limited-partnerships/faqs/copy_of_introduction

The table below outlines the breakdown of services offered by the TCSP sub-sector reporting entities:

Services offered	Approx. percent of sector offering services
CFAs	60%
Company services	40%
Trust Formation	46%
Limited Partnerships	15%

Proportion of cash intensive products and services

131. Less than 5% of all business would be conducted in cash. The majority of payments for services are made by Automatic Payment (AP), Direct Credit or Credit Card.
132. A large proportion of TCSPs do not meet their clients face to face, this indicates the opportunity to deal in cash is limited.

Proportion of international transactions

133. Approximately 70% of all TCSPs offer services to international customers. Approximately 20% do not specify whether international services are offered. It is, however, possible.
134. CFAs set up company structures for customers operating domestically and internationally. These services can be obtained via the internet making this service readily available for international customers wishing to establish companies in New Zealand. New Zealand government agencies indicate the majority of money laundering related transactions are made between international and domestic accounts linked to New Zealand registered companies.
135. Some trust service providers set up New Zealand foreign trusts and limited partnerships on behalf of their international clients from a range of jurisdictions. Respondents also noted that the majority of the time they would not meet clients in person as a large percentage of their clients were referrals from a known bank or lawyer overseas.

Proportion of high risk customers (e.g. PEPs, non-resident customers, private banking customers, trusts, bearer share holders etc)

136. The lack of CDD measures noted by some respondents in the TCSPs sector indicate significant risks associated with non-resident customers. Approximately 70% of all TCSPs offer services to international customers, 20% do not specify whether international services are offered, however it is possible.
137. New Zealand government agencies have noted some TCSPs conduct transactions with higher risk countries with weak AML/CFT measures and/or are known money laundering havens including Latvia, Lithuania, Estonia, Cyprus, Azerbaijan, Vanuatu, Panama and Seychelles.

138. Shell companies, limited partnerships and trusts are also considered higher risk. There is a lack of transparency in the formation process of these corporate vehicles and beneficial owners are sometimes difficult to establish.

Indicators of potential ML/FT activities

139. Recent media reports indicate New Zealand companies linked to TCSPs, including CFAs, have been involved in money laundering and munitions trading in the last few years. These reports note the use of shell companies and office services in these activities.
140. New Zealand government agencies have a current interest in CFAs and have identified a number of reporting entities that provide services to high risk customers.

Control measures

AML/CFT Regulations/Guidelines/Enforcement mechanisms in place

141. Currently TCSPs are unregulated and enforcement mechanisms are considered inadequate. FATF recommendations require TCSPs to be captured under AML/CFT legislation. None of the TCSPs consulted as part of the information collection process had established AML/CFT processes or training.

AML/CFT on-site inspections and off-site monitoring – supervisory compliance ratings

142. Currently TCSPs are not actively regulated for AML/CFT purposes in New Zealand. There is no compliance/audit regimes established and no on-site inspections or off-site monitoring.

Resources committed to AML/CFT by supervisory authorities (budget and number of staff)

143. TCSPs will need to be included as a reporting entity under the AML/CFT Act in order for the supervisor to have any regulatory authority.
144. At present, the Department's designated sector is not required to comply with their obligations under the AML/CFT Act, and consequently there is no compliance monitoring. There are currently five full time staff dedicated to implementing the Department's AML/CFT supervisory function. Enforcement officers will be recruited in preparation for the commencement of the AML/CFT Act and Regulations and the compliance monitoring programme.

Market entry/control (including fit and proper)

145. At present there are no market or entry controls in place for TCSPs, this includes any requirements to be registered or licensed.

Monitoring of transactions and adequacy of STR reporting

146. There have been no STRs submitted directly in relation to TCSPs.

147. Interview and questionnaire responses indicate TCSPs' current processes are inadequate to detect and report potential ML/FT activities. Some respondents indicated it was based on a 'gut feeling' approach.

Industry risks

148. The main risk associated with the use of TCSPs is the inability to determine the ultimate beneficial owner/s of companies, limited partnerships and trusts that use TCSP services. This is due to the inadequate CDD measures employed by most TCSPs. TCSPs have the ability to add another level of anonymity whilst increasing the appearance of a legitimate purpose.

149. It should be noted that there is a great variance in the levels of CDD conducted by the sector. Some trust service providers conduct greater levels of CDD on their clients. This may include certified identification, proof of residential address, declaration of source of funds, reference letter from a bank or lawyer and confirmation of advice on the tax structure in the clients jurisdiction (for those establishing foreign trusts). This level of CDD is significantly greater than some CFAs who offer services without conducting any CDD on entities involved in the company formation process.

Sector specific risks include:

150. **The exploitation of the New Zealand's companies registration process including the establishment of shell companies.** Risk areas include:

- Inadequate CDD measures including limited checks on directors and shareholders,

The FATF/APG Mutual Evaluation noted there is no requirement to obtain information on the purpose and intended nature of the business relationship.

- Beneficial owners are problematic to identify – shell companies can often have complex ownership structures using more than one entity,
- The ability to use the Certificate of Incorporation to establish bank accounts overseas,
- The ability to use New Zealand registered companies to conduct international wire transfers,
- Multi-jurisdictional structures that create a level of anonymity and the appearance of legitimacy,
- Conduits for funds transfers between third parties and company representatives,
- Some TCSPs offer services to international customers via the internet,
The FATF/APG Mutual Evaluation noted New Zealand has not implemented adequate AML/CFT measures for non-face to face business relationships or transactions
- Limited transaction reporting and monitoring capabilities.

151. **The use of nominee directors and shareholders.** Risk areas include:

- Beneficial owners are more problematic to identify due to the anonymity associated with the use of nominees,
- Clients can retain ownership and operational control through confidential ownership agreements or appointments that do not appear on company records (e.g. Vice President).

152. **The exploitation of weaknesses in TCSPs' processes to establish and manage trusts and limited partnerships for illegitimate purposes:** Risk areas include:
- Inadequate CDD measures including limited checks on beneficiaries and trustees,
 - Beneficial owners are problematic to identify - trusts can often have complex structures involving more than one entity,
 - Some TCSPs offer services to international customers via the internet,
 - The ability to transfer ownership of valuable assets such as property,
 - Limited transaction reporting and monitoring capabilities.
153. **The use of specialised financial intermediaries providing financial services.** Risk areas include:
- Financial intermediaries can conduct cash movements and asset management offshore,
 - Financial intermediaries can establish bank accounts on behalf on their clients,
 - The use of false invoicing or false investment losses,
 - Beneficial owners are more problematic to identify due to the anonymity associated with the use of specialist financial intermediaries.
154. **The use of virtual office services including registered offices and mail/phone forwarding services.** Risk areas include:
- Inadequate CDD measures including limited checks on directors and shareholders,
 - Beneficial owners are more problematic to identify ,
 - The use of registered offices and mail/phone forwarding services allow customers to establish a more significant local presence and increase legitimacy.

Casinos

Overview

155. The Department is mandated to enforce the provisions of the Gambling Act 2003. This legislation applies to gambling entities including casinos.
156. Under the Gambling Act, the Department is also authorised to issue Minimum Operating Standards (MOS) which set out internal controls for casinos. MOS currently include AML/CFT measures including transaction recording and reporting, as well as procedure for wire transfers. In a case of a breach of these standards, the Department may apply to the Gambling Commission for the cancellation or suspension of a casino licence.
157. SkyCity Entertainment Group (SkyCity) is the owner of SkyCity Auckland, Hamilton and Queenstown and a shareholder in Christchurch Casinos Ltd (about 33% directly, another 17% indirectly). Christchurch Casinos Ltd also has a small shareholding in Dunedin Casino. Lasseters Wharf Casino (Queenstown) is the only independently owned casino in New Zealand.
158. Casino products and services can be used in all stages of the money laundering process (Placement, Layering and Integration) however some may only be used during one stage.
159. Five of the six casinos have been interviewed as part of the information collection for the risk assessment.
160. The overall risk assessment rating for casinos is **MEDIUM/HIGH**.

Structural risks

Size of sub-sector: volume of money flow and number of transactions

161. There are six licensed casinos in New Zealand – Auckland, Hamilton, Christchurch, Dunedin and Queenstown (x2). The approximate revenue was \$465 million in the 2009 year. SkyCity Auckland is by far the largest casino with revenue of approximately NZD\$336 million for the 2008/2009 year. The approximate number of transactions¹⁵ for this period cannot be quantified, however research indicates it would be in the millions over all six casinos.

Proportion of cash intensive products and services

162. The majority of a casinos business is cash intensive. The following cash products/ services are offered in the casino sector:
 - Gambling on table games
 - Gambling using gaming machines
 - Purchase/redemption of gaming chips
 - Purchase/redemption of gaming machine tickets (TOTI¹⁶)

¹⁶ Ticket Out/Ticket In (TOTI) is a gaming machine system that allows gaming machines to accept either banknotes or tickets with a credit value printed on them (Ticket In) and up to, but not over the value of NZ\$500. TOTI also prints tickets with a credit value when a player wishes to 'cash out' of the gaming machine (Ticket Out). The player can then either redeem his/her ticket

¹⁵ This includes all transactions occurring as part of the casinos daily operations (cash desk, gaming machines, table games, customer accounts and VIP rooms)

- Redemption of gaming machine cancel credit transactions
- Issue/redemption of casino and other cheques
- Currency exchange
- Rewards points redeemed for cash

Proportion of international transactions

163. International transactions are deemed any transaction that involves an international customer. SkyCity Auckland can be considered the highest risk in regards to international transactions. Around 66% of all Sky City's international business in 2009/2010 came from SkyCity Auckland (\$14.5 million in 2009/2010 up from \$6.4 million in 2008/2009)¹⁷.

164. For Queenstown, Christchurch and Dunedin international transactions would account for less than 1% of all business.

Proportion of high risk customers (e.g. PEPs, non-resident customers, private banking customers, trusts, bearer share holders etc)

165. SkyCity Auckland has a high number of Asian patrons. This is primarily because it is a culturally attractive environment for them¹⁸. Known Asian Organised Crime (AOC) figures have been seen operating in SkyCity Auckland.

166. Very Important Person (VIP)/carded players account for a large number of all patrons in SkyCity Auckland and contribute a large proportion of all revenue. AOC figures have been known to frequent VIP rooms.

167. Casino based tourism or junkets at SkyCity Auckland allow non-residents to access casino gambling facilities in an organised gaming tour. The junket includes transport, accommodation, incentives and rewards to play at the casino and the transfer and management of funds in and out of the casino.

Indicators of potential ML/FT activities

168. 2.5% (638 out of 25,219) of all STRs submitted for the period 2004-2008 were related to casino gambling.

169. There have been thirteen known charges laid in relation to drug offending (a known money laundering predicate offence) that have had money laundering implications linked to the casino.

Control measures

AML/CFT Regulations/Guidelines/Enforcement mechanisms in place

170. The casinos are subject to the FTRA and are considered compliant in the following areas:
- a. Identity verification
 - b. Report suspicious transactions
 - c. Suspicious transaction reports not to be disclosed
 - d. Transaction recording

¹⁷ SkyCity Entertainment Group FY10 Full Year Result presentation, page 14, 17 August 2010

¹⁸ Findings of a strategic project completed by the Department in 2007 to analyse the extent of crime and criminality in the casinos.

e. Verification recording.

171. The Gambling Act 2003 and the Department are the main regulatory vehicles for ensuring compliance within the casinos; however there are no specific regulations relating to AML/CFT.
172. Casino Minimum Operating Standards (MOS) issued under the Gambling Act are enforceable instruments which include a range of AML/CFT requirements, essentially repeating and expanding on FTRA requirements and how they should be complied with in a casino environment. The SkyCity Cashiering MOS, for example, contain sections on Suspicious Transaction Reporting and procedures for identity verification in relation to large transactions, procedures for junkets, a definition of money laundering and indicators of suspicious transactions that may be deemed money laundering.
173. All front line staff receive training in FTRA reporting responsibilities and supervisors are responsible for submitting STRs. Relevant operational staff receive training in CDD in the context of the casinos' obligation under the FTRA; however at present this does not include specific AML/CFT requirements relating to the new regime.

AML/CFT on-site inspections and off-site monitoring – supervisory compliance ratings

174. Gambling inspectors are authorised to detect, investigate and prosecute offences under the Gambling Act 2003. This includes regular on site visits to the casino. Gambling Inspectors also have a statutory authority to obtain information to carry out their functions under this Act. Gambling inspectors can apply for search warrants under Sections 340 to 343 of the legislation. These powers are also designated to NZ Police.
175. The Gambling Act 2003 allows for a limited form of supervision via audits of compliance with casino Minimum Operating Standards (MOS). Casino inspectors audit compliance with AML/CFT related MOS as a small component of their audit function. This is a low priority due to the absence of full supervisory powers and resources.

Resources committed to AML/CFT by supervisory authorities (budget and number of staff)

176. Until the AML/CFT regime takes effect there are no compliance obligations under the AML/CFT Act. There are currently five full time staff dedicated to implementing the Department's AML/CFT supervisory function. Enforcement officers will be recruited in preparation for the commencement of the AML/CFT Act and Regulations and the compliance monitoring programme.

Market entry/control (including fit and proper)

177. Casinos are licensed by the Gambling Commission under the Gambling Act. The required procedures for granting a licence include 'fit and proper' checks, and such checks are also made by the Department on senior managers, Board members etc. All casinos must have a current casino venue licence and certain employees, including those involved in gambling and financial transaction must hold a Certificate of Approval (COA)¹⁹.

¹⁹ A COA is a legal document that permits and controls the persons employed by the casino. A COA is required for employees who interact with any form of gaming equipment including money or gaming chips.

Monitoring of transactions and adequacy of STR reporting

178. 638 STR were submitted for the period 2004 – 2008.

179. Casinos currently have STRs monitoring and reporting systems intended to fulfil FTRA requirements.

Industry Risks

180. The casino is a complex environment. The variety, frequency and volume of transactions as well as the high cash intensity of the business make the casino sector vulnerable to money laundering. The main concern when assessing risk in the casino is the difficulty in distinguishing money laundering from legitimate activity. Many of the money laundering methodologies identified (see Industry Risks below) are the same behaviours seen in innocent patrons using legitimate funds.

181. SkyCity Auckland can be considered higher risk predominantly due to its size (for the 2008/2009 financial year expenditure was approximately NZD\$336 million compared to NZD\$36.7million for Hamilton). The sheer volume and size of transactions within SkyCity Auckland means it is easier for criminals to maintain a level of anonymity and harder for casino staff to be fully aware of what is happening in the casino.

182. The majority of the risks identified below are drawn from information outlined in the *FATF/APG Vulnerabilities of Casinos and Gaming Sector March 2009*²⁰.

Casino Value Instruments

183. **Buying chips for cash or on account, then redeeming value by way of casino cheque or money transfer.** Risk areas include:

- Exploitation of the lack of communication between the tables and cash desks/main bank,
- Structured transactions below the \$9,999 FTRA identity verification requirements to avoid detection,
- Chips are easily transported and can be redeemed at other casinos in the SkyCity chain in New Zealand.

184. The risk is lowered when casino cheques or deposit accounts are used, as all activity is recorded by the casino.

185. **Cancel credits on Electronic Gaming Machines (EGM) or TOTI tickets.** Risk areas include:

- Crediting EGMs or TOTI tickets and cashing out immediately or with minimal play,
- Difficulty in distinguishing a cancel credit from a credit win²¹,
- Identification is only required on cancel credits or TOTI over the \$9,999 threshold,
- Casinos only record the names of persons requesting cancel credits over \$5000.

²⁰ This report addresses the money laundering vulnerabilities in the gaming and sector. The scope of the research included information relating to the gaming and casino sector in over 100 countries.

²¹ The cash value of credits paid to the credit meter as the result of a winning combination on a gaming machine.

186. **Use of chips as currency in illegal transactions.** Risk areas include:
- Chips are easily transported and can be redeemed in other casinos in the SkyCity chain,
 - Gaming chips are not defined as currency or a Bearer Negotiable Instrument (BNI) under the current AML/CFT legislation and there is no legal obligation to declare casino chips to New Zealand Customs Service on arrival to or departure from New Zealand.
187. **Purchase of casino rewards cards.** Risk areas include:
- Use of illicit funds to purchase casino rewards cards from legitimate patrons paying them a premium above the value of the reward,
 - Casino rewards cards are offered at all New Zealand casinos and members can accumulate points playing table games, EGMs as well as other facilities (including restaurants and bars and accommodation),
 - Casino rewards points can be redeemed for cash. Applicable limits vary from casino to casino and even within a casino depending on the membership tier.
188. **Purchase of chips from ‘clean’ players at a higher price.** Risk areas include:
- Gaming chips frequently change hands between patrons in VIP rooms
 - Money launderers are willing to suffer some loss in order to legitimise funds. Furthermore, the loss with the purchase of chips from clean players is lower than with gambling, where there is no guarantee of a return.
189. **Combining winnings and cash into casino cheques** – all casino cheques are recorded by the casino and the ratio of winnings to cash is noted and endorsed as non-verified²². Although this technique is possible it is unlikely as it does not afford patrons the level of anonymity associated with other methods.

Structuring/Refining

190. **Exchanging low denomination for high denomination currency.** Risk areas include:
- Refining using the cashiers desk – money launderers change funds from low to high denomination using the cashiers desk,
 - Refining using ‘note acceptors’ or gaming machines that accept cash – money launderers can insert multiple notes (up to and including \$20) and redeem credit after minimal or no play. This may also include patrons and/or syndicates chasing jackpots which legitimises funds further,
 - Refining using casino accounts – money launderers pay low denomination notes into their casino account and withdraw funds in higher denomination notes,
 - Transactions are often below the FTRA \$9,999 identity verification requirements to avoid detection,
 - Groups may refine money by dividing it amongst the groups before entering the casino,
 - This method is often associated with drug dealers who accumulate large amounts of small denomination notes from drug sales.

²² Non-verified is when the casino cannot verify that the funds were generated from gaming activity.

Use of casino accounts/facilities

191. **Cashing cheques into casino accounts.** Risk areas include:

- Cheques cashed or deposited into casino accounts and funds used to gamble.

192. **Deposits into casino accounts by wire transfer or bank cashiers cheque.** Risk areas include:

- Funds are deposited and then cashed out or transferred to another account with minimal or no gambling activity,
- The Department does not have access to casino account information.

Winning/intentional losses

193. **Use of illicit funds to gamble.** Risk areas include:

- This is the simplest method of legitimising illicit funds by generating certifiable winnings,
- It is difficult to distinguish a money launderer using illicit funds from an innocent patron gambling legally,
- In some casinos if the winnings are redeemed for a casino cheque it is endorsed as verified which further legitimises the money,
- This method is often associated with drug dealing.

194. **Parallel even betting/betting against associates/intentional losses.** Risk areas include:

- Transactions are often below the FTRA \$9,999 identity verification requirements to avoid detection,
- Typically witnessed on low odds, low risk games to ensure minimal loss.

195. **Buying winnings from legitimate customers.** Risk areas include:

- Money often changes hands in the casino so cannot be identified as the purchase of winnings,
- Money launderers are willing to suffer some loss in order to legitimise funds. Furthermore, the loss with the purchase of legitimate winnings is lower than with gambling where there is no guarantee of a return.

Currency Exchange

196. **Conversion of large sums of foreign currency.** Risk areas include:

- Sky City Auckland has a large foreign clientele (including junket groups and overseas commissioned players²³),
- Transactions are often below the FTRA \$9,999 identity verification requirements to avoid detection,
- No information is provided to the Department regarding individuals apprehended attempting to enter NZ with undeclared foreign currency.

Employee complicity

197. **Employee complicity.** Risk areas include:

- Difficulty in monitoring employees associations outside the casino,
- Employees failing to file suspicious transaction reports and/or record significant transactions,

²³ Junkets and Commission Based Players are discussed further in the document (see page 33)

- Employees tampering with documents/transactions related to CDD or reporting processes,
- Employees falsifying player ratings and other records

Credit/debit cards

198. **Use of credit cards to purchase gaming chips** – this is not currently permitted in SkyCity Auckland and Hamilton casinos. For those that do accept credit cards, there has only been one recorded instance of a credit card being used to purchase chips. The responsibility to identify the source of funds would be primarily placed on the relevant financial institution to which the credit card is associated.

False documents

199. **The use of false identification documents.** Risk areas include:

- Acceptance of only one form of identification,
- Acceptance of the New Zealand Driver Licence as a form of identification which is considered insufficient to verify identity,
- Fraudulent/false foreign passports will be more problematic to identify,
- Large number of recorded instances of false identification in the New Zealand casinos,
- In 2008 over 22,000 counterfeit passports were seized in Thailand²⁴; this indicates counterfeiting of passports is common and may have implications on New Zealand casinos with their large foreign clientele.

Casino based tourism

200. Casino-based tourism is more commonly known as junkets. Junkets are a holiday package for a group²⁵ of people to travel overseas in order to participate in gambling at casinos. They are usually afforded incentives to gamble at certain casinos. Junkets operations usually include transport, accommodation, incentives to gamble and the facilitation of the movement of funds for all participants. Typically money is pooled by the participants and the junket organiser pays it over in a lump sum to a casino account (which may be transferred from one of Skycity Auckland's overseas accounts located in Singapore and Hong Kong). A record is kept of individuals' winnings and these are distributed by the junket organiser at the end of the trip.

202. **The exploitation of the licensing process for junkets.** Risk areas include:

- Inadequate licensing process to conduct CDD on junket operators,
- Only the junket operator is subject to CDD before the arrival of the group,
- Reliance on DIA and Australian authorities to conduct relevant checks regarding the junket operator,
- Junket operators can waive the requirement to provide a Police Clearance from their country of residence by providing a signed statement outlining they were unable to obtain one,
- There is no requirement for copies of documentation relating to the junket operator to be verified,
- Junket members only provide identification on arrival to the casino,

²⁴ Reuters Foundation news article dated 27 April 2008

²⁵ Generally between 1 and 30 players in a group.

- Inadequate internal processes to establish legitimacy and/or source of funds,
- Ability to enter New Zealand without appropriate visa approval²⁶.

203. The use of foreign bank accounts/foreign holding accounts by junket groups.

Risk areas include:

- Inadequate internal processes to establish legitimacy and/or source of funds,
- Inadequate internal processes to establish beneficial owner,
- No enhanced CDD required,
- At the conclusion of the tour the funds are distributed by the junket operator and this distribution is not recorded by the casino.

204. The use of wire transfer by junket groups. Risk areas include:

- Junket operators control the financial transactions for the junket group, this creates a level of obscurity around the identity of the participants as well as the source and ownership of funds,
- Inadequate internal processes to establish legitimacy and/or source of funds,
- Inadequate internal processes to establish beneficial owner,
- No enhanced CDD required.

²⁶ There have been reported instances whereby junket operators have gained entry to New Zealand by New Zealand Customs Service without the appropriate visa. In these examples, operators have been given a warning but have still been allowed entry.

Currency Exchangers (CE)

Overview

205. The CE sector is a complex environment. Many of the reporting entities recorded as offering CE services often also offer remittance and in some cases lending services²⁷. Furthermore, there are approximately 600 that operate as part of New Zealand registered banks and credit unions and therefore will come under the supervision of The Reserve Bank.
206. Some CE companies offer personal and corporate services. It is important to note that all statistical information provided here includes both personal and corporate services and statistics for CE services provided by NZ registered banks.
207. Approximately 80% of the CE sector has been consulted as part of the information collection for this risk assessment.
208. The overall risk assessment rating for CE is **MEDIUM**

Structural risks

Size of sub-sector: volume of money flow and number of transactions

209. There are approximately 36 identified agencies offering CE exchange services. These companies are responsible for approximately 1216 subagents throughout New Zealand. Travelex is the dominant CE company and accounts for approximately 1100 of these subagents. As stated above, a number of these operate within New Zealand registered banks and are therefore the supervisory responsibility of The Reserve Bank.
210. The approximate number of CE transactions cannot be exactly defined but is estimated to be between 1 – 2 million on average per year.
211. The estimated total value of transactions within a year is approximately \$1.5 billion. This includes both personal and corporate transactions over the sector.

Proportion of cash intensive products and services

212. The majority of CE business is cash intensive. The following cash products/ services are offered:
- Retail and commercial foreign exchange
 - Travellers cheques
 - Prepaid currency cards
 - Drafts.
213. Some reporting entities also offer online services. This service allows customers to order currency online however the actual transaction (including payment) occurs in store.

²⁷ All remittance and lending services offered by CE companies have been assessed under their respective subsectors. For remittance see page 21 and lending see page 49.

Proportion of international transactions

214. It is difficult to determine the proportion of foreign exchange transactions that are international. Orders can be made online, and therefore can be done from anywhere in the world. It can also be assumed that most exchanges to foreign currency will be used overseas (including the purchase of Cash Passports, bank drafts and travellers cheques).

Proportion of high risk customers (e.g. PEPs, non-resident customers, private banking customers, trusts, bearer shareholders etc)

215. There is limited information regarding high risk customers for CE products and services, however research suggests customers include non-residents who are considered to be high risk.

Indicators of potential ML/FT activities

216. Less than 1% (240 out of 25,219) of all STRs submitted for the period 2004-2008 were related to bureaux de change²⁸.

217. A currency exchange company was implicated in a large multi million dollar money laundering operation in Auckland. The company was seen as a cover and to assist in the process of money laundering through the businesses services²⁹.

Control measures

AML/CFT Regulations/Guidelines/Enforcement mechanisms in place

218. Currently the FTRA contains the main legislative requirements in relation to AML. This legislation imposes certain obligations on financial institutions in relation to the conduct of financial transactions including identity verification and reporting.

219. Some of the identified reporting entities offering CE products and services have established AML/CFT policy, procedure and training. This includes KYC and CDD requirements.

AML/CFT on-site inspections and off-site monitoring – supervisory compliance ratings

220. Currently CE agents are not actively regulated for AML/CFT purposes. There are no compliance/audit regimes established and no on-site inspections or off-site monitoring.

Resources committed to AML/CFT by supervisory authorities (budget and number of staff)

221. At present, the Department's designated sector is not required to comply with obligations under the AML/CFT Act, and consequently there is no compliance monitoring. There are currently five full time staff dedicated to implementing the Department's AML/CFT supervisory function. Enforcement officers will be recruited in preparation for the commencement of the AML/CFT Act and Regulations and the compliance monitoring programme.

²⁸ Bureau de change is defined as an establishment where you can exchange foreign money.

²⁹ http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10660480

Market entry/control (including fit and proper)

222. CE companies are required to be registered under the Financial Service Providers (Registration and Dispute Resolution) Act 2008. All CE providers will be required to be registered by December 2010.

Monitoring of transactions and adequacy of STR reporting

223. 240 STR were submitted for the period 2004 – 2008 relating to bureau de change.

224. Some CE companies indicated they have adequate reporting systems to meet AML/CFT requirements.

Industry risks

225. Money laundering via CE facilities can be considered higher risk in the 'Placement' stage of the money laundering process. Placement can be conducted by purchasing a series of monetary instruments (foreign currency, cheques, cash passport, drafts) that are then collected or deposited into accounts at another location. 'Layering' may occur through a series of conversions or wire transfers however in order to be successfully laundered funds need to be re-entered into the financial system ('Integration') this may occur via investments in real estate, luxury assets or business ventures. It should be noted that some currency exchange agencies also offer remittance services (see MR page 21). This can make the transition to layering of illicit funds more simple and accessible.

Sector specific risks include:

226. **The purchase of foreign currency/the exchange of small denomination bills for larger denominations.** Risk areas include:

- The structuring of transactions under reporting thresholds to avoid detection,
- Use of online services to increase anonymity. However at present for some online services the actual transaction, including payment, is conducted in store.

227. **The use of prepaid currency cards (e.g. Cash Passport).** Risk areas include:

- The structuring of purchases or reloads³⁰ under reporting thresholds to avoid detection,
- The purchase of multiple cards in various currencies. Customers can have one card in every currency (EU€, GB£, US\$, AU\$ and NZ\$),
- Cash withdrawal is available and accessible at over 1.4 million ATMs worldwide.

228. **The use of travellers' cheques.** Risk areas include:

- The purchase or structuring of multiple cheques in a range of currencies under the reporting thresholds to avoid detection,
- Cheques are accepted at numerous locations worldwide.

³⁰ Cash passports can be reloaded online or in-store. A maximum of \$17,000 at one time can be loaded on a Cash Passport or \$51,000 total during any 12 month period.

229. It should be noted the use of travellers cheques has decreased with the introduction of the prepaid currency card.

230. **The use of bank drafts (foreign currency cheques).** Risk areas include:

- The purchase or structuring of multiple drafts under the reporting thresholds to avoid detection,
- Drafts are deposited into bank accounts (facilitating the Layering stage of money laundering).

231. **The use of fraudulent documents to exploit CE services.** Risk areas include:

- Most companies proof of identity process requires only one form of identification and in most cases accept a New Zealand Driver Licence which is considered insufficient to verify identity,
- Fraudulent/false foreign passports will be more problematic to identify.

Cash storage – Safe deposit boxes

Overview

232. Safe deposit boxes are viewed as a tool to store illicit funds whilst implementing the Placement, Layering and Integration stages of the money laundering process. Customers have unlimited access to the vaults during opening hours and due to the provider guaranteeing privacy of access and contents, safe deposit boxes vault employees are unable to identify the contents of the boxes or what customers do during access times.
233. Safe deposit boxes are currently offered at some of the registered banks in New Zealand, however the Act specifies a reporting entity will only have one designated supervisor therefore these will come under the Reserve Bank's supervision. The safe deposit facilities outside the registered banks will be supervised by the Department and all risks identified are in relation to non-bank safe deposit boxes.
234. 80% of identified reporting entities offering safe deposit facilities (outside the registered banks) were consulted as part of the information collection process.
235. The overall risk assessment rating for non-bank safe deposit boxes is **LOW/ MEDIUM**. This risk rating is higher primarily due to the inability to monitor safe deposit box contents and activities.

Structural risks

Size of sub-sector: volume of money flow and number of transactions

236. There are five vaults in New Zealand offering safe deposit box facilities. There is also another company in the process of establishing this service. The total number of available safe deposit boxes is approximately 11,000. Research indicates roughly 70% of these are currently rented.
237. The gross profit from safe deposit facilities is estimated at \$3 million based on information obtained from reporting entities consulted during the collection phase.
238. Transaction information for the safe deposit sector is difficult to quantify. Customers rent safe deposit boxes on an annual basis and make one rental payment per year usually by Direct Credit. In terms of access monitoring, customers' access ranges from daily to monthly. Most of the vaults monitor any significant increases in customers accessing the vaults (i.e. more than once daily) however exact access/ transaction information is unattainable.

Proportion of cash intensive products and services

239. In regards to payment for safe deposit boxes, most of the companies accept Direct Credit, Credit Cards, EFTPOS, cheques and cash, although three of the companies noted that cash payments were minimal.
240. All companies have strict privacy policies whereby they are not informed of the contents of the boxes. Three of the safe deposit companies noted that they assumed some of their customers were storing cash. This was seen as potentially more common with Asian customers.

Proportion of international transactions

241. Reporting entities indicate there are minimal international transactions. This is predominantly attributed to customers requiring physical access to the service. Less than 5% of customers reside overseas indicating there may be minimal international transactions in the form of annual payments for rentals.

Proportion of high risk customers (e.g. PEPs, non-resident customers, private banking customers, trusts, bearer share holders etc)

242. There is limited information regarding high risk customers for safe deposit facilities. The majority of the companies noted they had a high percentage of Asian customers (approximately 35% in Wellington and 60% in Auckland). However, this is not indicative of high risk customers and there is no evidenced link between safe deposit box use and AOC.

243. One company in Auckland offers 24 hour access and is located relatively close to the casino. This may pose a potential risk for AOC figures and money launderers using the safe deposit boxes to store illicit funds before or after using the casino as a means to launder them. Due to the fact that the contents of boxes are not disclosed this cannot be confirmed.

Indicators of potential ML/FT activities

244. There is one recorded STR that involved the movement of money from an individual's safety deposit box into their own current account. However, this STR was not made by the cash storage sector.

245. Four of the five safe deposit companies noted some interaction with Police regarding items contained in boxes by persons of interest. These have been linked with drugs and cash storage. One noted a Police warrant executed in 2008 revealed \$500,000 in cash.

Control measures

AML/CFT Regulations/Guidelines/Enforcement mechanisms in place

246. The regulations, guidelines and enforcement mechanisms for AML/CFT currently in place are considered low. However all respondents appeared to have robust CDD processes in place to mitigate issues related with the privacy policies guaranteed with safe deposit boxes.

AML/CFT on-site inspections and off-site monitoring – supervisory compliance ratings

247. Currently safe deposit facilities are not actively regulated for AML/CFT purposes. There is no compliance/audit regimes established and no on-site inspections or off-site monitoring.

Resources committed to AML/CFT by supervisory authorities (budget and number of staff)

248. At present, the Department's designated sector is not required to comply with their obligations under the AML/CFT Act, and consequently there is no compliance monitoring. There are currently five full time staff dedicated to implementing the

Department's AML/CFT supervisory function. Enforcement officers will be recruited in preparation for the commencement of the AML/CFT Act and Regulations and the compliance monitoring programme.

Market entry/control (including fit and proper)

249. At present there are no market or entry controls in place for safe deposit facilities. This includes any requirements to be registered or licensed. However market entry is limited as there are a small number of sufficiently secure vaults available in New Zealand.

Monitoring of transactions and adequacy of STR reporting

250. There is one recorded STR that involved the movement of money from an individual's safety deposit box into their own current account. However, this STR was not made by the cash storage sector.

251. Information provided by reporting entities indicates safe deposit companies have limited customer access monitoring and reporting capabilities. Four of the five companies indicated they provided information to NZ Police on request and in some instances reported suspicious activities however this was not in the form of an STR.

Industry risks

252. **The use of safe deposit boxes to store illicit funds.** Risk areas include:

- Privacy policies restrict companies from obtaining information relating to the contents of safe deposit boxes,
- Inadequate reporting systems to monitor patterns of access,
- Rogue employees allowing customers access without appropriate identification,
- High percentage of customer base is Asian therefore it is possible there may be AOC figures utilising safe deposit box facilities,
- 24 hour access increases money laundering ability by allowing added anonymity and more frequent access.

253. **The use of fraudulent documents to obtain a safe deposit box.** Risk areas include:

- The acceptance of only one form of identification,
- The acceptance of the New Zealand Driver Licence as a form of identification which is considered insufficient to verify identity,
- Fraudulent/false foreign passports will be more problematic to identify.

Cash Transport

Overview

254. The range of services offered by cash transport companies in New Zealand is varied. As well as cash collection and delivery these may include precious cargo, data transport, ATM collection and maintenance, safe clearance, cash storage, cash counting, cash deposit, cross border transportation and float supply and delivery.
255. Cash transport services can be seen as a vehicle to transfer illicit funds whilst adding another layer of anonymity. These services can be used in all stages of the money laundering process (Placement, Layering and Integration). The use of cash transport services can allow customers to enter money into the financial system via the cash collection service (Placement), obscure the trail of dirty money through the transfer (Layering) and re-enter the financial system through the bank deposit or delivery service (Integration).
256. Cash transport companies will be required to be compliant with the Private Security Personnel and Private Investigators Act 2010 (the PSPPI Act) from 1 April 2011. Under the PSPPI Act all persons and companies guarding any real or personal property (including cash) belonging to another are required to be licensed or certified. Employers, including self employed persons, must hold a licence and employees must hold a Certificate of Approval. This process will include checks relating to applicants' criminal history, mental health, experience, competence and skills. Although this new legislation may mitigate some of the risks associated with rogue employees it does not address the issue of the client using cash transport services to launder illicit funds.
257. 57% of identified reporting entities offering cash transport services were consulted as part of the information collection process.
258. The overall risk assessment rating for cash transport is **LOW/MEDIUM**.

Structural Risks

Size of sub-sector: volume of money flow and number of transactions

259. There are four companies currently identified as offering cash transport services in New Zealand. All reporting entities consulted indicated their core business was cash collection and delivery. Reporting entities vary significantly in size. The number of vehicles available for transport varies greatly and client contracts may be based on daily, weekly or monthly transactions. All respondents indicated they did offer services for ad-hoc events (for example galas and concerts) and they are normally based on a one-off collection and delivery transaction.
260. Volume of money flow for the cash transport sector is difficult to quantify. Information obtained during the collection phase indicates the sector can be separated into large and small companies. The larger companies have the ability and capacity to transport significantly larger quantities of cash and deal in the cross border movement of funds. The smaller firms transport lower quantities of cash, primarily for small to medium sized businesses.

Proportion of cash intensive products and services

261. All respondents indicated that cash transport was the core part of their business. As indicated above, the levels of cash held and transported by the reporting entities vary depending on their insurance levels and client contracts. The high volumes of cash being transported and the inability to establish the source of funds in some cases make this sector vulnerable to money laundering.
262. For those companies that do not offer cash counting services the cash is transported in a tamper-proof sealed bag and signed by the client and employee at the time of pick up and then again at drop off or deposit.
263. Most respondents also offer cash storage facilities. However cash is not normally stored for longer than 24 hours.

Proportion of international transactions

264. 50% of reporting entities consulted indicated they dealt in foreign currency which requires cross border movement of funds. The majority of these types of transactions were for registered banks with which they have established contracts. In most cases, the business relationship was with the New Zealand registered entity or branch and robust CDD processes were in place to lessen the risk of money laundering.

Proportion of high risk customers (e.g. PEPs, non-resident customers, private banking customers, trusts, bearer share holders etc)

265. There is limited information regarding high risk customers for cash transport companies. All respondents indicated they did not transport cash from private or residential addresses and the majority of their clients were banks and retailers, which were often chain stores. The majority of business relationships were long term contracts that require daily or weekly transactions. Some respondents did indicate they offered daily services to small to medium sized businesses. This presents the greatest money laundering risk to the sector as it is more problematic to identify the source of funds. Clients can easily combine illicit funds with genuine takings in order to disguise their origin and increase their legitimacy.

Indicators of potential ML/FT activities

266. Two of the four cash transport companies noted they had received requests to conduct private transactions from residential addresses; however, all requests had been declined. One respondent indicated money laundering was a possibility as 'dirty' money could be added to the takings of businesses and then deposited into the client's account by the cash transport company. In some cases reporting entities are unable to establish the source of funds which poses a potential money laundering risk.

Control Measures

AML/CFT Regulations/Guidelines/Enforcement mechanisms in place

267. The regulations, guidelines and enforcement mechanisms for AML/CFT currently in place are considered low. However one respondent indicated they have robust CDD processes in place to mitigate some of the potential money laundering risks associated with cash transport. These included Companies Office search, verification of directors (including a copy of passport or Driver Licence), credit check, historical information (including previous addresses and directors) as well as partnership or trust agreements, depending on the client type.
268. One respondent noted they were currently in the process of drafting their AML/CFT policy to meet the requirements of the AML/CFT Act. Another noted they had training for some staff that meets the AML/CFT requirements in the United States.

AML/CFT on-site inspections and off-site monitoring – supervisory compliance ratings

269. Currently cash transport companies are not actively regulated for AML/CFT purposes. There is no compliance/audit regime established and no on-site inspections or off-site monitoring.

Resources committed to AML/CFT by supervisory authorities (budget and number of staff)

270. At present, the Department's designated sector is not required to comply with obligations under the AML/CFT Act, and consequently there is no compliance monitoring. There is currently five full time staff dedicated to implementing the Department's AML/CFT supervisory function. Enforcement officers will be recruited in preparation for the commencement of the AML/CFT Act and Regulations and the compliance monitoring programme.

Market entry/control (including fit and proper)

271. At present there are no market or entry controls in place for cash transport companies. This includes any requirements to be registered or licensed. However the PSPPI Act which comes into force in 1 April 2011 will require all persons and companies guarding any real or personal property (including cash) belonging to another to be licensed or certified. Employers, including self employed persons, must hold a licence and employees must hold a Certificate of Approval.

Monitoring of transactions and adequacy of STR reporting

272. Information provided by reporting entities indicates cash transport companies have robust monitoring and reporting capabilities. Respondents indicated they had to record and sign off on cash collection and delivery, however they did note that they did not have established procedure for identifying suspicious activity and any reporting was based on a 'gut feeling'.

Industry Risks

273. Cash transport services can be used at all stages of the money laundering process (Placement, Layering and Integration). The main risk area with the cash transport sector is the lack of CDD by some reporting entities, including an inability to establish source of funds. Some respondents indicated the only checks they conducted on new clients were basic credit checks on the company which does

not include checks on individual directors and shareholders or company office checks.

274. **The use of cash transport services to transfer illicit funds.** Risk areas include:

- Procedure that restrict companies from obtaining information relating to the source of funds,
- Inadequate CDD measures including limited checks on individuals associated with the company
- Inadequate reporting and monitoring to identify patterns of suspicious activity.

275. **Employee complicity.** Risk areas include:

- Employees failing to report suspicious activity
- Difficulty in monitoring employees' associations outside of work

Non-Bank Non-Deposit-Taking Lenders (NBNDTLs)

Overview

276. A NBNDTL can be defined as a non-bank institution that lends to customers but does not take deposits from those applying for funds.
277. 9% of NBNDTL have been consulted as part of the information collection phase of this risk assessment.
278. The overall risk assessment rating for NBNDTL is **LOW**

Structural risks

Size of sub-sector: volume of money flow and number of transactions

279. There are approximately 190 identified reporting entities offering NBNDTL services. Approximately 8% of these offer one other service (either debt collection, financial leasing or foreign exchange³¹)
280. Volume turnover for NBNDTL is difficult to establish. Approximately 61% of all NBNDTL offer personal loans (up to \$50,000), 15% offer commercial loans (\$50,000+), 14% are charitable lenders offering small loans for charitable organisations and 10% are unknown.
281. The estimated total value of transactions within a year is approximately \$7.5 million for NBNDTL offering personal loans³².

Proportion of cash intensive products and services

282. Minimal activity in the NBNDTL business is cash intensive. The majority of repayments for loans are made via Direct Debit. Some customers make repayments in-store using cash but these are low value. Furthermore, funds are provided to customers via bank account deposits or direct to the company where the loan has been approved to purchase goods or services from (for example, payments made direct to car dealerships for vehicle loans).

Proportion of international transactions

283. Of the reporting entities that responded to the questionnaire or were interviewed, more than 95% did not offer loan facilities to international customers. Research indicates international transactions would be less than 1% in regards to loan repayments.
284. There is limited information relating to the source of funds used for lending. Some reporting entities noted they have overseas investors, this indicates some international transactions may occur in relation to investment funds. Further research is needed to fully comprehend the extent of international transactions in this area.

³¹ Debt collection, financial leasing and foreign exchange risks have been assessed under their respective sectors.

³² This value is an estimate based on available information provided by NBNDTL that responded to the questionnaire or were interviewed as part of the information collection process.

Proportion of high risk customers (e.g. PEPs, non-resident customers, private banking customers, trusts, bearer share holders etc)

285. There is limited information regarding high risk customers for NBNDTL services including investors. Research indicates some reporting entities offer loan services to individuals residing in New Zealand on work visas or permits. These customers can be classified as non-residents and therefore higher risk.

Indicators of potential ML/FT activities

286. There are no recorded STRs submitted in relation to NBNDTL and no recorded cases relating to money laundering activity in the NBNDTL sector in New Zealand. There is also little information available from international bodies such as FATF to indicate whether money laundering is prevalent in the NBNDTL sector.

287. Some NBNDTL indicated they had received loan applications using fraudulent identity documents and in some cases this was reported to NZ Police.

Control measures

AML/CFT Regulations/Guidelines/Enforcement mechanisms in place

288. Currently the FTRA contains the main legislative requirements in relation to AML. This legislation imposes certain obligations on financial institutions in relation to the conduct of financial transactions including identity verification and reporting.

289. The regulations, guidelines and enforcement mechanisms currently in place are considered low.

AML/CFT on-site inspections and off-site monitoring – supervisory compliance ratings

290. Currently NBNDTL are not actively regulated for AML/CFT purposes. There are no compliance/audit regimes established and no on-site inspections or off-site monitoring.

Resources committed to AML/CFT by supervisory authorities (budget and number of staff)

291. At present, the Department's designated sector is not required to comply with obligations under the AML/CFT Act, and consequently there is no compliance monitoring. There are currently five full time staff dedicated to implementing the Department's AML/CFT supervisory function. Enforcement officers will be recruited in preparation for the commencement of the AML/CFT Act and Regulations and the compliance monitoring programme.

Market entry/control (including fit and proper)

292. NBNDTLs are required to be registered under the Financial Service Providers (Registration and Dispute Resolution) Act 2008. All NBNDTLs will be required to be registered by December 2010.

Monitoring of transactions and adequacy of STR reporting

293. No STRs have been submitted in relation the money laundering in the NBNDTL sector.
294. Research indicates NBNDTLs have limited transaction monitoring and reporting capabilities. NBNDTLs who responded to the questionnaires and interviews indicated suspicious transactions and applications were identified using a 'gut feeling' approach and in most cases not reported to any form of law enforcement. Most respondents also indicated they did not conduct due diligence on the provider of the funds.

Industry risks

295. **The use of loan facilities offered by NBNDTL.** Risk areas include:
- The structuring of loan repayments under reporting thresholds to avoid detection,
 - The repayment of loans using large cash payments,
 - Applying for loans and paying them off in one large repayment,
 - The purchase of valuable assets (vehicles, property) using illicit funds to make repayments.
296. **The use of fraudulent documents to exploit NBNDTL.** Risk areas include:
- Acceptance of only one form of identification,
 - Acceptance of the New Zealand Driver Licence as a form of identification which is considered insufficient to verify identity,
 - Fraudulent/false foreign passports will be more problematic to identify.
297. **Money laundering by investing in or being the provider of funds for NBNDTL.** Risk areas include:
- Limited due diligence conducted on the provider of funds or investors,
 - Provider of funds or investors residing outside New Zealand,
 - Limited understanding of how funding/investment occurs in the NBNDTL sector by the Department.

Financial leasing

Overview

298. The AML/CFT Act 2009 defines businesses that carry out financial leasing activities as a financial institution. It does however exclude financial leasing arrangements in relation to consumer products.
299. Financial leasing is where companies engage in financing the purchase of tangible assets. The leasing company is the legal owner of the goods, but ownership is effectively conveyed to the lessee, who incurs all benefits, costs, and risks associated with ownership of the assets. Financial leases may also be referred to as Lease to Own agreements.
300. Financial Leasing companies are required to be compliant with the Credit Contracts and Consumer Finance Act 2003 (and its regulations). This legislation is designed to provide transparency between companies and customers and reduces unfair conduct. It does not have any AML/CFT requirements.
301. 36% of identified reporting entities offering financial leasing services were consulted as part of the information collection process.
302. APG specifies the purchase of valuable assets as a common money laundering typology. A financial lease works by way of transferring ownership of high value assets, such as vehicles and equipment, to lessees over the course of the lease agreement therefore financial leases can be considered a means to purchase valuable assets. However due to the complex and long term nature of lease agreements it may not be seen as the most efficient technique to launder money.
303. The overall risk assessment rating for financial leasing is **LOW**.

Structural risks

Size of sub-sector: volume of money flow and number of transactions

304. There are 25 identified companies offering financial leasing services in New Zealand, most of these being for vehicle or equipment financing. All of the reporting entities consulted identified operating leases (or the like) as their main business and financial leases only a small proportion of business (less than 10% of all business in most cases).
305. The extent of the money flow in the financial leasing sector cannot be fully identified however research suggests it would be low due to the low percentage of business it accounts for. Research indicates operating revenue for the last fiscal year would be approximately \$100 - 200 million for financial leases only (based on the average operating revenue for respondents).
306. Transaction information for the financial leasing sector is difficult to quantify. Reporting entities may have a certain number of customers but the customers can have up to ten lease agreements with the company and therefore numerous payments or transactions. Some respondents noted the average daily number of transactions to be between 40 and 70.

Proportion of cash intensive products and services

307. Financial leases rarely deal in cash. None of the reporting entities interviewed accepted cash as a form of regular payment. Lease payments are commonly paid by Direct Credit from customers.

Proportion of international transactions

308. Financial leasing companies have a low proportion of customers based outside of New Zealand. Of those that did provide international lease options this equated for less than 3% of all business (customers and transactions).

Proportion of high risk customers (e.g. PEPs, non-resident customers, private banking customers, trusts, bearer shareholders etc)

309. There is limited information regarding high risk customers for Financial Leasing companies however the majority of customers tend to be larger scale corporate entities (government, banks, telecommunications, airlines) or Small and Medium Enterprises. None of the reporting entities consulted offered financial leasing services to individuals.
310. Some companies offer financial lease services to Limited Liability Companies (LLC) which may pose a potential risk in terms of identifying the beneficial owner due to the ownership and management structures of some LLCs (see TCSP Industry Risks, page 28 for more information).

Indicators of potential ML/FT activities

311. No STR reports have been submitted in relation to the money laundering in the financial leasing sector, however there are four recorded STRs linked to Finance Companies, details of these reports are unknown.
312. None of the respondents indicated they had ever had a suspicious transaction or application and noted minimal interaction with any law enforcement agencies.

Control measures

AML/CFT Regulations/Guidelines/Enforcement mechanisms in place

313. At least 30% of all financial leasing companies have established AML/CFT policies, procedure and training. This can be attributed to their Australian and US branches having established protocol that is replicated in New Zealand.
314. For all other identified reporting entities the regulations, guidelines and enforcement mechanisms currently in place are considered low in regards to AML/CFT.

AML/CFT on-site inspections and off-site monitoring – supervisory compliance ratings

315. Currently Financial Leasing companies are not actively regulated for AML/CFT purposes in New Zealand. There is no compliance/audit regimes established and no on-site inspections or off-site monitoring.

Resources committed to AML/CFT by supervisory authorities (budget and number of staff)

316. At present, the Department's designated sector is not required to comply with obligations under the AML/CFT Act, and consequently there is no compliance monitoring. There are currently five full time staff dedicated to implementing the Department's AML/CFT supervisory function. Enforcement officers will be recruited in preparation for the commencement of the AML/CFT Act and Regulations and the compliance monitoring programme.

Market entry/control (including fit and proper)

317. At present there are no market or entry controls in place for financial leasing companies, this includes any requirements to be registered or licensed.

Monitoring of transactions and adequacy of STR reporting

318. There have been no STRs submitted directly by financial leasing companies.

319. Some companies claimed they had adequate reporting systems to identify suspicious activity; this appears more common in those with established AML/CFT procedures. For the rest of the sector the current systems are considered poor.

Industry risks

320. **The use of illicit funds to make lease repayments in order to acquire high value assets.** Risk areas include:

- Irregular or unusual repayments ,
- Full payments to terminate lease agreements early,
- Numerous lease agreements similar to structuring whereby money is laundered through various streams or transactions to avoid detection,
- Large cash repayments,
- Limited due diligence checks on companies and directors/shareholders of companies,
- Limited transaction reporting and monitoring capabilities.

321. **The use of shell companies to exploit financial leasing services.** Risk areas include:

- Limited due diligence checks on companies and directors/shareholders of companies,
- Beneficial owners are more problematic to identify – shell companies can often have complex ownership structures.

Non-Bank Credit Cards

Overview

322. Credit card companies are required to be compliant with the Credit Contracts and Consumer Finance Act 2003 (and its regulations). This legislation is designed to provide transparency between companies and customers and reduce unfair conduct. It does not have any AML/CFT requirements.
323. Non-bank credit cards pose similar risks to credit cards provided by registered banks. Credit card issuing and acquiring is viewed as posing a lower risk of money laundering compared with other financial products and services. The sophisticated application process and monitoring systems used in relation to credit card products and services combined with restrictions on cash payments, cash access and credit balances, make them less effective as a vehicle for money laundering.
324. Merchants³³ present different, and potentially somewhat higher, risks for money laundering than the issuing of cards or card application process. This is due to fundamental differences in the financial transactions being effected by the merchants compared to the card holders (including volume and value differences; the merchant's ability to effect refunds, which can raise the risk of collusion; charging for non-existent goods and transferability of charge receipts).
325. There are two types of non-bank credit cards:
- Open Loop Cards - these are typically issued by global associations and can be used at multiple retailers. Some open loop cards are accepted at multiple retailers but only in New Zealand.
 - Closed Loop Cards - these are typically used only at a specific retailer that issued the card and are not usually part of an association or global card network.
326. Some companies provide a variety of card options including options for personal and corporate use and various levels and rewards depending on the credit limits and income of customers.
327. 35% of identified reporting entities offering non-bank credit card facilities were consulted as part of the information collection process.
328. The overall risk assessment rating for non-bank credit cards is **LOW**.

Structural risks

Size of sub-sector: volume of money flow and number of transactions

329. There are fourteen identified non-bank credit cards in New Zealand.
330. Research suggests transaction numbers for non-bank credit cards is approximately 500,000 per month over all non-bank credit cards.
331. Volume of money flow in the non-bank credit card sector is difficult to quantify. Reporting entities have different credit levels for customers who are assessed

³³ Any person, firm or corporation that has contracted with an acquirer to process transactions.

using a risk based approach and allocated a credit level reflective of their risk rating.

332. The average purchase for open loop cards is \$300 for international transactions and \$150 for domestic purchases.

Proportion of cash intensive products and services

333. Card repayments can be made in cash either in-store, through NZ Post or via one of the registered banks, dependent on the payment options set up by the company.
334. Respondents to interviews noted that repayments made in cash were minimal. CDD and reporting for large or suspicious transactions made to registered banks is the responsibility of the banks and not the card company.
335. In some cases, enquiries are not made on large direct debit repayments.

Proportion of international transactions

336. There are two identified open loop non-bank credit cards. These cards process approximately 70,000 international transactions total per month. One of these providers accounts for 85% of all international transactions.

Proportion of high risk customers (e.g. PEPs, non-resident customers, private banking customers, trusts, bearer shareholders etc)

337. There is limited information regarding high risk customers for non-bank credit card use. Online application and approval services afford customers a level of anonymity and limit the companies' ability to have face to face interaction (less than 20% are met in person).
338. Some companies offer card services to corporate customers as well as individuals. The credit limits on these can be up to NZ\$1million.
339. Merchants pose a potential risk and have been known to use their personal cards to make purchases in their own stores to accumulate points and potentially conduct tax evasion.

Indicators of potential ML/FT activities

340. There are 131 recorded STRs for credit cards, however it is not specified whether they are in regards to bank or non-bank credit or charge cards.
341. Most suspicious reporting from non-bank credit cards has been in relation to large cash payments and/or structuring (making numerous payments a month) or refining (using multiple locations to make payments).

Control Measures

AML/CFT Regulations/Guidelines/Enforcement mechanisms in place

342. Global credit/charge cards have established AML/CFT policy, procedure and training in place.

343. Further information is required to assess the AML/CFT regulations, guidelines and enforcement mechanisms currently in place for all other reporting entities.

AML/CFT on-site inspections and off-site monitoring – supervisory compliance ratings

344. Currently non-bank credit card companies are not actively regulated for AML/CFT purposes in New Zealand. There are no compliance/audit regimes established and no on-site inspections or off-site monitoring.

Resources committed to AML/CFT by supervisory authorities (budget and number of staff)

345. At present, the Department's designated sector is not required to comply with obligations under the AML/CFT Act, and consequently there is no compliance monitoring. There are currently five full time staff dedicated to implementing the Department's AML/CFT supervisory function. Enforcement officers will be recruited in preparation for the commencement of the AML/CFT Act and Regulations and the compliance monitoring programme.

Market entry/control (including fit and proper)

346. Any entity that issues means of payment, including credit cards, are required to be registered under the Financial Service Providers (Registration and Dispute Resolution) Act 2008. All credit card providers will be required to be registered by December 2010.

Monitoring of transactions and adequacy of STR reporting

347. There have been 131 STRs submitted directly in relation to credit cards in general. Global credit/charge card companies submit STRs where appropriate. STR reporting for all other reporting entities is not yet fully understood.

348. Some companies claim they have adequate reporting systems to identify suspicious activity; this appears more common in those with established AML/CFT procedures.

Industry risks

349. **The use of fraudulent documents to obtain a non-bank credit card.** Risk areas include:

- Acceptance of only one form of identification,
- Acceptance of the New Zealand Driver Licence as a form of identification which is considered insufficient to verify identity,
- Fraudulent/false foreign passports will be more problematic to identify,
- Online services afford customers and increased level of anonymity.

350. **The structuring or refining of card repayments under reporting thresholds to avoid detection.** Risk areas include:

- Multiple smaller sum payments within a month,
- Multiple payments at a range of branches,
- Overpayments of due balance and/or credit limits,
- Where banks accept payment there is a level of reliance on the banks to report suspicious or significant transactions,

- The ability to have multiple authorised users on a single card or multiple cards,
- Limited transaction reporting and monitoring capabilities.

351. The use of non-bank credit cards to transfer funds overseas (for global open loop cards). Risk areas include:

- Ability to access cash at a range of ATMs worldwide,
- Multiple cash withdrawals in overseas locations,
- Easy cross border movement with limited audit trail,
- Unusual purchase of goods or services in countries regarded as posing a heightened risk for money laundering,
- Large cross border wire transfer payments,
- Limited transaction reporting and monitoring capabilities.

352. The purchase of valuable assets using non-bank credit cards. Risk areas include:

- Unusual cash advances and/or large cash payments,
- Overpayments on credit limits or available funds,
- Purchase of large items paid off in full.

353. Merchants using non-bank credit card facilities exploit card companies. Risk areas include:

- Excessive or unusual patterns of refunds,
- Collusion between customers and merchants,
- Charging of non-existent goods.

Factoring

Overview

354. Factoring can be defined as a financing method in which a business owner sells accounts receivable at a discount to a third-party (factor) to raise capital and the factor collects the debt.
355. Factoring is a complex sub-sector. Many identified reporting entities offer recourse and non-recourse factoring options³⁴, as well as other financial services including invoice discounting³⁵ and credit finance. In some cases factoring companies will also offer debt collection or non-bank non-deposit taking lending services³⁶.
356. 11% of identified reporting entities offering debt factoring services were consulted as part of the information collection process.
357. The overall risk assessment rating for factoring is **LOW**.

Structural risks

Size of sub-sector: volume of money flow and number of transactions

358. There are 27 identified companies offering factoring services in New Zealand. 55% of these offer only factoring services, 19% offer both factoring and debt collection and 26% offer factoring and NBNDTL.
359. At present it is difficult to quantify the number of transactions and money flow in the factoring sector. Respondents indicated the size of a transaction could vary significantly depending on the value of the invoice purchased. Respondents estimated they would process approximately 500 – 1000 invoices per month.

Proportion of cash intensive products and services

360. It is uncommon for factoring companies to deal in cash. All respondents indicated they would not accept cash as payment from debtors nor would they pay their clients in cash. The majority of transactions are conducted via bank transfer and a small amount through cheques (from debtors).

Proportion of international transactions

361. Respondents indicated less than 10% of their business would involve international transactions. One respondent did note that invoices purchased from international clients tended to be of greater value.

Proportion of high risk customers (e.g. PEPs, non-resident customers, private banking customers, trusts, bearer share holders etc)

³⁴ Recourse factoring can be defined as the legal ability of the purchaser (factor) of a financial asset to fall back on the original creditor if the current debtor defaults. Non-recourse is factoring whereby the purchaser (factor) assumes full credit risk and responsibility for collection of debt.

³⁵ Invoice discounting is a method to draw loans from a company's unpaid invoices that does not require the company to relinquish administrative control of the invoices.

³⁶ For the risk assessment of the non-bank non-deposit taking lenders subsector see page 49 and the debt collection sector see page 62.

362. The extent to which high risk customers are involved in the sector cannot be fully understood at present. Some respondents indicated they provided services to international clients in the USA, United Kingdom and Australia.
363. Respondents indicated the majority of their customers are small to medium sized businesses and in most cases they meet with the client more than once face to face. They also noted they had well established relationships with their customers as the majority were repeat customers. Respondents also indicated they also require confirmation that the goods or services have been supplied before the invoice purchase will occur.

Indicators of potential ML/FT activities

364. No STRs have been submitted in relation to money laundering in the factoring sector.
365. Some respondents noted they had received requests from government agencies (including Inland Revenue Department and the Serious Fraud Office) regarding one of their clients. These requests were in relation to fraud investigations.

Control measures

AML/CFT Regulations/Guidelines/Enforcement mechanisms in place

366. Currently the FTRA contains the main legislative requirements in relation to AML. This legislation imposes certain obligations on financial institutions in relation to the conduct of financial transactions including identity verification and reporting.
367. There are currently no AML/CFT specific regulations, guidelines or enforcement mechanisms in place.

AML/CFT on-site inspections and off-site monitoring – supervisory compliance ratings

368. Currently factoring agencies are not actively regulated for AML/CFT purposes in New Zealand. There are no compliance/audit regimes established and no on-site inspections or off-site monitoring.

Resources committed to AML/CFT by supervisory authorities (budget and number of staff)

369. At present, the Department's designated sector is not required to comply with obligations under the AML/CFT Act, and consequently there is no compliance monitoring. There is currently five full time staff dedicated to implementing the Department's AML/CFT supervisory function. Enforcement officers will be recruited in preparation for the commencement of the AML/CFT Act and Regulations and the compliance monitoring programme.

Market entry/control (including fit and proper)

370. There are currently no market entry/control requirements for factoring.

Monitoring of transactions and adequacy of STR reporting

371. There have been no STRs submitted in relation to factoring.

372. Some respondents indicated they currently have sufficient reporting systems able to perform monitoring and reporting for suspicious transactions related to money laundering activity. This includes trend analysis to identify patterns of client behaviour.

Industry risks

373. Factoring agencies are reliant on the information provided by their clients and are unable to conduct appropriate levels of CDD on debtors.

374. Money laundering through the use of false invoicing (which involves either the overpricing of legitimate invoices or the issuing of fictitious invoices) in order to use the excess or artificial amount to legitimise and launder the illicit funds. This process would require some form of collusion between any combination of the debtor, factor and client.

Debt collection

Overview

375. A debt collection agency will attempt to collect payments from debtors on behalf of their client. This is primarily because the client is unable to get hold of the debtor, the debtor refuses to pay the client or the client may want to outsource some of their debt collection activity for efficiency. The debt collection agency will charge a fee or commission for the debts recovered. Unrecoverable debt is normally returned to the client.
376. Debt collectors are reliant on the information provided by the client in relation to debtors and therefore it is difficult for debt collection agencies to conduct robust CDD on the debtor. Money laundering in the debt collection sub-sector would require some form of collusion between the debt collection agency, client and/or debtor.
377. 25% of identified reporting entities offering debt collection reporting entities were consulted as part of the information collection process.
378. The overall risk assessment rating for debt collection is **LOW**.

Structural risks

Size of sub-sector: volume of money flow and number of transactions

379. There are 65 identified companies offering debt collection services in New Zealand. 86% of these offer only debt collection services, 8% offer both debt collection and factoring and 6% offer debt collection and NBNDTL.
380. The debt collection sector can be loosely split in to large and small companies. The average debt collected for the smaller agencies ranges from \$55 - \$10,000 per customer with an average of 55 receipts a day³⁷. The larger companies are harder to approximate. They have hundreds of thousands of transactions per month and can collect up to \$40million in a year.

Proportion of cash intensive products and services

381. It is uncommon for larger companies to receive payments in the form of cash. They may on occasion have a debtor make cash payments into the head office; however the number and value are minimal. This is similar to the smaller companies; however they do on occasion receive small payments in cash to the office or during visits to debtors.

Proportion of international transactions

382. The majority of companies do not offer services to international customers. For those that do, international customers make up less than 5% of all customers and typically reside in Australia, therefore international transactions are minimal.

Proportion of high risk customers (e.g. PEPs, non-resident customers, private banking customers, trusts, bearer share holders etc)

³⁷ Average transaction information is based on responses from questionnaires

383. The extent to which high risk customers are involved in the sector cannot be fully understood at present. Debt collection agencies collect information on their clients but there is a high level of reliance on the client to conduct CDD on the debtor (as part of the initial business interaction and contract).

Indicators of potential ML/FT activities

384. No STRs have been submitted in relation to money laundering in the debt collection sector.

385. None of the respondents indicated they had ever had a suspicious transaction or application and noted minimal interaction with any law enforcement agencies in regards to money laundering.

Control measures

AML/CFT Regulations/Guidelines/Enforcement mechanisms in place

386. Currently the FTRA contains the main legislative requirements in relation to AML. This legislation imposes certain obligations on financial institutions in relation to the conduct of financial transactions including identity verification and reporting.

387. There are currently no AML/CFT specific regulations, guidelines or enforcement mechanisms in place.

AML/CFT on-site inspections and off-site monitoring – supervisory compliance ratings

388. Currently debt collection agencies are not actively regulated for AML/CFT purposes in New Zealand. There are no compliance/audit regimes established and no on-site inspections or off-site monitoring.

Resources committed to AML/CFT by supervisory authorities (budget and number of staff)

389. At present, the Department's designated sector is not required to comply with obligations under the AML/CFT Act, and consequently there is no compliance monitoring. There is currently five full time staff dedicated to implementing the Department's AML/CFT supervisory function. Enforcement officers will be recruited in preparation for the commencement of the AML/CFT Act and Regulations and the compliance monitoring programme.

Market entry/control (including fit and proper)

390. There are currently no market entry/control requirements for debt collection. The sector is however in the process of setting up a Debt Collectors Association (a forum used to discuss issues, trends and legislative changes within the sector).

Monitoring of transactions and adequacy of STR reporting

391. There have been no STRs submitted in relation to debt collection.

392. Some larger companies specified they currently have sufficient reporting systems able to perform monitoring and reporting for suspicious transactions related to money laundering activity.

Industry risks

393. Debt collection agencies are reliant on the information provided by customers and are unable to conduct appropriate levels of CDD on debtors.
394. Money laundering through debt collection agencies would require some level of collusion between the customer and debtor in order to legitimise the illicit funds via a 'money go round'.

Payroll Remittance

Overview

395. Payroll services can be classified into two types:
- Payroll administration services – the purpose of these businesses is to generate payroll information for clients by using timesheets to calculate payments and PAYE deductions. It does not include processing payroll payments which is completed by the client
 - Payroll bureau services – this includes the administration services as well as the direct deposit of pay into employee bank accounts on behalf of the client and managing the PAYE deductions
396. For the purpose of this risk assessment, only companies offering payroll bureau services are considered. It is understood that these companies are the only services required to be compliant under the AML/CFT Act and regulations.
397. 40% of identified reporting entities offering payroll remittance services were consulted as part of the information collection process.
398. The overall risk assessment rating for payroll remittance is **LOW**.

Structural risks

Size of sub-sector: volume of money flow and number of transactions

399. There are eleven identified payroll companies in New Zealand. 27% of these offer only payroll administration services and 73% offer both payroll administration and bureau services.
400. There are two forms of payroll remittance companies:
- Large corporate companies – these companies specialise in payroll remittance services and have a large customer base. In most cases they provide software and support also
 - Small and Medium Enterprises (SME)- businesses where payroll remittance is a portion of the services they provide to customers. Other services may include human resources, recruitment, administration and financial services. Often their clients are also SMEs with less than 20 employees
401. Research suggests transaction numbers for payroll remittance companies is 50 – 100 per month for the smaller companies and approximately 1500 for the larger corporate companies.

Proportion of cash intensive products and services

402. None of the reporting entities consulted made any remittances using cash. All of the transactions were made using direct debit transfers and used sophisticated software to process transactions.

Proportion of international transactions

403. International transactions are minimal in the payroll remittance sector. Some reporting entities have a small number of international clients. However this service is used to pay the New Zealand employees, and all customers are New Zealand registered companies.

Proportion of high risk customers (e.g. PEPs, non-resident customers, private banking customers, trusts, bearer share holders etc)

404. The extent to which high risk customers are involved in the sector cannot be fully understood at present. Payroll remittance agencies collect information on their clients but there is a high level of reliance on the client to provide accurate information on employees/recipients of payments.

Indicators of potential ML/FT activities

405. There are no recorded STRs linked to payroll remittance services.

406. One respondent indicated they had received enquiries from international companies requesting payroll remittance services however the enquirer refused to provide the required information and were therefore declined services. This may be indicative of potential money laundering or tax evasion activity.

407. There is a lack of international evidence signalling ML/TF risks in the payroll remittance sector.

Control measures

AML/CFT Regulations/Guidelines/Enforcement mechanisms in place

408. There are currently no AML/CFT specific regulations, guidelines or enforcement mechanisms in place for payroll remittance companies.

AML/CFT on-site inspections and off-site monitoring – supervisory compliance ratings

409. Currently payroll remittance agencies are not actively regulated for AML/CFT purposes in New Zealand. There are no compliance/audit regimes established and no on-site inspections or off-site monitoring.

Resources committed to AML/CFT by supervisory authorities (budget and number of staff)

410. At present, the Department's designated sector is not required to comply with obligations under the AML/CFT Act, and consequently there is no compliance monitoring. There is currently five full time staff dedicated to implementing the Department's AML/CFT supervisory function. Enforcement officers will be recruited in preparation for the commencement of the AML/CFT Act and Regulations and the compliance monitoring programme.

Market entry/control (including fit and proper)

412. At present there are no market or entry controls in place for payroll remittance companies. This includes any requirements to be registered or licensed. Some identified reporting entities are registered as PAYE intermediaries as part of the Inland Revenue Department (IRD) PAYE Intermediary scheme. This scheme allows employers who pay less than \$500,000 in PAYE and ESCT each year eligible for a subsidy (\$2 per employee per payday) to use a listed PAYE intermediary. PAYE intermediaries must be compliant with PAYE rules and the Tax Act 2007 and have appropriate administration and IT systems³⁸. PAYE intermediaries lower the ML risk as the direct association with IRD requires full disclosure of their business operations.

Monitoring of transactions and adequacy of STR reporting

413. Some companies claimed they had adequate reporting systems to identify suspicious activity however this was more prevalent with the larger corporate entities.

Industry risks

414. **The use of ‘ghost’ or ‘phantom’ employees (fictitious employees created on a payroll list) to exploit payroll remittance service. This may be through the use of fraudulent identity documents.** Risk areas include:

- Inability of payroll remittance companies to conduct CDD on employees of recipients of payments,
- Acceptance of only one form of identification,
- Acceptance of the New Zealand Driver Licence as a form of identification which is considered insufficient to verify identity,
- Fraudulent/false foreign passports will be more problematic to identify.

415. **The use of payroll cards³⁹ to exploit payroll remittance services.** Risk areas include:

- The structuring of purchases under reporting thresholds to avoid detection,
- Cash withdrawal is available via ATMs.

³⁸ <http://www.ird.govt.nz/resources/a/d/ad422f004bbe5bad9fcadfb87554a30/ir910-apr09.pdf>

³⁹ Payroll cards are an electronic card whereby wages are deposited via direct deposit, and the employee uses the card to withdraw cash at an ATM or purchase goods and services. Research indicates these are not currently offered in New Zealand.

Appendix A.

Assessment methodology

Structural risks	↑ Factors that increase the risk ↑	↓ Factors that reduce the risk ↓
Size	<ul style="list-style-type: none"> • Large assets held by entities in the industry • High values of transactions 	<ul style="list-style-type: none"> • Fewer assets held by entities in the industry • Low values of transactions
Volume	<ul style="list-style-type: none"> • High volumes of transactions making it harder to check the legitimacy of each transaction 	<ul style="list-style-type: none"> • Low volumes of transactions making it easier to check each transaction
Products and services	<ul style="list-style-type: none"> • High number of cash based products and services • High percentage of products and services paid for with cash or able to be loaded with cash 	<ul style="list-style-type: none"> • Limited or no products and services that rely on cash for payment or as part of the product (loading)
International transactions	<ul style="list-style-type: none"> • High level of transactions with overseas entities or to other countries • Parties to the transaction based in higher risk jurisdictions • Nested / payable through accounts available or operated through correspondent accounts • NZ is neither the origin nor destination in the transaction 	<ul style="list-style-type: none"> • Domestic only transactions • Transacts only with jurisdictions with known AML/CFT control requirements • Transacts with entities regulated for AML/CFT requirements in those jurisdictions
Customers	<ul style="list-style-type: none"> • Has customers that are: <ul style="list-style-type: none"> • Foreign PEPs • High net worth individuals • Trusts and charities • Overseas entities, especially those in off-shore secrecy havens 	<ul style="list-style-type: none"> • All or high number of domestic customers (NZ resident) • Low value accounts and transactions • Transactions consistent with profiles • Transparent ownership structures • Regulated entities for AML/CFT compliance
Indicators	<ul style="list-style-type: none"> • High number of reporting Suspicious Transaction Reports (STRs) • High number of those reports as quality reports showing tangible evidence of suspect behaviour or transactions • Low level of reporting of STR where inconsistent with the level expected in line with crime rates or reporting in other industries 	<ul style="list-style-type: none"> • Low number of STR reports consistent with expectation and lowering crime rates in NZ

Appendix B.

Acronyms

AML/CFT – Anti-money laundering/countering financing of terrorism

AOC – Asian Organised Crime

APG – Asia Pacific Group

BNI – Bearer Negotiable Instrument

CDD – Customer Due Diligence

CE – Currency Exchangers

CFAs – Company Formation Agents

COA – Certificate of Approval

EDD – Enhanced Due Diligence

EFTPOS - Electronic Funds Transfer at Point of Sale

EGMs – Electronic Gaming Machines

FIU – Financial Intelligence Unit (New Zealand Police)

FTRA – Financial Transaction Reporting Act 1996

IRS – Informal remittance system

KYC – Know Your Customer

LLC – Limited Liability Companies

ML/TF – Money laundering/Terrorist Financing

MOS – Minimum Operating Standards

MVTS – Money or Value Transfer Services

NBNDTL – Non-bank non-deposit-taking lenders

NRA – National Risk Assessment

SRA – Sector Risk Assessment

STRs – Suspicious Transaction Reports

TCSPs – Trust and Company Service Providers

TOTI - Ticket Out Ticket In

VIP – Very Important Persons

Appendix C.

Definitions

AML/CFT Supervisors – are defined by the FATF as “*the designated competent authorities responsible for ensuring compliance by financial institutions with requirements to combat money laundering and terrorist financing*”. New Zealand incorporates a multi supervisor model to capitalise on existing regulators expertise and industry knowledge of each financial sector. The supervisors are:

1. **Securities Commission of New Zealand** – supervisor for issuers of securities, trustee companies, futures dealers, funds managers, brokers and financial advisers.
2. **Reserve Bank of New Zealand** – supervisor for registered banks, non-bank deposit takers and life insurers.
3. **Department of Internal Affairs** – supervisor for money remitters, TCSPs, casinos, currency exchangers, NBNDTLs, financial leasing, safe deposit boxes, debt collection, payroll remittance, non-bank credit cards and entities not elsewhere supervised.

Bearer Negotiable Instruments – includes monetary instruments in bearer form such as: travelers cheques; negotiable instruments (including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee’s name omitted.

Beneficial Owner – means the individual who –

- a. has effective control of a customer or person on whose behalf a transaction is conducted; or
- b. owns a prescribed threshold of the customer or person on whose behalf a transaction is conducted

Bureau de change – is defined as an establishment where you can exchange foreign money.

Cash Passport – is a prepaid, PIN-protected travel money card available in five currencies. It can be reloaded online or in-store. A maximum of \$17,000 at one time can be loaded on a Cash Passport or \$51,000 total during any 12 month period.

Certificate of Approval (COA) – is a legal document that permits and controls the persons employed by the casino. A COA is required for employees who interact with any form of gaming equipment including money or gaming chips

Financial Institutions – are defined in Part 1, Section 3 of the FTRA96. The following entities are included in the definition under the FTRA96:

1. Accountants (within specified limits)
2. Building societies
3. Friendly societies or credit unions
4. Lawyers (within specified limits)
5. Licensed casinos
6. Life insurance companies
7. New Zealand Racing Board
8. Real estate agents

9. Registered banks
10. Reserve Bank of New Zealand
11. Sharebrokers
12. Trustees or managers of superannuation schemes
13. Trustees or managers of unit trusts
14. Any person whose business or a principal part of whose business consists of any of the following:
 - a. borrowing or lending or investing money;
 - b. administering or managing funds on behalf of other persons;
 - c. acting as trustee in respect of funds of other persons;
 - d. dealing in life insurance policies ; and
 - e. 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.

Hawala or Hundi – are alternative remittance systems that operate outside of traditional banking or financial channels.

Integration – the third stage of money laundering in which the funds re-enter the legitimate economy.

Junket – entering New Zealand for a limited period of time with the primary purpose of gambling in a casino where:

1. the arrangements are made, at least in part, by a junket organiser; and
2. all, or a substantial part, of the costs of transportation, food, and accommodation for the person entering New Zealand is paid by or on behalf of the holder of a casino licence.

Junket organiser – means a person who organises a junket for financial gain.

Layering – is the second stage of money laundering where the launderer engages in a series of conversions or movements of funds to distance them from their source.

Merchant – any person, firm or corporation that has contracted with an acquirer to process transactions.

Placement – the stage of money laundering where the launderer introduces his illegal profits into the financial system.

Reverse engineering – is the process of discovering the technological principles of a device, object or system through analysis of its structure, function and operation.

Ticket Out/Ticket In (TOTI) – is a gaming machine system that allows gaming machines to accept either banknotes or tickets with a credit value printed on them (Ticket In) and up to, but not over the value of NZ\$500. TOTI also prints tickets with a credit value when a player wishes to 'cash out' of the gaming machine (Ticket Out). The player can then either redeem his/her ticket for cash at a cashier (up to but not over NZ\$9,990), or insert the ticket straight into another TOTI machine and continue playing.