Te Tari Taiwhenua
Internal Affairs

New Zealand Government

Financial Institutions Sector Risk Assessment

December 2019

NOTE: This sector risk assessment is intended to provide a summary and general overview. It does not assess every risk relevant to the covered sectors. It does not set out the comprehensive obligations under the *Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act 2009* and associated AML/CFT regulations and codes of practice. It does not constitute, nor should it be treated as, legal advice or opinion. The Department of Internal Affairs accepts no liability for any loss suffered as a result of reliance on this publication.

Contents

Executive summary

Scope

1. This Sector Risk Assessment (SRA) is an update to the second anti-money laundering and countering financing of terrorism (AML/CFT) risk assessment undertaken by the Department of Internal Affairs (DIA) for reporting entities determined to be Financial Institutions under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the Act).

2. As part of the definition of 'Financial Institutions', DIA supervises money remitters, currency exchangers, payment providers, non-bank non-deposit taking lenders (NBNDTLs), non-bank credit cards, stored value cards, tax pooling, cash transport, debt collection, factoring, financial leasing, payroll remittance and safe deposit boxes. A new sector, virtual asset service providers, (VASPs) has been created as part of the 2019 update, reflecting the development and growth of this sector, and newly issued guidance from international sources. VASPs were previously covered as part of the payment providers sector.

3. The trusts and company service providers (TCSPs) and casino sectors have been moved from the previous 'Phase 1' SRA to the new 'Designated non-financial businesses and professions' (DNFPBs) SRA – this was previously the 'Phase 2' SRA

4. DIA also supervise any other businesses whose activities are covered by the Act and are not supervised by the Reserve Bank of New Zealand (RBNZ) or the Financial Markets Authority (FMA).

5. **Reporting entities do not have to read the whole document. All reporting entities should read the Executive Summary, Parts 1 to 5 and Part 20. Each reporting entity should review their sector-specific assessment covering general risks and industry characteristics associated with money laundering and terrorism financing (ML/TF). They should also be familiar with the high risks and vulnerabilities impacting on their sector.**

6. The Financial Institutions SRA 2019 has two functions: it will help DIA AML/CFT supervisors in their continuing understanding of the risks of ML/TF in the Financial Institution sectors, and it will help the Financial Institution sectors meet their AML/CFT obligations. This includes identifying, monitoring and mitigating ML/TF risks, and reporting suspicious or unusual activity to the New Zealand Police Financial Intelligence Unit (FIU). The RBNZ and FMA have published similar risk assessments for the sectors they supervise.[1]

7. All countries are exposed to illicit international money flows. The global nature of ML/TF is reflected in the work of the Financial Action Task Force (FATF) based on input from experts across the globe. The FATF 40 Recommendations form the basis of international efforts to counter ML/TF. New Zealand, via products such as the Financial Institutions SRA 2019, is working towards implementing the FATF 40 Recommendations in a way that is tailored towards its own ML/TF risks.

8. The Financial Institutions SRA 2019 is separated into two parts: the SRA itself and the SRA support document. The SRA can be read on its own and will provide reporting entities with an overview of their key ML/FT risks and vulnerabilities. The support document contains all appendices for the SRA and covers more technical aspects, including the risk assessment process and methodology, and details on significant vulnerabilities and high-risk factors.

9. A companion document to the SRA – *AML/CFT Risk Assessment and Programme: Prompts and*

[1] FMA. (2017). *Anti-Money Laundering and Countering Financing of Terrorism Sector Risk Assessment 2017*. http://bit.ly/2jTH2Pg
RBNZ. (2017). *Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Sector Risk Assessment for Registered Banks, Non-Bank Deposit Takers and Life Insurers*. http://bit.ly/2hPOaIa

Notes for DIA reporting entities [2]– provides some direction and basic supervisory expectation to help DIA reporting entities in meeting the minimum requirements of the Act. DIA recommends that reporting entities' AML/CFT compliance officers (compliance officer) be familiar with this document.

Limitations

10. For consistency when comparing sectors, DIA did not consider the adequacy or effectiveness of any ML/TF controls. The Financial Institutions SRA 2019 is an assessment of **inherent** risk across each sector. The SRA does not assess **residual** risk.

11. Inherent risk is the assessed ML/TF risk **before** any controls or mitigation measures have been put in place. Residual risk is the assessed ML/TF risk **after** any controls or mitigation measures have been put in place. Reporting entities are responsible for determining their individual levels of inherent ML/TF risk that they face in the ordinary course of business. Once they have determined their inherent risk, they can then apply their AML/CFT controls and determine their residual ML/TF risk.

12. The Financial Institutions SRA 2019 has drawn on aspects of the FIU's current National Risk Assessment (NRA 2019), historical National Risk Assessments, historical FIU Quarterly Typology Reports, and the existing SRAs of DIA, FMA and RBNZ. In addition, the Financial Institutions SRA uses guidance and reports from other jurisdictions and international organisations such as the Asia Pacific Group (APG) and the FATF, which are inter-governmental bodies developing and promoting policies to combat ML/TF.

13. This document is designed to give Financial Institution entities guidance on AML/CFT and to help them meet their obligations under the Act. The Financial Institutions SRA 2019 works on two distinct levels: it provides an assessment of ML/TF risk, and it identifies key ML/TF vulnerabilities and how they impact each sector. **A risk rating for ML/TF is not an indication of instability or criminality of any business type or reporting entity within the sector.**

[2] http://www.dia.govt.nz/Services-Anti-Money-Laundering-Sector-and-National-Risk-Assessments

Assessment of risk

14. The table below summarises the currently assessed **inherent** ML/TF risk of each sector in comparison to the initial assessments. [3]

Sector – Financial Institutions	Inherent risk of ML/TF 2019	Inherent risk of ML/TF risk 2011	Sector – DNFBPs & Casinos	Inherent risk of ML/TF 2017	Inherent risk of ML/TF 2019
Money remittance	High	High	Trust and company service providers [4]	High	High
Virtual asset service providers	High	n/a[5]	Lawyers	Medium-high	Medium-high
Currency exchange	Medium-high	Medium	Accountants	Medium-high	Medium-high
Payment provider	Medium-high	n/a	Real estate agents	Medium-high	Medium-high
Non-bank non-deposit taking lenders	Medium	Low	High-value dealers	Medium-high	Medium-high
Non-bank credit cards	Medium	Low	Racing Industry Transition Agency	Medium-high	Medium-high
Stored value cards	Medium	n/a	Casinos[6]	Medium-high	Medium-high
Cash transport	Medium	Medium	Conveyancers	Low	Medium
Tax pooling	Low	n/a			
Debt collection	Low	Low			
Factoring	Low	Low			
Financial leasing	Low	Low			
Payroll remittance	Low	Low			
Safe deposit boxes	Low	Medium			

15. **Note:** The categories of Financial Institution sectors have been refined from the first 2011 SRA and are based on current annual report data. The Phase 1 SRA 2018 added the payment provider, tax pooling and stored value cards sectors, and the Financial Institutions 2019 SRA sees the movement of the casinos and TCSPs sectors to the DNFBPs and Casinos SRA, and the addition of a specific category for virtual asset service providers, reflecting newly issued guidance and international understanding of the sector.

[3] The risk ratings are compared with the 2011 Phase 1 SRA ratings (adjusted) and the 2017 Phase 2 SRA risk ratings.

[4] TCSPs were previously included in the 'Phase 1' SRA with financial institutions, they are now part of the DNFBPs and Casinos SRA (previously the 'Phase 2' SRA

[5] VASPs are now a sector separate from payment providers

[6] Casinos were previously included in the 'Phase 1' SRA with financial institutions, they are now part of the DNFBPs and Casinos SRA (previously the 'Phase 2' SRA).

16. ML/TF risk is assessed using a 5×5 risk matrix in line with the DIA Enterprise Risk Management Tool (see Appendix 1). The ratings (high, medium-high, medium and low) are based on supervisory experience, available data, new and existing guidance and structured professional opinion.

17. It is worth emphasising that the inherent risk ratings in both SRAs do not consider risk controls or mitigation measures that are in place in reporting entities or across the sectors. This assessment of **residual** risk is not part of the SRA.

Overall risk rating summary

18. The overall **high** risk rating for the money remittance sector is consistent with the characteristics of the industry in the absence of AML/CFT controls. This is to be expected given the relatively large size of the sector and the number and the types of customers it has. The risk rating reflects the role it plays in facilitating the cross-border movement of funds (including cash) and easy access to high-risk products and services.

19. The overall **medium-high** risk rating for the foreign exchange sector reflects the size of the sector, its ease of access, and its provision of a number of higher risk products and services. This sector has overlaps with the money remittance sector and is vulnerable to a number of ML/TF factors and may present an attractive avenue for ML/TF.

20. The overall **medium-high** risk rating for payment providers reflects the relatively unknown nature and scale of ML/TF vulnerabilities associated with this sector. However, recognised risks exist in relation to anonymity, new technology and products and the potential for cross border movement of funds.

21. The overall **medium** risk rating for non-bank non-deposit taking lenders reflects the large size of the sector, its ease of access and the number and the types of customers. While the sector does have higher risk products and services, these are relatively small in number and represent lower value transactions.

22. The overall **medium** risk rating for the non-bank credit cards sector reflects the smaller size and relatively limited products and services it provides. However, these products and services are widely available, easy to access and vulnerable to a number of high-risk ML/TF activities and industry-specific risk factors. The sector has been highlighted internationally and domestically as being vulnerable to ML/TF activities.

23. The overall **medium** risk rating for the stored value cards sector reflects the smaller size and relatively limited products and services covered by the Act. However, the sector – widely spread and easy to access – is vulnerable to a number of high-risk ML/TF activities and industry-specific risk factors. The sector has been highlighted internationally and domestically as being vulnerable to ML/TF activities.

24. The overall **medium** risk rating for the cash transport sector reflects the intrinsic ML/TF risk around cash, cash intensive businesses and the ability to move large amounts of funds, potentially across borders. However, the risk is slightly offset by the sectors small size and relatively limited products and services.

25. The overall **high** risk rating for the virtual asset service provider sector reflects the myriad vulnerabilities this sub-sector faces. These include ease of access, anonymity and beneficial ownership issues, the role it plays in cross-border payments and prior association with organised crime.

26. The overall **low** risk ratings for the remaining sectors reflect a variety of lower risk factors and vulnerabilities. These include small size, low levels of accessibility, low transactional value, volume and velocity, restricted exposure to higher risk customers and inherent difficulty as a method of ML/TF.

Key vulnerabilities and high-risk factors

27. The Financial Institutions SRA 2019 identifies 10 key ML/TF vulnerabilities and high-risk factors in line with domestic and international experience. Reporting entities should consider these vulnerabilities and high-risk factors **regardless** of the overall ML/TF risk of their business.

28. When considering their own risk assessments, reporting entities should consider the vulnerabilities and high-risk factors and how they impact on their business.

29. The vulnerabilities and high-risk factors presented in the list below are in no particular order, as each sector will prioritise them differently. **DIA strongly recommends that reporting entities are familiar with the vulnerabilities and high-risk factors described in full in Appendix 16.**

Vulnerabilities:

- Cash and liquidity
- Anonymity and complexity
- New payment technology
- Lack of ML/TF awareness

High Risk Factors:

- Trusts, shell companies and other legal arrangements
- International payments
- High-risk customers and jurisdictions
- Politically exposed persons and high net worth individuals
- Gatekeepers
- Money Service Businesses

Predicate offending

30. The term "predicate offence" describes the offences underlying ML/TF activity. Taking direction from overseas experience and the findings of the NRA 2019, it is important that Financial Institution reporting entities are aware of the full range of criminal offending that can lead to ML/TF activity. The NRA 2019 identifies three main domestic predicate offences: drug offending, fraud and fax offending. This is consistent with previous iterations of the NRA, and also identifies that an organised crime structure and/or networked offending are common factors in predicate offending cases.

Domestic and international money laundering threat

31. The FIU estimates that NZ$1.35 billion is generated annually for laundering. This figure excludes transnational laundering of overseas proceeds and laundering the proceeds of domestic tax evasion. The transactional value of ML and the harm caused by ML and predicate offending is likely to be significantly more than this figure.

32. Three key overseas threat areas identified by the FIU are:

- Specific transnational organised crime groups in which the group is linked to New Zealand – offending of this sort is closely associated with overseas-based networks entering the domestic New Zealand drug market with the intention of repatriating illicit profits. This activity drives domestic offending and harm to New Zealand communities by developing the criminal enterprise's links and influence in New Zealand.
- Overseas launderers and terrorism financiers not generally connected to New Zealand who move funds through the global financial system. Any type of overseas criminal may attempt to use jurisdictions with reputations of high integrity and stability to facilitate money laundering or terrorist financing.
- International criminal networks specialising in money laundering services, which have been identified by FATF and other law enforcement agencies as a growing concern. These networks give transnational criminals direct access to the international monetary system and utilise sophisticated ML techniques, such as the use of alternative

remittance, and misuse of complex structures – such as a combination of New Zealand and offshore trusts, companies and charities.

Terrorism financing

33. Given the increasingly important and dynamic nature of TF risk, this topic is covered in a dedicated section of the Financial Institutions SRA ("Part 20: Terrorist and proliferation financing"). Although TF risk is assessed as low in New Zealand, it is important to include guidance on the vulnerabilities and risks associated with the global issue of TF.

Part 1: Introduction

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

34. The Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the Act) was passed in October 2009 and came into full effect on 30 June 2013. The purposes of the Act are:
    - To detect and deter ML and TF
    - To maintain and enhance New Zealand's international reputation by adopting, where appropriate in the New Zealand context, recommendations issued by the FATF[7]
    - To contribute to public confidence in the financial system

35. Under section 131 of the Act, one of the functions of each AML/CFT supervisor is to assess the level of risk of ML/TF across all the reporting entities that it supervises. To meet this responsibility, DIA produced the Phase 2 SRA in 2017. The Phase 2 SRA has been subsequently replaced by the DNFBPs and Casinos SRA 2019.

Purpose of the Financial Institutions SRA 2019

36. This is the third iteration of the SRAs produced by DIA in relation to the ML/TF risks in the financial institution sectors and has the following roles:
    - To help DIA as an AML/CFT supervisor to understand ML/TF risks within its sectors
    - To provide guidance to reporting entities on the risks relevant to their sector and to inform their risk assessments
    - To contribute to the ongoing FIU assessment of ML/TF risks in New Zealand
    - To meet the FATF Recommendations which require countries to adequately assess ML/TF risk and provide effective AML/CFT regulation and supervision

[7] http://www.fatf-gafi.org/

Alignment of SRAs

37. This Financial Institutions SRA uses the same methodology as the DNFBPs SRA. This ensures consistency across the risk assessment and provides all DIA reporting entities with the same level of guidance.

Three levels of risk assessment

38. Three levels of ML/TF risk assessment are undertaken in New Zealand: national, sector, and individual reporting entity.

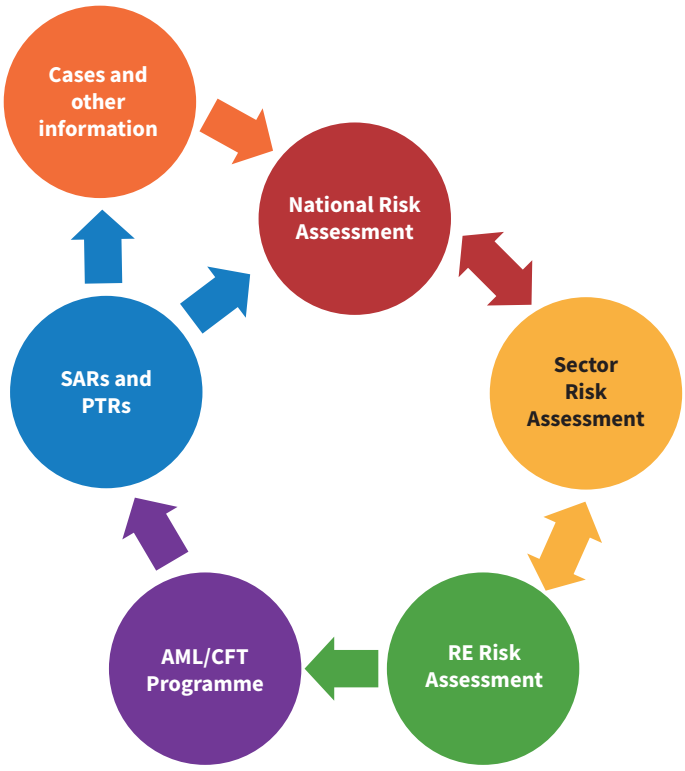
39. National risk assessment (NRA) – The NRA 2019 gives an overview of ML/TF issues affecting New Zealand from a law enforcement perspective. It is informed by a variety of information sources including suspicious activity reports (SARs), and Asset Recovery Unit data. Information from government organisations, both domestic and international, also contributes to this assessment. The FIU develops and maintains indicators of ML/TF and publishes AML/CFT related assessments including the historical Quarterly Typology Reports. DIA recommends that reporting entities and staff with AML/CFT duties refer to the NRA 2019 and the Quarterly Typology Reports[8] to gain a better understanding of ML/TF. The NRA 2019 contains information on how money is laundered and how ML/TF impacts New Zealand. It also identifies the different types of "threats" (domestic and international) and how they exploit ML/TF vulnerabilities.

40. Sector risk assessment (SRA) – The AML/CFT supervisors have each produced a risk assessment for their own sectors. The Financial Institutions SRA 2019 draws on a variety of sources including AML/CFT supervisory experience, domestic and international guidance, FIU risk assessments and reporting entity risk assessments. DIA will conduct ongoing SRA work to continue to improve its understanding of the risks associated with the Financial Institution sectors, and inform reporting entities on risk indicators, trends and emerging issues. The Financial Institutions SRA may be revised regularly or on an ad-hoc basis, depending on how ML/TF risks affect the sectors.

41. Reporting entity risk assessment – 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 have regard to the following:
    - The nature, size and complexity of their business
    - The products and services offered
    - The methods of delivery of these products and services
    - The types of customers they deal with
    - The countries they deal with
    - The institutions they deal with
    - Applicable guidance material produced by AML/CFT supervisors and the FIU
    - Any other factors provided for in regulation

42. DIA encourage reporting entities to access international AML/CFT guidance, in particular the material produced by the FATF, APG and the Australian Transaction Reports and Analysis Centre (AUSTRAC – the organisation responsible for AML/CFT in Australia).

43. The following diagram outlines the inter-relationship of the risk assessment processes and how each informs the other. It shows the flow of SAR and prescribed transaction report (PTR) data to the FIU and the mutually supportive sharing of information between the different types of risk assessment.



[8] http://www.police.govt.nz/advice/businesses-and-organisations/financial-intelligence-unit-fiu/fiu-reports

How reporting entities should use the SRA

44. All reporting entities should read the Executive Summary, Parts 1 to 5 and Part 20. This will help them understand the scope of the Financial Institutions SRA 2019 and its limitations. Each reporting entity must review their sector-specific assessment covering general risks and industry characteristics associated with ML/TF (noting that individual reporting entities will vary from the sector average).

45. The SRA will help reporting entities understand the vulnerabilities and higher-risk areas that DIA has identified within their sector. If reporting entities operate in more than one sector, they must review and have regard to the SRA for each of those sectors.

46. Regardless of the ML/TF risk ratings in the Financial Institutions SRA 2019, when reporting entities assess their own ML/TF risk they should consider what level of risk they are willing to accept, sometimes referred to as their "risk appetite".

47. The AML/CFT Risk Assessment and Programme: Prompts and Notes[9] document has been produced as a companion to the SRA to help reporting entities in meeting the requirements of the Act. These prompts and notes have been designed primarily for DIA-supervised small and medium-sized businesses and to provide direction and supervisory expectation.

48. The guidance contained in the AML/CFT Risk Assessment and Programme: Prompts and Notes for DIA reporting entities is not meant to replace critical thought or proper understanding of the ML/TF risks faced by reporting entities. The prompts and notes are not a "tick box exercise" but rather provide a framework for adequate and effective assessment and mitigation of risk. They do not constitute legal advice. After reading this guidance, if reporting entities still do not understand their obligations they should seek legal advice or contact their AML/CFT supervisor.

[9] http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Anti-Money-Laundering-Sector-and-National-Risk-Assessments?OpenDocument#NOTES

The Financial Institutions SRA 2019 and the SRA Guides

49. The SRA Guides can be read in conjunction with the Financial Institutions SRA 2019, and are intended to update and replace the SRA Guides 2014. The SRA Guides take the relevant sector-specific information from the 2019 SRAs and put them into a smaller, more accessible format. These should be considered by a reporting entity when undertaking its ML/FT Risk Assessment or AML/CFT Programme. However, the Guides are not intended to replace a reporting entity's own risk assessment of its business; nor do they constitute a reporting entity's risk assessment.

The risk-based regime

50. The regime introduced under the Act enables AML/CFT activities to be based on risk. The purpose of a risk-based approach is to make sure AML/CFT measures are proportionate, and that more resources are most effectively targeted towards high-risk and priority areas. It is important to understand that in a risk-based regime not all entities will adopt the same AML/CFT controls. Context is everything and no two reporting entities are the same. Nor does it mean that a single incident of ML/TF invalidates the adequacy or effectiveness of a reporting entity's AML/CFT controls.

51. A risk-based regime recognises that **there can never be a zero-risk situation,** and reporting entities should determine the level of ML/TF exposure they can tolerate. This is not a legislative requirement but may help reporting entities in their risk management.

Stages of money laundering

52. It is worthwhile returning to some of the basics of ML/TF before considering ML/TF risk. ML is generally considered to take place in three phases: placement, layering and integration. TF shares many of the characteristics of ML but may also involve legitimate funds and usually involves smaller amounts.

- **Placement** occurs when criminals introduce proceeds of crime into the financial system. This might be done by breaking up large amounts of cash into smaller sums that are then deposited directly into an account, or by purchasing shares or by loading credit cards. From some offences, such as fraud or tax evasion, placement is likely to occur electronically and may be integral to the predicate offending.
- **Layering** occurs once proceeds of crime are in the financial system. Layering involves a series of conversions or movements of funds to distance or disguise them from their criminal origin. The funds might be channelled through the purchase and sale of investment instruments or be wired through various accounts across the world. In some instances, the launderer might disguise the transfers as payments for goods or services, thus giving them a legitimate appearance.
- **Integration** occurs once enough layers have been created to hide the criminal origin of the proceeds. This stage is the ultimate objective of laundering: funds re-enter the legitimate economy, such as in real estate, high-value assets, or business ventures, allowing criminals to use and benefit from the criminal proceeds of their offending.

Other relevant legislation

53. **Crimes Act 1961** – Essentially, money laundering means concealing or disguising the proceeds of an offence. An "offence" means any offence (or any offence described as a crime) that is punishable under New Zealand law. Refer to section 243 of the Crimes Act for further details.

54. **The Criminal Proceeds (Recovery Act) 2009 (CPRA)** provides for a civil restraint and forfeiture regime. Although this regime was in force at the time of the NRA 2010, data was only available on the initial six months of actions taken under the CPRA. The NRA 2019 findings have drawn on actions since the commencement of the CPRA.

55. **Financial Action Task Force (FATF)** – While not legislation, the FATF 40 Recommendations and 11 Immediate Outcomes represent a global standard of AML/CFT. Compliance with, and effective use of, these standards are an important part of New Zealand's ability to combat ML/TF and its international reputation. New Zealand will be evaluated on these standards and outcomes in 2020.

56. **Anti-Money Laundering and Countering Financing of Terrorism (Exemptions) Regulations 2011** and **Anti-Money Laundering and Countering Financing of Terrorism (Definitions) Regulations 2011** – Supplementary legislation to the AML/CFT Act, these designate relevant thresholds, exemptions and definitions that are important for certain entities, services and sectors.

Part 2: Phase 1 AML/CFT sectors

Nature and size of the Financial Institution sectors

57. Based on the DIA's most recent data[10], there were 1,217 Financial Institution AML/CFT reporting entities carrying out one or more of the financial activities covered by the Act. Most are based in the Auckland region, followed by Canterbury and Wellington. The nature and size of each sector is briefly described below. This is based on the best information available at the time and reflects the fact some reporting entities did not submit an annual report.

58. **Money remitters** – There are 99 money remitters. The sector is diverse and is primarily based in the larger towns and cities with most in the Auckland area. Reporting entities range from large multinational organisations down to small outlets based in local businesses.

59. **Currency exchanges** – There are 31 currency exchangers (also called foreign exchange services) some of which may also offer money remittance services. This number includes hotels offering currency exchange that are covered by the Act.

60. **Payment providers** – There are 54 payment providers. This includes both established means of payments and more recent mobile and internet-based systems such as digital wallets and alternative banking platforms. There are a variety of business models and providers can vary significantly in functionality and structure. However, they fall within the definition of issuing or managing means of payment under the Act. Note: virtual asset exchanges were not caught in the annual report data and are now covered by the section on virtual asset service providers (VASPs) as part of the Financial Institutions SRA.

[10] Data retrieved from internal DIA database on 9/9/2019

61. **Non-bank non-deposit taking lenders (NBNDTLs)** – There are 622 NBNDTLs. A NBNDTL can be defined as a non-bank financial institution that lends to customers but does not take deposits from those applying for funds. Reporting entities range from very small short term low value lenders to large national or international operators.

62. **Non-bank credit cards** – There are 13 non-bank credit card providers. Open-loop cards are typically issued by global associations and can be used at multiple retailers. Closed loop cards are typically used only at a specific retailer that issued the card and are not usually part of an association or global card network.

63. **Stored value cards** – There are six stored value card providers. This sector can include open loop cards (e.g. network branded cards) and closed loop cards (e.g. gift cards) with varying levels of functionality including the ability to use overseas and at ATMs.

64. **Cash transport** – There are seven cash transport providers. The range of services offered is varied and includes cash collection and delivery, ATM collection and maintenance, safe clearance, cash storage and counting and cross border transportation.

65. **Tax pooling** – There are five tax pooling reporting entities. Tax pooling is a financial service which is used by companies operating in New Zealand to help manage their provisional tax needs.

66. **Debt collection** – There are 59 debt collection reporting entities. A debt collection agency will attempt to collect payments from debtors on behalf of their client.

67. **Factoring** – There are 28 factoring reporting entities. 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.

68. **Financial leasing** – There are 38 financial leasing reporting entities. The Act defines businesses that carry out financial leasing activities as a financial institution. However, it excludes financial leasing arrangements in relation to consumer products.

69. **Payroll** – There are 16 payroll reporting entities. The purpose of payroll administration services is to generate payroll information for clients by using timesheets to calculate payments and PAYE deductions. Payroll services 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

70. **Safe deposit boxes** – There are six non-bank safe deposit box providers. If safe deposit boxes are offered by a registered bank these will come under supervision of RBNZ. Safe deposit facilities outside the registered banks are supervised by DIA.

71. **Virtual asset service providers** – There are 11 registered VASPs. DIA has defined a VASP as a business offering one of the following five services: virtual asset exchanges, virtual asset wallet providers, virtual asset broking, initial coin offering providers, and entities offering investment opportunities in virtual assets. DIA also acknowledges that there are further VASPs that are supervised by the FMA – the FMA produces specific guidance that reflects the nature of these businesses. The number of known entities in VASPs sector is expected to expand rapidly as new guidance is issued and additional sector engagement is undertaken by DIA.

Part 3: Methodology

72. The Financial Institutions SRA 2019 works on two levels: it provides an **assessment of ML/TF risk**, and it i**dentifies key ML/TF vulnerabilities**. For a more detailed explanation of the methodology, please refer to Appendix 1.

Methodology – assessment of risk

73. DIA assessed ML/TF risk for each sector using the variables contained in section 58(2)(a)–(f) of the Act and in the Risk Assessment Guideline 2018[11] published by the AML/CFT supervisors in May 2018. The six variables are:
    - Nature, size and complexity of the sector
    - Products/services
    - Methods for delivery of products/services
    - Customer types
    - Country risk
    - Institutions dealt with

74. For each of these variables, DIA considered several ML/TF questions. The responses to these questions helped guide the assessment of inherent risk for each variable. This was done in combination with structured professional knowledge, domestic and international guidance, and input gathered during consultation. At the end of this process, DIA assigned an overall assessment of inherent ML/TF risk to each sector using ratings of low, medium, medium-high or high (see Appendix 2-16).

75. To simplify the SRA process, DIA did not assess residual risk. Reporting entities, as part of their AML/CFT programme, are expected to address the inherent risks identified in their ML/TF risk assessment.

Methodology – identification of key vulnerabilities and high-risk factors

76. For the Financial Institutions SRA 2019 DIA identified four key vulnerabilities and six high-risk factors, which were informed by the NRA and structured professional knowledge (refer part 5). Selection was based on subject matter expertise, supervisory experience, domestic and international guidance and their relative commonality across the sectors.

[11] https://www.dia.govt.nz/Pubforms.nsf/URL/AMLCFT-Risk-Assessment-Guideline-2018.pdf/$file/AMLCFT-Risk-Assessment-Guideline-2018.pdf

Part 4: Predicate offending and SARs

77. Predicate offences are the crimes underlying ML/TF activity and it is important that the various types of predicate offence are understood. The tables below are taken from FIU research.

Domestic threat

Threat	Action	Phase	Description
Drug offending	• Self-laundering • Laundering by close associates • Laundering by professional services and high value dealers (HVDs) • Possible access to international laundering networks	Predicate offending	Cash based
		Placement	Cash deposits, cash purchase of assets, cash remittance, co-mingling with business earnings
		Layering	Domestic transactions, may remit funds internationally, may use trusts, may use professional services – particularly in higher-value cases
		Integration	Real estate, high-value commodities
Fraud	• Self-laundering • Laundering by professional service providers	Predicate offending	Both cash and non-cash based
		Placement	Likely to occur through cash transactions as well as electronic transactions, potentially in the vehicle used to commit predicate offence (e.g. in business, company or market)
		Layering	Use of companies and businesses, likely to be professionally facilitated. Movement of funds offshore through complex networks set up by professional ML facilitators.
		Integration	Real estate, high value commodities
Tax	• Self-laundering • Laundering by professional service providers	Predicate offending	Both cash and non-cash based
		Placement	Likely to occur through electronic transactions, potentially in the vehicle used to commit predicate offence (e.g. in business, company or market)
		Layering	Nominees, trusts, family members or third parties etc. Movement of funds offshore through complex networks set up by professional ML facilitators. Also via gambling and co-mingling with apparently legitimate businesses.
		Integration	Reinvestment in professional businesses, real estate, high-value commodities

International threat

Threat	Description of likely methods
Drug offending connected to New Zealand	• Remittance (particularly informal or 'hawala' arrangements) • Movement of funds through financial institution, DNFBPs, businesses and assets • Trade-based laundering through merchandise trade
Corruption and other economic crime	• Trade-based laundering • Remittance (particularly informal or 'hawala' arrangements) • Attempts to seek safe haven (either in person as fugitives or to store proceeds while maintaining control from offshore)
Organised criminal groups with trans-Tasman connections	• Remittance (particularly informal or 'hawala' arrangements) • Movement of funds through financial institution, DNFBPs, businesses and assets • Trade-based laundering through merchandise trade
Tax evaders and other economic criminals	• Trade-based laundering using trade in services and legal structures
Organised crime and economic criminals with no link to New Zealand	• Use of legal structures and alternative payment platforms
Organised crime	• Remittance (particularly informal or 'hawala' arrangements) • Movement of funds through financial institution, DNFBPs, businesses and assets • Trade-based laundering through merchandise trade
International controllers	• Remittance (particularly informal or 'hawala' arrangements) • Trade-based laundering
Economic criminals	• Abuse of legal structures • Movement of funds through financial institution, DNFBPs, businesses and assets • Attempts to seek safe haven (either in person as fugitives or to store proceeds while maintaining control from offshore)

78. Drug offending generates large amounts of cash and may involve simple ML methods. The greater financial sophistication of fraud offenders can lead to more complex ML, which may make detection more difficult. This is exacerbated by under-reporting by the victims of fraud. Individual criminals are assessed as the greatest generator of proceeds of crime (both of drug crime and fraud) and as being associated with the most sophisticated ML/TF methods.

79. The FIU reports that organised crime groups have access to ML networks that can be sophisticated and hard for law enforcement to combat. They are likely to seek to abuse New Zealand structures to carry out criminal activity, launder proceeds, and act as a conduit to move and layer criminal funds. New Zealand's reputation as a stable, low-risk country is likely to be exploited and degraded by overseas offenders abusing the financial system and New Zealand companies and trusts.

80. The NRA 2019 lists the following factors as the highest priority observed vulnerabilities for New Zealand; international wire transfers, alternative payment methods, new technology, gatekeeper professions (including formation of companies, trusts and charities), cash, businesses and high value goods.

81. Note: The FIU have produced a useful guide for the submission of SARs – *Suspicious Activity Reporting Guideline 2018.*[12] The guideline contains many indicators and warnings, or red flags, of ML/TF activity that reporting entities should consider when assessing ML/TF risk.

[12] http://www.police.govt.nz/sites/default/files/publications/suspicious-activity-reporting-guideline.pdf

Part 5: Key ML/TF vulnerabilities and high-risk factors

Key vulnerabilities

82. The key ML/TF vulnerabilities for Financial Institutions identified below impact in varying degrees on each of the Phase 1 sectors. Reporting entities are encouraged to consider applicable sector vulnerabilities (detailed in Appendix 17) when conducting their risk assessment.

Vulnerability	Comment
Cash and liquidity	Cash continues to be an easy and versatile method of transferring value. This includes the use of money mules, cash couriers and bulk movements. Also, the purchase of high-value goods with cash is an easy method of transferring value and disguising/concealing the proceeds of crime. Cash-intensive businesses, where its use is considered normal, lend themselves to all phases of ML. Customers that use cash or highly liquid commodities (including casino chips) present a significant risk of ML/TF.
New payment technologies	Rapid development of technology may create vulnerabilities that emerge faster than ML/TF controls can respond. For instance, ML/TF via internet and online banking presents a quick, easy and anonymous movement of funds across borders. This vulnerability also includes payment providers, alternative banking platforms and virtual assets.
Anonymity and complexity	Anonymity/complexity can take the form of identity fraud, anonymous products, disguised beneficial ownership or executive control, persons on whose behalf a transaction is conducted, non-face-to-face customer due diligence (CDD), use of intermediaries and abuse of electronic verification.
Lack of ML/TF awareness	Not being able to recognise ML/TF is a significant vulnerability that leaves a reporting entity open to misuse for ML/TF. Reporting entities need to promote an AML/CFT culture and increase and develop their knowledge of the ML/TF environment.

Key high-risk factors

83. The key ML/TF high-risk factors for Financial Institutions identified below impact in varying degrees on each of the sectors. Reporting entities are encouraged to consider applicable high-risk factors (detailed in Appendix 16) when conducting their risk assessment.

High-risk factor	Comment
Trusts, shell companies and other legal arrangements	The use of nominee directors and shareholders, shell companies, limited partnerships, or trusts to create complex legal structures and conceal beneficial ownership are well-recognised ML/TF typologies. New Zealand's open business environment, its registration requirements for financial service providers operating offshore, and the common use of trusts make this activity especially vulnerable to ML/TF. In particular, shell companies and trusts should be considered high risk.
International payments	The value, volume and velocity of money moving through the international payment systems continues to present ML/TF opportunities. Facilitating or receiving international payments, combined with other ML/TF vulnerabilities, presents a high risk of ML/TF.
High-risk customers and jurisdictions	Certain customers are considered high risk – for example, trusts, non-profit organisations and cash-intensive businesses. Criminals may be attracted to certain businesses because they provide access to other facilitators of crime such as transport or high-value commodities. Countries with weak/insufficient AML/CFT measures, high degrees of bribery and corruption, tax evasion, TF, conflict zones and organised crime present a clear ML/TF risk. High-risk customers from high-risk countries compound ML/TF risk.
PEPs and high net worth individuals	This category includes politically exposed persons (PEPs) and their relatives/ close associates, high net worth customers, and people in control of multinational organisations. PEPs, especially in combination with high-risk countries, present a range of ML/TF risks with the potential for far-reaching and serious consequences.
Gatekeepers	The legal, accountancy and real estate sector professionals and businesses, and TCSPs, are known as "gatekeepers". This refers to the role they play in providing services and products that can be used to facilitate the entry of illicit funds into the legitimate financial system. Gatekeepers provide three principal opportunities for criminals; providing an impression of respectability and normality, frustrating detection and investigation of ML/TF and access to specialist services and techniques.
Money Service Businesses	Money service businesses (MSBs), also called money remitters or money or value transfer services (MVTS), are primarily included in the list of high-risk factors as a typology and not as an indication of the industry as a whole. Domestic and international experience, along with FATF guidance, has highlighted this sector as presenting significant ML/TF risk.

84. The following table shows the key ML/TF vulnerabilities and high-risk factors for each Financial Institution sector.

	Cash and liquidity	New payment technology	Anonymity and complexity	Lack of ML/TF awareness	Trusts, shell companies, etc.	International payments	High risk customers / jurisdictions	PE Ps and high wealth individuals	Gatekeepers	Money Service Businesses
Money remittance	Y	Y	Y	Y		Y	Y	Y	Y	Y
Currency exchange	Y	Y	Y	Y		Y	Y		Y	Y
Payment providers		Y	Y	Y		Y				Y
NBNDTLs	Y			Y		Y	Y		Y	
Non-bank credit cards	Y	Y		Y		Y	Y	Y		
Stored value cards	Y	Y		Y		Y	Y			
Cash transport	Y			Y			Y	Y		
Tax pooling			Y	Y	Y		Y	Y	Y	
Debt collection	Y			Y			Y			
Factoring		Y	Y	Y	Y			Y	Y	
Financial leasing		Y	Y	Y	Y				Y	
Payroll remittance		Y	Y	Y						
Safe deposit boxes	Y		Y	Y			Y	Y	Y	
Virtual asset service providers (VASPs)		Y	Y	Y		Y	Y	Y		

85. Key vulnerabilities and high-risk factors **do not operate in isolation** but in combination, resulting in a compounding risk of ML/TF. **Context is essential** in identifying and determining the degree of ML/TF vulnerability and risk. For instance, a reporting entity may be assessed as presenting a low inherent risk of ML/TF as part of its ordinary course of business. However, if it does not have adequate or effective AML/CFT awareness, this vulnerability could leave it open to abuse by not recognising ML/TF activity when it occurs.

86. DIA encourages reporting entities to research their own business-specific vulnerabilities and risks. They must also have regard to current guidance – for example, via DIA newsletters and FIU AML/CFT assessments[13].

[13] http://www.police.govt.nz/advice/businesses-and-organisations/financial-intelligence-unit-fiu/fiu-reports

Part 6: Sector risks – money remittance

Overall inherent risk: high

Both domestic and international evidence and guidance highlight the significant ML/TF risks presented by the money remittance sector[14]. The high-risk services/products of this sector combined with ease of access, wide geographic spread, high-risk customers and the ability to move funds overseas means this sector presents high inherent risk of ML/TF. This sector is assessed as presenting a high ML/TF risk.

87. Money remittance is the transfer of funds between individuals or companies in different locations. Terms used to describe money remittance include money or value transfer services, money service businesses, wire transfer, international money transfer, telegraphic transfer and electronic transfer. The FATF has produced several reports specific to the vulnerabilities of the money remittance sector[15]. The NRA 2019 also highlights the money remittance sector as being highly vulnerable to ML/TF through both international payments and the use of cash (for placement and layering).

88. The money remittance sector ranges from large multi-national providers to small-medium sized business servicing a particular ethnic community and remitting funds to or from a particular country or region. Money remitters carry out these transfers as their core business, but other businesses, including banks, casinos and currency exchanges may also offer money remittance services.

89. Money remitters usually utilise bank accounts to provide their services. However, their international transfers are not normally transacted between countries through a formal banking payment system (such as SWIFT). Rather, it is the money remitter (and not the bank) that controls and has overall visibility of the different parties to the transfer. Payments out to the beneficiary in the destination country may be made by domestic payment from a bank account held or controlled in that country. Or by an agent in that country, or another money remitter that they have a business relationship with or is part of an international network. For inbound remittance to New Zealand, the process works in reverse.

90. Informal or 'hawala' arrangements for the transfer of funds or value are alternative systems of money or value transfer that operate within the money remittance sector. The word 'hawala' originates from the Middle East. In other geographical regions, similar arrangements are sometimes known by other names such as 'hundi' in India or 'fei-chien' in China. In combination however, all these arrangements are commonly referred to as "Informal or 'hawala' systems" of money or value transfer. FATF refer to the providers of such arrangements as "Hawala and other similar service providers" (HOSSPs).

91. There are numerous methods and types of informal or 'hawala' arrangements for money or value transfer. Some of these systems have evolved over many centuries by migrant communities and along trade routes. These systems are usually based on trust and effect transfers of value without the use of the banking system or funds necessarily being relocated. There are other types of informal or 'hawala' arrangements for remittance that do use the banking system and bank accounts. These systems have evolved with the development of the internet and the increased availability of online banking.

[14] http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-money-value-transfer-services.pdf

[15] This includes 'Guidance for a Risk Based Approach – Money or Value Transfer Services (February 2016)', 'Money Laundering through Money Remittance and Currency Exchange Providers (July 2010)' and 'International best practice: Combating the Abuse of Alternative Remittance Systems (June 2003)'.

92. Informal or 'hawala' systems of money remittance are considered to be particularly high risk for ML/TF. Reasons for this include the lack of transparency of transactions when compared to transfers made through formal channels. This may make ML difficult to detect by law enforcement agencies. This makes informal or 'hawala' money remitters particularly attractive to criminals seeking to launder the proceeds of crime. The FATF has produced a report on the vulnerabilities of the informal or 'hawala' remittance sector.[16]

93. Overseas experience has also identified some instances where informal or 'hawala' money remitters have been established, or infiltrated, to serve criminals and circumvent AML/CFT controls. In other instances, informal underground remitters have been set up as part of specialised criminal ML networks managed by offshore international "controllers". The FATF found that these types of networks may be expanding internationally and are a growing concern.

94. Since the Act came into effect a significant number of informal or 'hawala' money remitters in New Zealand have experienced difficulties opening, or maintaining, bank accounts to enable them to transact their money remittance services. This is also consistent with the experience of the money remittance sector in various overseas jurisdictions.

95. DIA is aware that some money remitters in New Zealand have only been able to continue to provide their remittance services by using personal bank accounts in the names of the owner, or family members, or other associated persons. Alternatively, some money remitters have incorporated "shell" companies and opened bank accounts without declaring to the banks that the account will be used to transact a money remittance service. Consistent with overseas jurisdictions, these practices, in which multiple and continually changing bank accounts are used for transacting money remittance services, increase the level of ML/TF risk.

96. DIA recognises that the money remittance sector is diverse with a wide range of business models used by the different reporting entities in the sector. Some of these business models pose a higher ML/TF risk than others. DIA produced a Guide in 2014 for remitters identifying higher and lower risk characteristics associated with the sector.

97. AUSTRAC have also released a ML/TF assessment in relation to the Pacific Islands remittance corridor which may assist reporting entities in their own risk assessments[17].

Nature, size and complexity

98. The DIA currently identifies 99 non-bank reporting entities as providers of money remittance services. This does not include agents of money remitters, which are estimated to be in the hundreds. There is no professional body with oversight for the sector.

99. The money remittance sector consists of a few large multi-national providers who have multiple agents around the country, such as dairies and other small non-financial businesses. There are also some large providers that only provide services online and do not accept cash.

100. The remaining majority of money remitters in the sector are small-medium sized businesses that use informal or 'hawala' systems of money remittance. They predominantly service a specific ethnic community and mostly remit to and from only one particular country or region. For instance, the Chinese community, the Filipino community and the Pacific Islands.

101. The use of multiple and continually changing bank accounts by some money remitters because of banking difficulties adds significant complexity to the overall structure and transparency of the sector.

102. There is also an underground remittance sector consisting of money remitters that are not registered on the Financial Service Providers Register. Underground remitters often utilise informal or 'hawala' arrangements of money or value transfer. Determining the number

[16] https://www.fatf-gafi.org/media/fatf/documents/reports/Role-of-hawala-and-similar-in-ml-tf.pdf

[17] http://www.austrac.gov.au/remittance-corridors-australia-pacific-island-countries

of unregistered remitters and the size of the underground sector is difficult. Unregistered remitters are not likely to maintain adequate records of their customers and transactions and may actively seek to avoid AML/CFT compliance.

Products and services

103. Money remittance services can be used at all three stages of the ML process. The majority of transactions in the money remittance sector involve the transfer of funds between New Zealand and another jurisdiction (whether inbound or outbound).

104. This includes money remittance that is funded in cash. This could be paid to the money remitter directly, or it could be collected at an agent location. Payments out in the destination country may also be in cash or alternatively by transfer into a bank account. Other money remittance business models only accept funds by online bank transfer. In these circumstances, customer on-boarding may be conducted remotely.

Methods of delivery

105. The use of agent locations is a common form of delivering a money remittance service. Some reporting entities also deliver their services, in some cases exclusively, through online and/or mobile channels. This allows customers to engage in a money remittance transaction remotely using online banking via the internet or mobile device without needing to interact with a money remitter, or their agent, face-to-face.

106. Non-face-to-face methods of delivery also include remote on-boarding (potentially including overseas customers) and the use of intermediaries. While non-face-to-face delivery of money remittance services normally avoids the use of cash, there are other significant ML/TF vulnerabilities when compared to face-to-face delivery. Reporting entities should assess the ML/TF vulnerabilities associated with their methods of delivery.

107. Informal or 'hawala' methods of delivery of money remittance are often significantly more complex than remittance provided through more formal channels by multi-national providers or through the formal banking system.

108. To be able to meet their remittance settlement obligations in different countries, it is common for an informal or 'hawala' money remitter to engage another money remitter to source funds in the country they are required. This can include wholesale transactions with a larger money remitter, or even a bank, typically for larger amounts, and involve the funds of various customers bundled together.

109. Other informal or 'hawala' practices may include making or receiving payments to and from each other's customers as well as short term credit arrangements, which are then settled through subsequent transactions. Sometimes, and particularly where money remitters also provide currency exchange services and have surplus cash supplies, cash deposits and exchanges can also occur as part of the remittance settlement process.

110. Where these informal or 'hawala' practices occur, the origin and destination of an individual transfer of funds may often be obfuscated. This is particularly attractive to criminals seeking to launder the proceeds of crime, providing the opportunity for criminally derived and legitimate funds to be co-mingled.

Customer types

111. A large proportion of New Zealand's outbound money remittance customers are from migrant communities or migrant workers sending money to family members in their home countries. This is balanced by inbound remittance being used for investment, migration or to support international students.

112. Money remitters need to know their customers and be aware of the ML/TF risks associated with them. Reporting entities should assess the ML/TF vulnerabilities associated with particular customer types (see Appendix 16: Key ML/TF vulnerabilities and high-risk factors). Access to money remittance services and activities by non-residents (see the "Country risk" section below) is also a factor that can increase the risk of ML/TF if there are no genuine reasons for using their services in New Zealand.

Country risk

113. A countries ML/TF risk is dependent on its levels of bribery and corruption, tax evasion, capital flight, organised crime and if it has sufficient AML/CFT measures.

114. In addition, money remitters should consider whether the country is a conflict zone and if the country is known for the presence of, or support of, terrorism and/or organised people trafficking. Money remitters should consider not only the countries they are remitting funds to or from, but also their neighbouring countries, as ML/TF often involves the movement of funds across borders.

115. In some circumstances, money remittance transactions to or from a country or region may involve several stages, and multiple remittance brokers in multiple countries, known as the "remittance corridor". Money remitters may then need to consider country risk associated with all the various countries involved in delivering a remittance to its destination country.

116. Reporting entities can find information on higher-risk countries from several sources, including the FATF, Transparency International, the United Nations Office on Drugs and Crime (UNODC) and open source media. Reporting entities will need to gain their own level of comfort when assessing jurisdictional risk. Compliance officers will be expected to develop and maintain awareness around this topic and incorporate it into their AML/CFT programme. Reporting entities should refer to the *Countries Assessment Guideline* produced by the AML/CFT supervisors.[18]

Institutions dealt with

117. Most remitters will use bank accounts to transact their money remittance services. Some money remitters will also have business relationships with other money remitters and currency exchanges. Otherwise, most money remitters will have limited exposure to other types of financial institution or DNFBPs.

118. Money remitters may wish to review the SRAs produced by the FMA[19] and RBNZ[20] for additional information on the ML/TF risks when dealing with the financial and banking sector.

119. While informal or 'hawala' remitters may transact a large part of their remittance transfers outside conventional banking channels, there are occasions when settlement or clearing of accounts between money remitters may take place through the formal banking system.

[18] https://www.dia.govt.nz/pubforms.nsf/URL/AMLCFT_CAG_July2012.pdf/$file/AMLCFT_CAG_July2012.pdf

[19] http://bit.ly/2jTH2Pg

[20] http://bit.ly/2hPOaIa

Part 7: Sector Risks – currency exchange

Overall inherent risk: medium-high

Both domestic and international evidence and guidance highlight the significant ML/TF risks presented by the currency exchange sector, especially when overlapped with money remittance services. The services and products of this sector, the ease of access, global spread and the ability to process large cash transactions makes this an inherently medium-high risk sector.

120. Many of the reporting entities recorded as offering currency exchange services also offer remittance (and in some cases lending) services. In addition, some companies offer personal and corporate services. Currency exchange businesses are exposed to a number of inherently high-risk factors and vulnerabilities including the use of cash, prepaid cards and international payments. FATF reports related to currency exchanges are often connected to money remittance.[21] The NRA 2019 also highlights the money remitter sector as being highly vulnerable to ML/TF through international payments.

121. DIA recognises that some currency exchangers may not offer all of the services/products discussed in this section and as a result some generalisations have been made. DIA has produced a guide for currency exchangers providing industry specific higher and lower risk factors.

[21] This includes 'Guidance for a Risk Based Approach – Money or Value Transfer Services (February 2016)', 'Money Laundering through Money Remittance and Currency Exchange Providers (July 2010)'

Nature, size and complexity

122. DIA currently identifies 31 non-bank reporting entities as providers of currency exchange services (also called foreign exchange providers). The currency exchange sector is a complex environment of reporting entities and sub-agents. Some currency exchanges may also offer remittance and lending services which further increases the ML/TF risk presented by the sector.

123. In addition, there are a large number of currency exchange providers that operate as part of New Zealand registered banks and credit unions who come under the supervision of RBNZ. Hotels may also offer currency exchange services.

Products and services

124. Easy access to services to convert currency is attractive to money launderers. Exchanging funds for an easily exchangeable and transportable currency, often at a variety of institutions, allows for funds to be moved into other countries without the scrutiny that may be raised from electronic transactions or wire transfers. Criminals may exchange low value foreign currency notes for higher value denominations that are more easily transportable. This is sometimes referred to as refining.

125. There are a number of high risk products and services provided by currency exchanges which go beyond the changing of one currency to another. These include:

126. **Prepaid travel cards** - The use of prepaid currency or travel cards (e.g. Cash Passport) presents numerous ML/TF risks. These cards can be used by criminals to facilitate the structuring of purchases or reloads under reporting thresholds to avoid detection. In addition, criminals can purchase multiple cards in various currencies to further disguise and conceal the source of funds. Currency cards also facilitate the physical transport of value across borders and make it difficult to determine how much value is on each card without suitable equipment at the border. They also provide cash withdrawal and accessibility to ATMs worldwide. Some currency exchanges offer linked cards which can provide further opportunity for ML/TF activity.

127. **Payment services -** Some currency exchanges offer international payment services which can provide customers the ability to pay bills or mortgages overseas or conduct one-off purchases such as real estate or high value goods.

128. **Services for business** - Some currency exchanges offer business level services and outsourcing functions including foreign exchange operations, wholesale bank note supply and foreign exchange ATM services. These services and products make it easy for customers to move funds and withdraw foreign cash from a wide range of locations and ATMs.

129. **Travellers cheques -** Despite their decline in use traveller's cheques appear in international case studies of ML and are accepted at numerous locations worldwide.

130. **Drafts -** Foreign currency drafts, whilst being uncommon, provide an easy method of removing funds from the country, and depositing them into bank accounts.

Methods of delivery

131. Provision of currency exchange services has traditionally been done face-to-face but there has been an increase in the use of online and phone methods of delivery. For instance, a customer can order currency online and pick it up at a store located at numerous locations. Stored value travel cards can be reloaded online although there are normally restrictions on the amounts and thresholds of the funds involved.

132. Non-face-to-face application for, and delivery of, products/services is regarded as being more vulnerable to ML/TF activity than face-to-face delivery. Reporting entities should assess the ML/TF vulnerabilities associated with the channels of delivery. Non face-to-face channels of delivery may include on-boarding of overseas clients, the use of intermediaries and the use of other professional services/ gatekeepers.

Customer types

133. Currency exchangers will be in contact with domestic customers and international customers and tourists. Depending on the business models adopted by the reporting entity the demographics of the currency exchanger will vary significantly.

134. Currency exchangers need to know their customers and be aware of the ML/TF risks associated with them. Reporting entities should assess the ML/TF vulnerabilities associated with particular customer types (see Appendix 17: Key ML/TF vulnerabilities and high-risk factors). Access to currency exchange services and activities by non-residents (see the "Country risk" section below) is also a factor that can increase the risk of ML/TF if there are no genuine reasons for using their services in New Zealand.

Country risk

135. Country risk comes from dealing with persons, entities or countries in jurisdictions with poor or insufficient AML/CFT measures. Currency exchanges, especially those offering services that facilitate the movement of funds across borders, should also consider the levels of bribery and corruption, tax evasion, capital flight and organised crime activity in a jurisdiction.

136. In addition, currency exchangers should consider whether the country is a conflict zone and if the country is known for the presence of, or support of, terrorism and/or organised people trafficking. They should consider not only the country being dealt with but also their neighbouring countries, as ML/TF often involves the movement of funds across the border.

137. Reporting entities can find information on higher-risk countries from a number of sources, including the FATF, Transparency International, the United Nations Office on Drugs and Crime (UNODC) and open source media. Reporting entities will need to gain their own level of comfort when assessing jurisdictional risk. Compliance officers will be expected to develop and maintain situational awareness around this topic and incorporate it into the AML/CFT Programme. Reporting entities should refer to the *Countries Assessment Guideline* produced by the AML/CFT supervisors.[22]

Institutions dealt with

138. Currency exchangers may have interactions with money remitters and should be aware of the risks and vulnerabilities associated with this sector.

139. Currency exchangers, depending on the services and advice they provide, should consider reviewing the SRAs produced by the FMA[23] and RBNZ[24] for additional information on the risks associated with the financial and banking sector.

Part 8: Sector Risks – payment providers

Overall inherent risk: medium-high

Domestic and international evidence and guidance highlight significant ML/TF risks presented by the payment provider sector, especially in regard to anonymity and the use of new technology. The services and products of this sector, the ease of access, lack of regulation, global reach, international transfer of funds and the ability to process large numbers of high value transactions makes this an inherently medium-high risk sector.

140. The payment providers sector is broad and includes mobile and internet-based payment systems, digital wallets, electronic money and alternative banking platforms. These new payment products and services (NPPS) are developing rapidly and increasing in functionality and use globally, also raising concerns as to whether they allow for customer anonymity. The FATF has published guidance for a risk-based approach for NPPS.[25]

141. This SRA includes a new sector risk assessment that deals with the ML/TF risk associated with virtual asset service providers. These entities were previously considered to be part of the payment providers sector, however in light of developments in this sector and the recent issuance of guidance from international bodies on their regulation, DIA has elected to develop a specific risk assessment. In the New Zealand context, DIA is the lead supervisor for VASPs, however the FMA also holds responsibility for part of the sector based upon the specific services provided and provide risk assessment information designed for these entities. . In addition, the FIU have produced a quarterly typology report on this topic.[26]

142. The problem of regulating and supervising some payment providers is exacerbated by the fact that their services can be carried out from anywhere via the internet and do not require a physical presence in a particular jurisdiction.

[22] https://www.dia.govt.nz/pubforms.nsf/URL/AMLCFT_CAG_July2012.pdf/$file/AMLCFT_CAG_July2012.pdf

[23] http://bit.ly/2jTH2Pg

[24] http://bit.ly/2hPOaIa

[25] 'Guidance for a Risk Based Approach – Prepaid Card, Mobile Payments and Internet based Payment systems (June 2013)'.

[26] http://www.police.govt.nz/sites/default/files/publications/fiu-qtr-q1-2016-17-cryptocurrency.pdf

Such payment providers are therefore able to choose a jurisdiction where they are not subject to regulation and provide their services from there.

143. Further, some payment providers may seek to register on New Zealand's Financial Service Provider Register (FSPR) to present themselves as operating in or from a place of business in New Zealand (when in fact, they are not). This misuse of the FSPR is intended to take advantage of New Zealand's reputation as a high integrity, low risk country and to provide a veneer of respectability for their business. Their FSPR registration credentials may be displayed on their website to incorrectly indicate they are subject to financial regulation in New Zealand. For alternative banking platforms in particular, their websites may provide a disclaimer to ensure they are not breaching New Zealand's banking legislation. For example, *"XYZ Savings & Loans Limited is not a registered bank in New Zealand. We operate as a New Zealand Offshore Finance Company".*

144. As a whole the payment provider sector presents a number of unknowns in terms of ML/TF risk. As DIA knowledge of the sector matures it may be that the assessment of inherent risk will require updating.

Nature, size and complexity

145. DIA currently identifies 54 payment providers. This includes both established means of payments and more recent mobile and internet-based systems such as digital wallets and alternative banking platforms. In addition, there are also a number of businesses registered with the Financial Service Provider Register who are dealing with virtual currency. There are a variety of business models and providers can vary significantly in functionality and structure. However, they fall within the definition of issuing or managing means of payment under the Act. The various types of payment provider (whose products and services often overlap with each other) can be summarised below.

146. **Internet payment systems -** Internet payment services are increasingly interconnected with new and other traditional payment services. Funds can be received, transferred or paid using a variety of payment methods, including cash, money remittance, new payment methods, bank wire transfers and credit cards. Some internet payment system providers issue prepaid cards to their customers, giving them access to cash withdrawal through the worldwide ATM networks facilitating cross-border transactions. Internet based payment services use a variety of business models that include digital wallets, digital currencies, virtual currencies, or electronic money.

147. **Mobile payment services -** Allows non-bank and non-securities account holders to make payments with mobile phones. The nature and operation of mobile payment services vary greatly between business models, and commonly involve new technologies and links with other types of NPPS, which presents challenges for effective AML/CFT regulation.

148. **Pre-funded accounts -** Pre-funded accounts are among the most dominant internet-based payment system. Recipients may or may not be required to register with the payment service provider to receive a funds transfer. Customers may pre-fund an internet-based payment account from a regular bank account. Funds in the internet-based payment account can be used for transfers to other customers of the same provider or can be transferred back to the customer's regular bank account. Pre-funded internet-based payment accounts are often used for online auction payments.

149. Alternative banking platforms: Alternative banking platforms are systems that provide the functionality of a bank but operate outside the traditional global banking space (or regulation). They are also known as payment platforms or virtual banks. The FIU has identified a number of instances where New Zealand Offshore Finance Companies (NZOFCs) have been established using particular New Zealand TCSPs to support the movement of illegal proceeds. Frequently, NZOFCs identified by the FIU use similar criminal methodologies to alternative banking platforms. The FIU have produced a quarterly typology report in regard to alternative banking platforms.[27]

[27] http://www.police.govt.nz/sites/default/files/publications/fiu-qtr-q4-2015-16-alternative-banking-platforms.pdf

Products and services

150. Given the diversity of the payment provider sector it is not possible to identify all the potential products and services they offer. However, some common risks associated with payment providers include:
    - Speed of transaction
    - Difficulty in monitoring transaction activity
    - International movement of funds
    - High value transactions
    - Anonymity
    - Third party funding
    - Insufficient or lack of AML/CFT regulation
    - New technology
    - Non face-to-face delivery of products/ services
    - Use of accounts to pool funds and disguise beneficial ownership
    - Combination with other high-risk products/ services

Methods of delivery

151. Many payment providers rely on non-face-to-face business relationships and transactions.

152. Non face-to-face application for, and delivery of, products/services is regarded as being more vulnerable to ML/TF activity than face-to-face delivery. Reporting entities should assess the ML/TF vulnerabilities associated with the channels of delivery. Non face-to-face channels of delivery may include on-boarding of overseas clients, the use of intermediaries and the use of other professional services/ gatekeepers. Non face-to-face methods of delivery also increase the ML/TF risks associated with customers who are not who they say they are.

153. For payment providers that provide their services online, the ML/FT risks associated with non face-to-face methods of delivery are exacerbated. With a provider located in one jurisdiction but offering its services solely via the internet, and with customers located in numerous different jurisdictions, services can potentially be accessed from anywhere in the world. Across the various types of payment providers, and the various methods they use to transfer or make funds available to or for customers, the sector has global reach and can facilitate cross-border payments with ease.

Customer types

154. Payment providers need to know their customers and be aware of the ML/TF risks associated with them. Reporting entities should assess the ML/TF vulnerabilities associated with particular customer types (see Appendix 16: Key ML/TF vulnerabilities and high-risk factors). Access to payment provider services and activities by non-residents (see the "Country risk" section below) is also a factor that can increase the risk of ML/TF if there are no genuine reasons for using their services in New Zealand.

Country risk

155. Country risk comes from dealing with persons, entities or countries in jurisdictions with poor or insufficient AML/CFT measures. Payment providers, especially those offering services that facilitate the movement of funds across borders, should also consider the levels of bribery and corruption, tax evasion, capital flight and organised crime activity in a jurisdiction.

156. In addition, payment providers should consider whether the country is a conflict zone and if the country is known for the presence of, or support of, terrorism and/or organised people trafficking. They should consider not only the country being dealt with but also their neighbouring countries, as ML/TF often involves the movement of funds across the border.

157. Reporting entities can find information on higher-risk countries from a number of sources, including the FATF, Transparency International, the United Nations Office on Drugs and Crime (UNODC) and open source media. Reporting entities will need to gain their own level of comfort when assessing jurisdictional risk. Compliance officers will be expected to develop and maintain situational awareness around this topic and incorporate it into the AML/CFT Programme. Reporting entities should refer to the *Countries Assessment Guideline* produced by the AML/CFT supervisors.[28]

Institutions dealt with

158. Payment providers may have interactions with money remitters and should be aware of the risks and vulnerabilities associated with this sector.

159. Payment providers, depending on the services and advice they provide, should consider reviewing the SRAs produced by the FMA[29] and RBNZ[30] for additional information on the risks associated with the financial and banking sector.

Part 9: Sector risks – NBNDTLs

Overall inherent risk: medium

The medium risk rating for NBNDTLs recognises that despite having relatively few products, lower value transactions and a domestic customer base the sector does have moderately high levels of transactions by volume. Also, the sector is easily accessed across a wide geographic area and is vulnerable to ML/TF exploitation.

160. New Zealand has a diverse non-bank lending sector - from nationwide lenders to payday loans to micro-lenders to social lending to factoring (refer Part 17). Given the diversity of the sector and the emerging financial technology defining NBNDTLs can be problematic. This is compounded by NBNDTLs not being regulated or represented by a peak body.

161. NBNDTLs generally operate in niche markets that are unattractive to banks. In terms of activity, most NBNDTLs have a predominantly domestic customer base. However, NBNDTLs are exposed to ML/TF risks and high-risk customers and in some instances operate at high volumes and high total values of transactions.

162. DIA recognises that some NBNDTLs may not offer all of the services/products discussed in this section and as a result some generalisations have been made. DIA has produced a guide for NBNDTLs providing industry specific higher and lower risk factors.

[28] https://www.dia.govt.nz/pubforms.nsf/URL/AMLCFT_CAG_July2012.pdf/$file/AMLCFT_CAG_July2012.pdf

[29] http://bit.ly/2jTH2Pg

[30] http://bit.ly/2hPOaIa

Nature, size and complexity

163. A NBNDTL is a non-bank institution that lends to customers but does not take deposits from those applying for funds. Reporting entities range from low value payday loan providers to nationwide lenders. NBNDTLs can be considered as 'third tier' lending institutions. Currently there are 622 NBNDTLs in New Zealand which constitutes DIA's largest Financial Institution sector by number.

164. Social lenders - In addition to the third-tier lending aspect of NBNDTLs, social lending has emerged as a form of financing for parties that may not be eligible for traditional forms of commercial financing. Social lending is used to support community projects or social outcomes. Both recipient and lender are often non-profit organisations. Social lending tends to sit between commercial loans and investment and charitable grants and donations. Social lending generally provides funds where commercial lenders would not.

165. Some social lenders may want to take abnormal lending risks for philanthropic purposes. Some lenders may want to take extreme or illogical risks which may indicate a higher risk of ML.

Products and services

166. Personal and business lending are not often perceived as risky areas for ML/TF but can be exposed to higher risk activities. Criminals can obtain a loan by fraudulent means then pay off the loan with the proceeds of crime making the loan appear legitimate. The funds from the loan may then be used however the criminal wishes.

167. Minimal activity in the NBNDTL business is cash intensive with the majority of repayments made via Direct Debit. Some customers make repayments in-store using cash, but these are typically of 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).

168. Most NBNDTLs do not offer loan facilities to international customers and international transactions are assessed as constituting a very small percentage of total transaction by number and value. Onsite supervisory visits and annual report data suggest international transactions account for only a minimal percentage of the volume and value of transactions in the NBNDTL sector.

169. There is a risk that illicit funds or criminal proceeds may be used for early repayment of a loan funding a legitimate asset purchase. The opportunity for ML in this area usually occurs where loan repayments can be made in cash and the source of funds for large cash payments is unclear.

170. Variations in loan arrangements such as the acceleration of an agreed repayment schedule, either by means of lump sum repayments or early termination without commercial rationale also poses a higher risk of ML.

Methods of delivery

171. Non face-to-face application for, and delivery of, products/services is regarded as being more vulnerable to ML/TF activity than face-to-face delivery. Reporting entities should assess the ML/TF vulnerabilities associated with the methods of delivery.

Customer types

172. There is typically a demand for loans from NBNDTLs from people with low incomes, cash flow problems, existing debt and/or poor credit rating, as well as home owners lacking equity in their homes.[31] Third tier lenders are known to have an 'ease and speed' approach offering same-day loan approval and pay-outs, as well as online and phone applications for loans.[32]

173. NBNDTLs need to know their customers and be aware of the ML/TF risks associated with them. Reporting entities should assess the ML/TF vulnerabilities associated with particular customer types (see Appendix 16: Key ML/TF vulnerabilities and high-risk factors).

[31] 'Third-tier Lender Desk-based Survey 2011, Ministry of Consumer Affairs, July 2011 https://www.mbie.govt.nz/assets/d461101f89/using-a-third-tier-lender-experiences-of-nz-borrowers-2011.pdf

[32] *Ibid.*

174. The domestic customer base for NBNDTLs coupled with low 'value' clientele means identity fraud and structuring methodologies are possible, but the low value customer type do not represent significant consequences in terms of ML. However, in terms of TF this could represent a more significant customer risk, especially in conjunction with high risk jurisdictions.

Country risk

175. A significant proportion of transactions in this sector are domestic payments. Most customers are likely to be New Zealand residents, although some overseas resident customers are to be expected, resulting in overseas payments and pay-outs.

176. Country risk comes from dealing with persons, entities or countries in jurisdictions with poor or insufficient AML/CFT measures. NBNDTLs should also consider the levels of bribery and corruption, tax evasion, capital flight and organised crime activity in a jurisdiction.

177. In addition, NBNDTLs should consider whether the country is a conflict zone and if the country is known for the presence of, or support of, terrorism and/or organised people trafficking. NBNDTLs should consider not only the country being dealt with but also their neighbouring countries, as ML/TF often involves the movement of funds across borders.

178. Reporting entities can find information on higher-risk countries from a number of sources, including the FATF, Transparency International, the United Nations Office on Drugs and Crime (UNODC) and open source media. Reporting entities will need to gain their own level of comfort when assessing jurisdictional risk. Compliance officers will be expected to develop and maintain awareness around this topic and incorporate it into their AML/CFT programme. Reporting entities should refer to the *Countries Assessment Guideline* produced by the AML/CFT supervisors.[33]

Institutions dealt with

179. NBNTLs will have limited exposure to different institutions. They may wish to review the SRAs produced by the FMA[34] and RBNZ[35] for additional information on the ML/TF risks when dealing with the financial and banking sector.

180. Social lending activities differ from other financial lenders; there is no profit seeking on the part of the entity. Not-for-profit social lenders are subject to lower risk in some circumstances than financial lenders where these entities do not accept investment from other sources.

[33] https://www.dia.govt.nz/pubforms.nsf/URL/AMLCFT_CAG_July2012.pdf/$file/AMLCFT_CAG_July2012.pdf

[34] http://bit.ly/2jTH2Pg

[35] .http://bit.ly/2hPOaIa

181. Although wire transfers are generally completed through New Zealand banks or money remittance services, the receipt and payment of funds by wire transfer through NBNDTs is still a risk. Wire transfer transactions on behalf of non-customers also increase ML/TF risk where due diligence has not been undertaken or a profile of expected transactions has not been established.

Part 10: Sector risks – non-bank credit cards

Overall inherent risk: medium

The medium risk rating for non-bank credit cards is consistent with domestic and international guidance. Risks associated with credit cards are cross border transactions, ease of transport, loading with high levels of value, balance payments made in cash and payments made by third parties.

182. Some non-bank credit cards offered within the sector are only accepted at retailers in New Zealand. Several non-bank credit cards are issued by global associations and can be used at multiple retailers. Some non-bank business credit cards have partnerships with banks and credit card companies as well.

183. Credit cards in general are considered higher risk products based on known ML typologies. For instance, the RBNZ Sector Risk Assessment 2017 highlights cards, including credit cards, as a key vulnerability[36]. The NRA 2019 also highlights the risk of placement and layering using non-bank credit cards.

184. DIA recognises that some non-bank credit card providers may not offer all of the services/ products discussed in this section and as a result some generalisations have been made. DIA has produced a guide for non-bank credit cards providing industry specific higher and lower risk factors.

Nature, size and complexity

185. There are 13 non-bank credit card providers. There are two types of non-bank credit cards, open loop and closed loop. Open loop cards 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 are typically used only at a specific retailer that issued the card and are not usually part of an association or global card network.

[36] https://www.rbnz.govt.nz/-/media/ReserveBank/Files/regulation-and-supervision/anti-money-laundering/SRA-2017.pdf?la=en

186. Risk areas include the use of non-bank credit cards to transfer funds overseas and the ability to access cash at a range of ATMs worldwide allowing easy cross border movement of funds with a limited audit trail.

187. Credit cards are vulnerable to structuring or refining of card repayments under reporting thresholds to avoid detection. Some ML/TF indicators associated with credit cards include:
- Balance payments made in cash, particularly large payments, and payments made by third parties
- Structuring or refining of card repayments under reporting thresholds to avoid detection
- Multiple smaller sum payments within a month
- Multiple payments at a range of branches
- Ability to transfer funds overseas (global open loop cards)
- Purchase of valuable assets using non-bank credit cards
- Overpayments on credit limits or available funds
- Cash advances which are then used for wire transfers to high risk jurisdictions
- Overpayment with large amounts of funds and taken overseas and withdrawn from ATMs

188. Some ML/TF risks associated with credit cards include:
- Ability to have multiple authorised users on a single card or multiple cards
- Ability to access cash at a range of ATMs worldwide
- Easy cross border movement with limited audit trail
- Ability to load or overpay credit cards and request refunds
- Ability to have cash advances
- Use in wire transfers

Products and services

189. Open loop cards are typically issued by global associations and can be used at multiple retailers. Closed loop cards are typically used only at a specific retailer that issued the card and are not usually part of an association or global card network.

190. Multiple payments on the same day or at various locations have alerted authorities in other jurisdictions to potential ML. A further method of blurring the origin of funds is for overpayments to be made followed by a request for refunds. Credit cards may be used for cash advances which are then used for bank cheques or wire transfers to high risk jurisdictions.

191. Some non-bank credit cards also offer other services such as international money transfer (through online platforms) and foreign exchange for individuals or business. Refer to the currency exchange section (part 8) for more information.

Methods of delivery

192. The credit card application and approval process may be conducted face-to-face or online.

193. ML/TF risk is present if customers can access non-bank credit cards through indirect methods. Anonymity risks occur when products and services are provided to customers via intermediaries and other methods where the reporting entity does not have face-to-face contact with the customer.

Customer types

194. Non-bank credit card providers need to know all their customers and be aware of the ML/TF risks associated with them. Reporting entities should assess the ML/TF vulnerabilities associated with particular customer types (see Appendix 17: Key ML/TF vulnerabilities and high-risk factors).

195. Access to non-bank credit card services by non-residents (see the "Country risk" section below) is also a factor that can increase the risk of ML/TF if there are no genuine reasons for operating in New Zealand. The use of credit card services and activities by PEPs also heightens ML/TF risk due to their potential exposure to fraud, bribery and corruption. Likewise, high net worth customers pose a higher risk due to the larger amounts they have available to invest and the ease of fund movement through New Zealand facilities.

Country risk

196. Country risk comes from dealing with persons, entities or countries in jurisdictions with poor or insufficient AML/CFT measures. Non-bank credit card providers should also consider the levels of bribery and corruption, tax evasion, capital flight and organised crime activity in a jurisdiction.

197. In addition, non-bank credit card providers should consider whether the country is a conflict zone and if the country is known for the presence of, or support of, terrorism and/or organised people trafficking. Non-bank credit card providers should consider not only the country being dealt with but also their neighbouring countries, as ML/TF often involves the movement of funds across borders.

198. Reporting entities can find information on higher-risk countries from a number of sources, including the FATF, Transparency International, the United Nations Office on Drugs and Crime (UNODC) and open source media. Reporting entities will need to gain their own level of comfort when assessing jurisdictional risk. Compliance officers will be expected to develop and maintain awareness around this topic and incorporate it into their AML/CFT programme. Reporting entities should refer to the *Countries Assessment Guideline* produced by the AML/CFT supervisors.[37]

Institutions

199. Non-bank credit card providers depending on the services and advice they provide should also consider reviewing the SRAs produced by the FMA[38] and RBNZ[39] for additional information on the ML/TF risks when dealing with the financial and banking sector.

[37] https://www.dia.govt.nz/pubforms.nsf/URL/AMLCFT_CAG_July2012.pdf/$file/AMLCFT_CAG_July2012.pdf

[38] http://bit.ly/2jTH2Pg

[39] http://bit.ly/2hPOaIa

Part 11: Sector risks – stored value cards

Overall inherent risk: medium

The use of stored value cards to launder money is a recognised ML/TF typology. Their ease of transport, ability to hold large amounts of value and ability to facilitate the cross-border movement of funds make them vulnerable to criminal exploitation. They are assessed as presenting a medium risk of ML/TF.

200. Stored value cards are a means of payment. However, they differ from other payment providers (refer Part 8: Payment Providers) because there is a physical card held by the user. Stored value cards also differ from non-bank credit cards in that they hold a prepaid balance that is debited rather than extend a level of credit to consumers. A sufficient available prepaid balance must exist on the stored value card at the time of purchase in order for a transaction be authorised.

201. Like other payment providers, stored value cards are recognised as an emerging payment technology. Stored value cards enable the real-time transfer of cash domestically or overseas. In isolation, individual cards pose limited ML risk, but when purchased in bulk they can be used to move large amounts of funds overseas or to transfer value to another individual domestically. The FATF also reported on the ML/TF risk associated with stored value cards as part of new payment methods.[40]

202. Where stored value cards offer the ability to load, or reload, funds from different sources, including third parties, they have an increased risk of use in laundering money. In addition, some stored value cards can be loaded with and provide access to funds in currencies other than the New Zealand dollar. These may be particularly susceptible to ML/TF with illicit funds loaded and sent overseas for a person to use or trade overseas.

[40] http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf

203. DIA recognises that some stored value card providers may not offer all of the services/ products discussed in this section and as a result some generalisations have been made. DIA has produced a guide for stored value cards providing industry specific higher and lower risk factors.

Nature, size and complexity

204. There are six stored value card providers. This sector can include closed loop cards (e.g. gift cards) and open loop cards (e.g. network branded cards).

205. Closed loops cards have a very limited negotiability, such as only being available for use at a particular retail chain and not allowing cash withdrawals. Open loop cards may have significant levels of functionality, including being reloadable, usage overseas, the ability to withdraw cash at ATMs and the functionalities of a payment instrument tied to a payment account. It is not always necessary to have a bank account with an institution offering stored value cards.

206. Open loop stored value cards are now widely used and accepted as a method of making a payment.

207. Some ML/TF risks associated with stored value cards include:
- Ability to have multiple authorised users on a single card or multiple cards
- Ability to access cash at a range of ATMs worldwide
- Easy cross border movement with limited audit trail
- Ability to load or overpay stored value cards and request refunds
- Ability to have cash advances
- Use in wire transfers
- Technical difficulties in identifying and reading a card's stored value
- Purchase of valuable assets using stored value cardsAbility to transfer funds overseas (global open loop cards)
- Structuring or refining of card re-loading under reporting thresholds to avoid detection

208. Some stored value cards can be loaded with and provide access to funds in currencies other than the New Zealand dollar. These cards may be particularly susceptible to being loaded with illicit funds and sent overseas to use or trade. Multiple purchases of cards may be an indicator of this type of activity.

209. Other risks and vulnerabilities include:
- Customers and non-customers accessing foreign exchange pre-paid cards at bank branches
- Persons operating accounts acting on behalf of customers as nominees with multiple persons having access to cards on an account
- Cash passports reloaded with cash in structured amounts to avoid reporting thresholds
- Cash withdrawals made worldwide in a variety of currencies in a structured manner

Products and services

210. Most stored value cards offered within the sector are only accepted at retailers in New Zealand. Several stored value cards are issued by international organisations and can be used at multiple retailers in multiple jurisdictions.

211. At one end of the spectrum are gift cards that can only be used for purchases at a single, or among a limited network, of merchants (commonly referred to as closed-loop prepaid cards). These cards do not allow reloads or withdrawals, do not provide access to the global ATM network, and are not able to have cash refunded through merchants. Although closed loop cards typically have a limited negotiability, the ML risk in closed-loop prepaid cards occurs when used as an intermediary store of value.

212. At the other end of the spectrum are payment network-branded cards that allow transactions with any merchant or service provider participating in the payment network (commonly referred to as open loop stored value cards). Open loop cards can typically serve as an alternative to a variety of traditional banking products and services

213. For the majority of open loop stored value cards, customers use the cards to access related funds which are held in an associated payment account. They offer similar options to those provided by a payment account and related instruments to move funds and may allow cash access via ATMs globally. These stored value cards can be funded using cash and other electronic payment instruments.

214. The global reach of some stored value cards to make payments, access cash and transfer funds are features that make cards attractive for ML purposes. Stored value cards which can be used to access funds internationally are particularly vulnerable due to the logistical benefits of transporting a discreet number of stored value cards loaded with high fund values rather than transporting large, bulky amounts of cash using cash couriers.

Methods of delivery

215. Face-to-face contact with a customer offers some form of tangible business relationship and an opportunity to interact with the customer. Transactions made online, over the phone or via an intermediary reduce this exposure to the customer, decrease effective identification, and increase vulnerability to ML/TF.

Customer types

216. Stored value card providers need to know their customers and be aware of the ML/TF risks associated with them. Reporting entities should assess the ML/TF vulnerabilities associated with particular customer types (see Appendix 17: Key ML/TF vulnerabilities and high-risk factors).

217. Access to stored value provider services by non-residents (see the “Country risk” section below) is a factor that can increase the risk of ML/TF. Use of stored value card services and activities by PEPs also heighten ML/TF risk due to their potential exposure to fraud, bribery and corruption. Likewise, high net worth customers pose a higher risk due to the larger amounts they have available to them and the ease of fund movement through New Zealand facilities.

Country risk

218. Country risk comes from dealing with persons, entities or countries in jurisdictions with poor or insufficient AML/CFT measures. Stored value card providers should also consider the levels of bribery and corruption, tax evasion, capital flight and organised crime activity in a jurisdiction.

219. In addition, stored value card providers should consider whether the country is a conflict zone and if the country is known for the presence of, or support of, terrorism and/or organised people trafficking. Stored value card providers should consider not only the country being dealt with but also their neighbouring countries, as ML/TF often involves the movement of funds across borders.

220. Reporting entities can find information on higher-risk countries from a number of sources, including the FATF, Transparency International, the United Nations Office on Drugs and Crime (UNODC) and open source media. Reporting entities will need to gain their own level of comfort when assessing jurisdictional risk. Compliance officers will be expected to develop and maintain awareness around this topic and incorporate it into their AML/CFT programme. Reporting entities should refer to the *Countries Assessment Guideline* produced by the AML/CFT supervisors.[41]

Institutions

221. Stored value card providers, depending on the services and advice they provide, should consider reviewing the SRAs produced by the FMA[42] and RBNZ[43] for additional information on the ML/TF risks when dealing with the financial and banking sector

Part 12: Sector risks – cash transport

Overall inherent risk: medium

The medium risk rating reflects the cash transport sector's size, accessibility, geographic spread and specialised products and services. ML/TF vulnerability remains around cash, cash intensive businesses and the movement of funds overseas.

222. Cash transport services can be used as a vehicle to transfer illicit funds whilst adding a layer of anonymity. These services can be used in all stages of the ML 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).

223. In addition, the FATF continues to highlight ML/TF through the physical transportation of cash as a key typology.[44]

224. Cash transport providers are required to be compliant with the Private Security Personnel and Private Investigators Act 2010 (the PSPPI Act). 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. This may mitigate some of the risks associated with rogue employees but does not address the issue of the client using cash transport services to launder illicit funds.

[41] https://www.dia.govt.nz/pubforms.nsf/URL/AMLCFT_CAG_July2012.pdf/$file/AMLCFT_CAG_July2012.pdf

[42] http://bit.ly/2jTH2Pg

[43] http://bit.ly/2hPOaIa

[44] http://www.fatf-gafi.org/publications/methodsandtrends/documents/ml-through-physical-transportation-of-cash.html

225. DIA recognises that some cash transport providers may not offer all of the services/products discussed in this section and as a result some generalisations have been made. DIA has produced a guide for cash transport services, providing industry specific higher and lower risk factors.

Nature, size and complexity

226. There are seven cash transport providers whose core business is cash collection and delivery. In addition, cash transport services may include data transport, cash deposit, cross border transportation and float supply and delivery. The use of cash transport services can allow customers to enter money into the financial system via the cash collection service, as well as obscure the trail of dirty money through the transfer and re-enter the financial system through the bank deposit or delivery service.

227. Cash transport providers vary significantly in size. 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. The volume of money flow for the cash transport sector is difficult to quantify. The levels of cash held and transported by the various cash transport providers reporting vary depending on their insurance levels and client contracts.

Products and services

228. The range of services offered is varied and includes cash collection and delivery, ATM collection and maintenance, safe clearance, cash storage and counting, cross border transportation and float supply and delivery.

229. Risks associated with cash transport products and services include the following:
    - Cash transfer (bank deposit or cash delivery) where customers disguise illegal sources of funds by combining them with genuine takings increasing the legitimacy of funds
    - High volumes of cash transported
    - Movement of foreign currency across borders
    - Transactions from private or residential addresses

230. Another potential risk is the use of several separate providers carrying out individual steps of the cash transport transaction. This can disguise and conceal beneficial ownership and the source of funds and hinder potential investigations.

Methods of delivery

231. At the core of this sector is the transportation of cash. Cash is collected and transported in a tamper-proof sealed bag and signed by the client and employee at the time of pick up.

232. The number of vehicles available for transport varies greatly and client contracts may be based on daily, weekly or monthly transactions. Cash transportation services may also be provided for ad-hoc events (for example galas and concerts) as a one-off collection and delivery transaction.

Customer types

233. Most customers and transactions will be domestic and low risk. Cash transport providers need to know their customers and be aware of the ML/TF risks associated with them, in particular cash intensive businesses. Reporting entities should assess the ML/TF vulnerabilities associated with particular customer types (see Appendix 17: Key ML/TF vulnerabilities and high-risk factors).

Country risk

234. Country risk comes from dealing with persons, entities or countries in jurisdictions with poor or insufficient AML/CFT measures. Cash transport providers should also consider the levels of bribery and corruption, tax evasion, capital flight and organised crime activity in a jurisdiction.

235. In addition, cash transport providers should consider whether the country is a conflict zone and if the country is known for the presence of, or support of, terrorism and/or organised people trafficking. Cash transport providers should consider not only the country being dealt with but also their neighbouring countries, as ML/TF often involves the movement of funds across borders.

236. Reporting entities can find information on higher-risk countries from a number of sources, including the FATF, Transparency International, the United Nations Office on Drugs and Crime (UNODC) and open source media. Reporting entities will need to gain their own level of comfort when assessing jurisdictional risk. Compliance officers will be expected to develop and maintain awareness around this topic and incorporate it into their AML/CFT programme. Reporting entities should refer to the *Countries Assessment Guideline* produced by the AML/CFT supervisors.[45]

Institutions

237. Cash transport businesses, depending on the services and advice they provide, should consider reviewing the SRAs produced by the FMA[46] and RBNZ[47] for additional information on the ML/TF risks when dealing with the financial and banking sector. They should also be aware of the risks associated with cash intensive businesses.

[45] https://www.dia.govt.nz/pubforms.nsf/URL/AMLCFT_CAG_July2012.pdf/$file/AMLCFT_CAG_July2012.pdf

[46] http://bit.ly/2jTH2Pg

[47] http://bit.ly/2hPOaIa

Part 13: Sector risks – tax pooling

Overall inherent risk: low

The overall low risk rating for the tax pooling sector reflects the small number of reporting entities and relatively limited products and services covered by the Act. However, the sector is potentially vulnerable to industry-specific risk factors such as using tax pooling to disguise high value ML transactions.

238. Tax pooling is a government approved scheme whereby 'approved intermediaries' operate tax pooling accounts with Inland Revenue. Instead of making payments directly to their account at Inland Revenue, taxpayers can deposit their funds into a tax pooling trust account at Inland Revenue held by trustees. By bringing parties together who have overpaid and underpaid, Inland Revenue approved intermediaries are then able to offset under and overpayments to increase the return on overpayments and reduce Use of Money Interest (UOMI) exposure on underpayments for those taxpayers in the pool. It essentially allows a business to offset any underpayments of provisional tax made with any overpayments within the pool and at a more favourable interest rate than Inland Revenue UOMI rates.

239. Tax pooling can also assist businesses that are not yet members of the pool, by allowing them to buy tax credits where a company or individual has missed their provisional tax or terminal tax due date.

240. Inland Revenue ensures that funds to be transferred out of a tax pool are matched against a known tax debt. This leaves a potential risk area around pooling – the situation where people are putting money through the system for sale or refund, although these transactions are assessed as representing a relatively small proportion of tax pool transactions.

241. DIA have produced a guide for tax pooling providers providing industry specific higher and lower risk factors.

Nature, size and complexity

242. There are five tax pooling reporting entities. Tax pooling is a financial service which is used by New Zealand companies to help manage their provisional tax needs. Tax intermediaries are relatively new to the New Zealand finance sector. They emerged in 2003 to improve tax repayment records.

243. Late payers can use a tax intermediary who has at their disposal pooled tax dollars sold at a rate lower than what Inland Revenue charges and loaned out at a below standard borrowing charges. Although tax pooling is open to anyone in tax arrears, the main buyers of tax are small and medium size businesses facing cash flow problems (for example, contractors or small businesses with seasonal revenue).

Products and services

244. The main services provided by tax pooling intermediaries include pooling, purchasing and financing.

245. **Pooling -** In the pooling scenario, the tax intermediary can offset an overpayment of provisional tax by a client with another taxpayer's underpayment and return a higher rate of interest to the client.

246. **Purchasing** - In the purchasing scenario, a client who has underpaid their instalment of provisional tax would typically have interest to pay as well as late payment penalties from Inland Revenue for not meeting their uplift liabilities. If the client approached a tax pooling intermediary to purchase this tax based at an intermediary's interest rate, the client would have less interest to pay and zero late payment penalties.

247. **Financing -** Where a client is unable to make an upcoming provisional tax payment on time, a client can approach a tax pooling intermediary to finance this payment on its due date. By financing the payment the client would be able to purchase tax paid not at the due date but at a later date when it has sufficient cash flow. This way, a client can avoid late payment penalties from Inland Revenue for not meeting their uplift liabilities.

248. Some ML/TF risks include:
- Customers may deposit money and then seek a refund of funds held in a tax pool account either immediately or after some years
- People transferring money out of a tax pool to cover a tax debt before a return is filed, and the actual liability is less than the tax transferred out and the customer then wants a refund
- People depositing money and then putting it up for sale, particularly after the tax return is filed where the amount for sale is a significant sum

249. The amount of tax which can be purchased for any single transaction is dependent solely on the amount of tax there is available for sale. There is no minimum purchase. Given that tax intermediaries are already regulated by Inland Revenue, their lending requirements are not as stringent as other creditors. For instance, tax finance arrangements made through an intermediary are not subject to credit approvals. The reason for this is that their debt is with the Inland Revenue because the money is paid into the Inland Revenue and therefore if the customer doesn't meet the payment at the end, the lender receives their funds back from the Inland Revenue and it reverts to a debt between to the client and the Inland Revenue.

Methods of delivery

250. Face-to-face contact with a customer offers some form of tangible business relationship and an opportunity to interact with the customer. Services made online, over the phone or via an intermediary reduce this exposure to the customer, decrease effective identification, and increase vulnerability to ML/TF.

Customer types

251. Late payers can use tax pooling services that can provide pooled tax dollars which are sold at a rate lower than IRD and loaned out at below standard borrowing charges. Although tax pooling is open to anyone in tax arrears, the main buyers of tax are small and medium size businesses facing cash flow problems (for example, contractors or small businesses with seasonal revenue). Most customers and transactions will be domestic and low risk. Tax pooling providers need to know their customers and be aware of the ML/TF risks associated with them. Reporting entities should assess the ML/TF vulnerabilities associated with particular customer types (see Appendix 16: Key ML/TF vulnerabilities and high-risk factors).

252. Access to tax poling services by non-residents (see the "Country risk" section below) is also a factor that can increase the risk of ML/TF if there are no genuine reasons for operating in New Zealand. The services and activities by PEPs also heightens ML/TF risk due to their potential exposure to fraud, bribery and corruption. Likewise, high net worth customers pose a higher risk due to the larger amounts they have available to them and the ease of fund movement through New Zealand facilities.

Country risk

253. Country risk comes from dealing with persons, entities or countries in jurisdictions with poor or insufficient AML/CFT measures. Tax pooling providers should also consider the levels of bribery and corruption, tax evasion, capital flight and organised crime activity in a jurisdiction.

254. In addition, tax pooling providers should consider whether the country is a conflict zone and if the country is known for the presence of, or support of, terrorism and/or organised people trafficking. Tax pooling providers should consider not only the country being dealt with but also their neighbouring countries, as ML/TF often involves the movement of funds across borders.

255. Reporting entities can find information on higher-risk countries from a number of sources, including the FATF, Transparency International, the United Nations Office on Drugs and Crime (UNODC) and open source media. Reporting entities will need to gain their own level of comfort when assessing jurisdictional risk. Compliance officers will be expected to develop and maintain awareness around this topic and incorporate it into their AML/CFT programme. Reporting entities should refer to the *Countries Assessment Guideline* produced by the AML/CFT supervisors.[48]

Institutions

256. Tax pooling providers will have limited exposure to the ML/TF risk presented by other institutions. Depending on the services and advice they provide, they should consider reviewing the SRAs produced by the FMA[49] and RBNZ[50] for additional information on the ML/TF risks when dealing with the financial and banking sector.

Part 14: Sector risks – debt collection

Overall inherent risk: low

Debt collection agencies have limited exposure to high-risk products/services, and their interaction with generally lower-risk customers and institutions mean this sector presents a low inherent risk of ML/TF. However, potential exposure to the ML/TF risk presented by cash, cash intensive businesses and organised crime groups remains.

257. 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.

258. DIA recognises that debt collection agencies are not all the same and are largely exempt from the Act. For the purposes of this SRA, some generalisations have been made. DIA has produced a guide for debt collection services providing industry specific higher and lower risk factors.

Nature, size and complexity

259. There are 59 debt collection reporting agency entities of varying sizes and business models.

260. Debt collection agencies are exempt from conducting CDD. In addition, they are reliant on the information provided by their client in relation to debtors and therefore it may be difficult for debt collection agencies to conduct robust CDD on the debtor.

[48] https://www.dia.govt.nz/pubforms.nsf/URL/AMLCFT_CAG_July2012.pdf/$file/AMLCFT_CAG_July2012.pdf

[49] http://bit.ly/2jTH2Pg

[50] http://bit.ly/2hPOaIa

Products and services

261. Laundering money in the debt collection sector would require some form of collusion between the debt collection agency, client and/or debtor.

262. Some debt collection agencies have been connected to organised crime groups which present their own range of ML risks including cash, predicate offending and cross border movement of funds.

Methods of delivery

263. Third-party involvement in carrying out debt collection transactions can present ML/TF risk by disguising and concealing the source of funds and beneficial ownership.

Customer types

264. Most customers and transactions will be domestic and low risk. Despite their exemptions under the Act debt collection agencies will need to be aware of the ML/TF risks associated with their customers, in particular cash intensive businesses. Reporting entities should assess the ML/TF vulnerabilities associated with particular customer types (see Appendix 17: Key ML/TF vulnerabilities and high-risk factors).

Country risk

265. Country risk comes from dealing with persons, entities or countries in jurisdictions with poor or insufficient AML/CFT measures. Debt collection agencies, despite their exemptions, should consider the levels of bribery and corruption, tax evasion, capital flight and organised crime activity in a jurisdiction. Reporting entities should refer to the *Countries Assessment Guideline* produced by the AML/CFT supervisors.[51]

Institutions

266. Debt collection agencies, depending on the services and advice they provide, should consider reviewing the SRAs produced by the FMA[52] and RBNZ[53] for additional information on the ML/TF risks when dealing with financial and banking sector.

Part 15: Sector risks – factoring

Overall inherent risk: low

The lower transaction values, domestic focus and lack of high risk customers and transactions in the sector result in a low risk rating. However, ML through factoring arrangements is a possible typology and should not be discounted. In addition, the role of factoring in trade-based ML needs to be considered.

267. Factoring is a financing method in which a business owner sells accounts receivable at a discount to an invoice finance company (the factor) to raise capital and the factor collects the debt. This involves a contract between an invoice finance company and their client[54] referring to the purchase and sale of accounts receivable invoices at a discount.

268. The factor manages the client's sales ledger and typically provides the credit control and collection services. The factor will then typically advance up to 85% of the invoiced amount. The balance, less charges, is then paid to the client once the debtor makes full payment to the factor.

269. DIA recognises that factors are not all the same and for the purposes of this SRA, some generalisations have been made. DIA has produced a guide for factoring services providing industry specific higher and lower risk factors. The NRA 2019 also highlights the factoring sector as being vulnerable to abuse using international payment via trade-based money laundering, though has also indicated that international payments comprise less than 10 percent of the overall business.

[51] https://www.dia.govt.nz/pubforms.nsf/URL/AMLCFT_CAG_July2012.pdf/$file/AMLCFT_CAG_July2012.pdf

[52] http://bit.ly/2jTH2Pg

[53] http://bit.ly/2hPOaIa

[54] Companies selling their receivables are typically referred to as "clients" or "sellers" (not "borrowers"). The client's customers, who actually owe the money represented by the invoices, are generally known as "account debtors" or "customers".

Nature, size and complexity

270. There are 28 factor reporting entities. Factoring is a complex sub-sector and transactions can be undertaken as either recourse or non-recourse.

271. In a non-recourse transaction, the factor purchases the underlying credit risk associated with each factored invoice. The client therefore incurs no liability to the factor if the account debtor proves financially unable to make payment. In such an event, the factor must either absorb the loss or take direct enforcement action against the account debtor.

272. A recourse transaction, however, allows the factor to make claims against the client in order to recover losses caused by account debtor insolvencies. Recourse factoring agreements generally require the client to repurchase any invoices that remain unpaid after a certain number of days.

Products and services

273. The level of physical cash receipts directly received within the invoice factoring sector is very low, as the majority of debtors will settle outstanding invoices by way of cheque or electronic payment methods.

274. Factoring differs from commercial lending because it involves a transfer of assets rather than a loan of money. In assessing risk, therefore, factors look primarily to the quality of the asset being purchased (i.e. the ability to collect client receivables), rather than to the underlying financial condition of the seller/client. This focus often makes factoring a suitable vehicle for many growing businesses when traditional commercial borrowing proves either impractical or unavailable.

275. The principal ML risks within the factoring sector are payments against invoices where there is no actual movement of goods or services provided. Or alternatively, where the value of goods is overstated to facilitate the laundering of funds. This provides factors with some exposure to exposure to TBML, which is a dynamic and global ML/TF typology. The FATF have produced several documents in relation to TBML.[55]

276. Laundering money 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. The ability to conceal or disguise large value transactions is a potential vulnerability.

277. Factors may also provide other financial services including invoice discounting, credit finance, debt collection or NBNDTL services.

Methods of delivery

278. Face-to-face contact with a customer offers some form of tangible business relationship and an opportunity to interact with the customer. Services made online, over the phone or via an intermediary reduce this exposure to the customer, decrease effective identification, and increase vulnerability to ML/TF.

[55] http://www.fatf-gafi.org/media/fatf/documents/recommendations/BPP%20Trade%20Based%20Money%20Laundering%202012%20COVER.pdf

Customer types

279. Factoring services are predominantly provided to domestic customers but could be provided to international customers. This exposes reporting entities to a wide range of customer and country risk (see below).

280. Factors need to know their customers and be aware of the ML/TF risks associated with them. Reporting entities should assess the ML/TF vulnerabilities associated with particular customer types (see Appendix 17: Key ML/TF vulnerabilities and high-risk factors).

Country risk

281. Country risk comes from dealing with persons, entities or countries in jurisdictions with poor or insufficient AML/CFT measures. Factors should also consider the levels of bribery and corruption, tax evasion, capital flight and organised crime activity in a jurisdiction.

282. In addition, factors should consider whether the country is a conflict zone and if the country is known for the presence of, or support of, terrorism and/or organised people trafficking. Factors should consider not only the country being dealt with but also their neighbouring countries, as ML/TF often involves the movement of funds across borders.

283. Reporting entities can find information on higher-risk countries from a number of sources, including the FATF, Transparency International, the United Nations Office on Drugs and Crime (UNODC) and open source media. Reporting entities will need to gain their own level of comfort when assessing jurisdictional risk. Compliance officers will be expected to develop and maintain awareness around this topic and incorporate it into their AML/CFT programme. Reporting entities should refer to the *Countries Assessment Guideline* produced by the AML/CFT supervisors.[56]

Institutions

284. Factoring providers, depending on the services they provide, should consider reviewing the SRAs produced by the FMA[57] and RBNZ[58] for additional information on the ML/TF risks when dealing with the financial and banking sector.

[56] https://www.dia.govt.nz/pubforms.nsf/URL/AMLCFT_CAG_July2012.pdf/$file/AMLCFT_CAG_July2012.pdf

[57] http://bit.ly/2jTH2Pg

[58] http://bit.ly/2hPOaIa

Part 16: Sector risks – financial leasing

Overall inherent risk: low

The lower transaction values, domestic focus and lack of high risk customers and transactions in the sector result in a low risk rating. However, ML through repayment of leasing arrangements is a possible typology and should not be discounted.

285. Financial leasing involves 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.

286. DIA recognises that financial leasing agencies are not all the same. For the purposes of this SRA, some generalisations have been made. DIA has produced a guide for financial leasing services providing industry specific higher and lower risk factors.

287. 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.

Nature, size and complexity

288. There are 38 financial leasing reporting entities. The Act defines businesses that carry out financial leasing activities as a financial institution but excludes financial leasing arrangements in relation to consumer products.

Products and services

289. Money launderers may consider the use of financial leases as a means to legitimise money by making lease repayments using illicit funds. Most financial leasing services will be paid directly via electronic means (e.g. debit card). Use of cash will be rare.

290. The purchase of valuable assets is a common ML typology. Using a financial lease to transfer ownership of high value assets, such as vehicles and equipment, to lessees over the course of the lease agreement can be considered a typology for ML. However due to the complex and long-term nature of lease agreements it may not be the most efficient technique to launder money.

291. ML/TF red flags 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
    - The use of shell companies to access financial leasing services
    - Problems identifying beneficial owners and complex ownership/organisation structures

Methods of delivery

292. Face-to-face contact with a customer offers some form of tangible business relationship and an opportunity to interact with the customer. Services made online, over the phone or via an intermediary reduce this exposure to the customer, decrease effective identification, and increase vulnerability to ML/TF.

Customer types

293. Financial leasing customers are generally low-risk New Zealand-based companies and associated individuals. However, consideration is required in regard to the ML/TF risk in relation to trusts, shell companies and legal entities associated with PEPs, as well as businesses associated with organised crime groups and high-risk industries. Determining beneficial ownership and executive control of customers also needs attention, as do persons acting on their behalf.

294. Most customers and transactions will be domestic and low risk. Financial leasing providers need to know their customers and be aware of the ML/TF risks associated with them. Reporting entities should assess the ML/TF vulnerabilities associated with particular customer types (see Appendix 17: Key ML/TF vulnerabilities and high-risk factors).

Country risk

295. Country risk comes from dealing with persons, entities or countries in jurisdictions with poor or insufficient AML/CFT measures. Financial leasing providers should also consider the levels of bribery and corruption, tax evasion, capital flight and organised crime activity in a jurisdiction.

296. In addition, financial leasing providers should consider whether the country is a conflict zone and if the country is known for the presence of, or support of, terrorism and/or organised people trafficking. Financial leasing providers should consider not only the country being dealt with but also their neighbouring countries, as ML/TF often involves the movement of funds across borders.

297. Reporting entities can find information on higher-risk countries from a number of sources, including the FATF, Transparency International, the United Nations Office on Drugs and Crime (UNODC) and open source media. Reporting entities will need to gain their own level of comfort when assessing jurisdictional risk. Compliance officers will be expected to develop and maintain awareness around this topic and incorporate it into their AML/CFT programme. Reporting entities should refer to the *Countries Assessment Guideline* produced by the AML/CFT supervisors.[59]

Institutions

298. Financial leasing providers, depending on the services they provide, should consider reviewing the SRAs produced by the FMA[60] and RBNZ[61] for additional information on the ML/TF risks when dealing with the financial and banking sector.

[59] https://www.dia.govt.nz/pubforms.nsf/URL/AMLCFT_CAG_July2012.pdf/$file/AMLCFT_CAG_July2012.pdf

[60] http://bit.ly/2jTH2Pg

[61] http://bit.ly/2hPOaIa

Part 17: Sector risks – payroll remittance

Overall inherent risk: low

The high values and volume of payroll remittance activity exposes the sector to ML/TF vulnerabilities. However, the limited exposure to cash and other high-risk products/services, and interaction with generally lower-risk customers and institutions, mean this sector presents a low inherent risk of ML/TF.

299. Payroll remittance services include payroll administration services and payroll bureau services. However, only companies offering payroll bureau services are covered by the Act.

300. The purpose of payroll administration services is to generate payroll information for clients by using timesheets to calculate payments and PAYE deductions. Payroll bureau services include 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.

301. DIA recognises that payroll remittance providers are not all the same and for the purposes of this SRA, some generalisations have been made. DIA has produced a guide for payroll remittance providers highlighting industry specific higher and lower risk factors.

Nature, size and complexity

302. There are 16 payroll reporting entities providing payroll bureau services. There are two types:
    - Large corporate companies – these companies specialise in payroll remittance services, have a large customer base and in most cases provide software and support.
    - Small and Medium Enterprises (SME) - these businesses provide payroll remittance as a part of the broader 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.

Products and services

303. Payroll bureau services include 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.

304. ML/TF typologies for payroll remittance are limited although the use of ‘ghost’ or ‘phantom’ employees is a possible method to conduct ML.

Methods of delivery

305. Face-to-face contact with a customer offers some form of tangible business relationship and an opportunity to interact with the customer. Services made online, over the phone or via an intermediary reduce this exposure to the customer, decrease effective identification, and increase vulnerability to ML/TF.

Customer types

306. Payroll remittance customers are generally low-risk New Zealand-based companies. However, they need to consider ML/TF risk in relation to trusts, shell companies and legal entities associated with PEPs, as well as businesses associated with organised crime groups and high-risk industries.

307. Payroll remittance providers need to know their customers and be aware of the ML/TF risks associated with them. Reporting entities should assess the ML/TF vulnerabilities associated with particular customer types (see Appendix 17: Key ML/TF vulnerabilities and high-risk factors).

Country risk

308. Country risk comes from dealing with persons, entities or countries in jurisdictions with poor or insufficient AML/CFT measures. Payroll remittance providers should also consider the levels of bribery and corruption, tax evasion, capital flight and organised crime activity in a jurisdiction.

309. In addition, payroll remittance providers should consider whether the country is a conflict zone and if the country is known for the presence of, or support of, terrorism and/or organised people trafficking. Payroll remittance providers should consider not only the country being dealt with but also their neighbouring countries, as ML/TF often involves the movement of funds across borders.

310. Reporting entities can find information on higher-risk countries from a number of sources, including the FATF, Transparency International, the United Nations Office on Drugs and Crime (UNODC) and open source media. Reporting entities will need to gain their own level of comfort when assessing jurisdictional risk. Compliance officers will be expected to develop and maintain awareness around this topic and incorporate it into their AML/CFT programme. Reporting entities should refer to the *Countries Assessment Guideline* produced by the AML/CFT supervisors.[62]

Institutions

311. Payroll remittance providers, depending on the services they provide, should consider reviewing the SRAs produced by the FMA[63] and RBNZ[64] for additional information on the ML/TF risks when dealing with the financial and banking sector.

[62] https://www.dia.govt.nz/pubforms.nsf/URL/AMLCFT_CAG_July2012.pdf/$file/AMLCFT_CAG_July2012.pdf

[63] http://bit.ly/2jTH2Pg

[64] http://bit.ly/2hPOaIa

Part 18: Sector risks – safe deposit boxes

Overall inherent risk: low

Safe deposit box providers have limited exposure to high-risk products/services and generally lower-risk New Zealand customers. It is assessed this sector presents a low inherent risk of ML/TF. However, potential use by criminals (especially exploiting anonymity and the ability to store illicit goods) should not be discounted.

312. Note: If safe deposit boxes are offered by a registered bank these will come under supervision of RBNZ. Safe deposit facilities outside the registered banks are supervised by DIA.

313. Safe deposit boxes have been linked to organised crime group activity. Both New Zealand and overseas media reports describe police raids of safety deposit boxes which have led to the seizure of cash, weapons and drugs.

314. DIA recognises that safe deposit boxes providers are not all the same and for the purposes of this SRA, some generalisations have been made. DIA has produced a guide for safe deposit box services providing industry specific higher and lower risk factors.

Nature, size and complexity

315. There are six vaults in New Zealand offering safe deposit box facilities (outside of registered banks). There is also another company in the process of establishing this service. Based on 2017 annual report data the total number of safe deposit boxes is approximately 11,000.

316. Transaction information for the safe deposit sector is difficult to quantify and safe deposit box providers have strict privacy policies and are not informed of the contents of the boxes. Customers normally rent safe deposit boxes on an annual basis and make one rental payment per year. In terms of access monitoring, customers' access ranges from daily to monthly.

317. Payment for safe deposit boxes is mostly via Direct Credit, Credit Cards, EFTPOS, cheques and cash, although some companies have historically noted that cash payments were minimal.

Products and services

318. ML/TF risks and vulnerabilities associated with safe deposit boxes include:
    - Being used as a tool to store illicit funds as part of the ML process
    - Customers having unlimited access to the vaults during opening hours
    - Providers offering a guarantee of privacy of access and contents
    - Employees unable to obtain information relating to the contents of the boxes
    - Privacy policies restricting companies from obtaining information relating to the contents of safe deposit boxes
    - Potentially inadequate reporting systems to monitor patterns of access by customer or third parties
    - Rogue employees allowing customers access without appropriate identification

Methods of delivery

319. Safe deposit box providers offer their products and services via both face-to-face and non-face-to-face means. Access to the actual safe deposit box will be in person.

Customer types

320. Safe deposit box provider customers are generally New Zealand-based companies and individuals. However, they do need to consider ML/TF risk in relation to PEPs and high net wealth individuals, as well as customers associated with organised crime groups and high-risk industries. Determining beneficial ownership and executive control of customers and persons acting on their behalf may present challenges.

321. Reporting entities should assess the ML/TF vulnerabilities associated with particular customer types (see Appendix 17: Key ML/TF vulnerabilities and high-risk factors).

Country risk

322. Safe deposit box providers operate in New Zealand. However, the global and dynamic international ML/TF risk environment presents some ML/TF vulnerability and should not be discounted entirely.

323. Country risk comes from dealing with persons, entities or countries in jurisdictions with poor or insufficient AML/CFT measures. Safe deposit box providers should also consider the levels of bribery and corruption, tax evasion, capital flight and organised crime activity in a jurisdiction. In addition, they should consider whether the country is a conflict zone and if the country is known for the presence of, or support of, terrorism and/or organised people trafficking. Safe deposit box providers should consider not only the country being dealt with but also their neighbouring countries, as ML/TF often involves the movement of funds across borders.

324. Reporting entities can find information on higher-risk countries from a number of sources, including the FATF, Transparency International, the United Nations Office on Drugs and Crime (UNODC) and open source media. Reporting entities will need to gain their own level of comfort when assessing jurisdictional risk. Compliance officers will be expected to develop and maintain awareness around this topic and incorporate it into their AML/CFT programme. Reporting entities should refer to the *Countries Assessment Guideline* produced by the AML/CFT supervisors.[65]

Institutions

325. Safe deposit box providers, depending on the services they provide, should consider reviewing the SRAs produced by the FMA[66] and RBNZ[67] for additional information on the ML/TF risks when dealing with the financial and banking sector.

[65] https://www.dia.govt.nz/pubforms.nsf/URL/AMLCFT_CAG_July2012.pdf/$file/AMLCFT_CAG_July2012.pdf

[66] http://bit.ly/2jTH2Pg

[67] http://bit.ly/2hPOaIa

Part 19: Sector Risks – virtual asset service providers

The virtual asset service providers (VASPs) Sector Risk Assessment is a new addition to the SRA 2019. VASPs were previously dealt with under the payment provider sector in the SRA 2018. Due to developments in this area and updates to international guidance, the following risk assessment has been prepared in order to specifically deal with risks relevant to the sector.

Overall inherent risk: high

Whilst individual VASPs will have their own level of residual risk determined by the ML/TF risk factors that apply to their specific services and activities and the controls they will put in place to mitigate these risks, both domestic and international evidence and guidance points to risks presented by the VASP sector. The easy access and wide geographic spread of VASP services, coupled with their pseudo-anonymous nature and use in every phase of ML/TF and in many different ML/TF typologies, means this sector presents a high inherent risk of ML/TF.

326. "Virtual Asset Service Provider" is a term that encompasses several different activities and services that an individual business may offer some or all. Consult the Appendix: Types of VASPs at the end of this document for definitions that can assist in determining whether a business should be considered a VASP. Guidance issued by FATF may also assist with definitions of VASPs.

327. In the New Zealand context, VASPs may be supervised by either DIA (at the primary regulator) or the FMA. The supervisor is determined based upon the activities a VASP undertakes. VASPs that are unsure of who their supervisor is should contact the DIA.

328. The FATF has produced guidance related to VASPs[68] and the steps regulators may take to ensure ML/TF risks are mitigated through the adoption of FATF standards[69]. The FATF Standards permit jurisdictions to prohibit certain activities based on risk and scope in that jurisdiction (e.g. casinos, in jurisdictions where gambling is illegal) and, provided the prohibition is enforced, does not require jurisdictions to have measures to regulate those prohibited activities. Some countries may decide to prohibit virtual assets based on their own assessment of risk.[70]

329. The VASP sector ranges from large multi-national providers with extensive customer bases, to small businesses providing broking or consulting services to a core group of individuals.

330. Depending on the characteristics of the transaction, VASPs can face similar risks to the money remittance sector, providers of currency exchange, and payment providers, all of which are considered providers of high-risk products/services.

331. A VASP's risk assessment must have regard to all the risk factors that the VASP as well as its supervisory authorities consider relevant. In the New Zealand context, these factors are detailed in Section 58(2) of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 ('the Act').

Nature, size and complexity

332. The nature of the virtual asset will have a large impact on the overall risk the VASP faces. Whether a virtual asset is centralised or decentralised, and convertible or non-convertible, may change the risk profile significantly. Many of the listed risks are applicable for some virtual assets but not others – i.e. non-convertible virtual assets do not face risks associated with the conversion to other virtual assets, or back to into fiat currency.

[68] http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

[69] https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

[70] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html

333. Decentralised systems are particularly vulnerable to anonymity risks. For example, by design, Bitcoin addresses, which function as accounts, have no names or other customer identification attached, and the system has no central server or service provider. The Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with a real-world identity. A centralised system may mitigate some of these risks, however they should not be considered exempt from them.

334. The size of VASPs can vary, but the technology in most cases will allow for rapid expansion as seen in numerous exchanges following the 'bitcoin boom' of 2017. This could lead to VASPs becoming overwhelmed and unable to complete thorough CDD or transaction monitoring.

335. VASPs should pay particular attention to where their activities intersect with the regulated fiat currencies and the institutions that they interact with in regard to these.

Products and services

336. The services VASPs offer can be used to quickly move funds globally and to facilitate a range of financial activities – from money or value transfer services to securities, commodities or derivatives related activity, among others.

337. Once a virtual asset is held, the asset's value can be layered through exchanges. Crypto-only exchanges allow an individual to purchase multiple currencies, thereby moving between blockchains to obscure their transaction path. For money laundering it is highly likely that an individual will purchase currency with enhanced privacy features.

338. Off-chain transactions provide another avenue to obscure the movement of funds. Off-chain transactions are the transfer of value outside of the blockchain. This can occur through the transfer of virtual assets between personal wallets, physical exchange of paper or hardware wallets, transfer of one cryptocurrency to another within an exchange or through the purchase of cryptocurrency for cash via a peer-to-peer service. In these examples, the transactions stay off-chain until they are transferred or spent outside of the intermediary entity. At this point it will be difficult to determine the true source of funds.

339. Sanctions are another key risk for VASPs. VASPs should be aware that all virtual assets are considered to have the same obligations as fiat currencies and other 'real-world' assets in terms of international sanctions.[71]

Methods of delivery

340. The initial purchase of a virtual asset will usually involve the exchange of fiat currency to virtual asset. The conversion to and from fiat currency is the point where a launderer is most exposed.

341. VASPs should be aware of potential risks involved with fiat payment methods, such as their policy around the acceptance of cash or cheques.

342. Virtual assets can enable non-face-to-face business relationships. This is a risk factor for ML/TF as customers may take advantage of this in order to obfuscate their true identity to avoid sanctions or attention from law enforcement.

343. Virtual asset 'ATMs' or 'Kiosks' present unique risks because they provide or actively facilitate virtual asset activities via a physical terminal. Examples include structuring transactions or failing to collect and retain required customer identification information.

[71] https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs

Customer types

344. Virtual assets have a history of having a high-risk of exposure to criminals and organised crime. Examples of this can include the 'Silk Road' website, Liberty Reserve,[72] unregistered peer-to-peer exchanges, and malware that extorts payment from victims in cryptocurrency.

345. The use of virtual assets to avoid international sanctions is a known risk.[73] As regimes and individuals are cut off from the global financial system, they search for alternatives. This has resulted in some countries and rogue actors trying to turn to digital currencies to offset the impact of economic sanctions. (i.e. Venezuela and the 'Petro', North Korea's 'Lazarus' Hacking Group).

346. The risk of TF is also significant – terrorist organisations and their supporters and sympathisers are also constantly looking for ways to raise and transfer funds without detection or tracking by law enforcement, and the level of anonymity that virtual assets can provide is attractive to them. There are documented cases of organisations such as Hamas and al-Qaeda utilising virtual currencies to raise funds from donors and move money internationally.[74]

347. A potential indicator of suspicion could be a customer who utilises additional enhanced security measures such as encrypted messaging, proxies and VPNs. This customer may be utilising these services to obfuscate their true identity to avoid sanctions or attention from law enforcement.

348. Some potential customers may be the victims of scams involving cryptocurrency. VASPs should be aware of customers stating they need to send money to unlock a computer (ransomware) or pay tax debt, and of customers who have a limited knowledge of virtual assets.

349. VASPs should be aware of risks involving customers who conduct transactions with wallets or virtual assets that have been linked to darknet marketplaces or other illicit activity. Warning signs could include customer transactions being initiated from IP addresses associated with Tor, customer's wallet details appearing on public forums associated with illegal activity, or a transaction that makes use of mixing and tumbling services.

350. VASPs should be aware of risks of customers who may be operating as unregistered or Illicit peer-to-peer exchangers. Warning signs could include customers receiving a series of deposits from disparate sources that, in aggregate, amount to nearly identical aggregate funds transfers to a known virtual currency exchange platform within a short period of time, or the customer's phone number or email address being connected to a known peer-to-peer exchange platform advertising exchange services.

Country risk

351. VASPs should be aware that some countries may decide to prohibit virtual asset activities or VASPs themselves based upon their assessment of risk and national regulatory context, or to support other policy goals. Whilst this is not the case in the New Zealand context, the global nature of virtual assets means New Zealand-based VASPs may have other compliance obligations and burdens depending on the reach of their business. This is particularly relevant for the USA, who have indicated that despite being foreign located, VASPs are likely to have obligations under US Law if their business activity is substantially located there.[75]

[72] http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

[73] https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs

[74] https://home.treasury.gov/news/press-releases/sm687

[75] https://home.treasury.gov/news/press-releases/sm687

352. The use of virtual assets to avoid international sanctions is a known risk. As regimes and individuals are cut off from the global financial system, they search for alternatives. This has resulted in some countries and individuals trying to turn to digital currencies to offset the impact of economic sanctions (i.e. Venezuela and the 'Petro', North Korea's 'Lazarus' Hacking Group).

353. The global reach of virtual assets increases its potential ML/TF risks. Virtual asset systems can be accessed via the Internet (including via mobile phones) and can be used to make cross-border payments and funds transfers.

354. Virtual assets commonly rely on complex infrastructures that involves several entities, often spread across several countries, to transfer funds or execute payments. This segmentation of services means that responsibility for AML/CFT compliance and supervision/enforcement may be unclear. Individuals or entities seeking to launder money may deliberately seek out jurisdictions with weak AML/CFT regimes.

Institutions dealt with

355. VASPs will typically interact with other VASPs to provide their services, particularly in the case of exchanges and wallet providers. VASPs should be aware of the risks involved with their interactions and the risks of the individual institutions they are dealing with.

356. VASPs should be aware of customers who are dealing with institutions known to be from jurisdictions with weak AML/CFT controls.

357. VASPs should pay particular attention to where their activities intersect with the regulated fiat currencies and the institutions that they interact with in regard to these.

Part 20: Terrorism financing issues

358. In the immediate aftermath of the March 2019 Christchurch Terror Attack, the domestic terrorist threat environment in New Zealand was raised to 'high'. It was subsequently lowered to 'medium', where it remains at the time of writing. The NRA 2019 notes that whilst New Zealand is not considered at high-risk for TF, even small-scale financing within New Zealand could have significant impact. In light of this assessment, it is prudent for all DIA reporting entities to consider the vulnerabilities and risk factors associated with TF and the potential red flags that may indicate TF activity. Reporting entities should consider not only high-risk countries but also their neighbouring countries, as TF often involves the movement of funds across borders. Further information is included in Appendix 18 and in the NRA 2019.

359. TF funding covers a wide range of terrorism-related activity, including operational funds, equipment, salaries and family compensation, social services, propaganda, training, travel, recruitment and corruption. **It is not necessary for reporting entities to identify the purpose of TF. Any potential TF-related information must be reported to the FIU as soon as possible. Reporting entities reporting TF activity must ensure it is accurate, timely and treated with urgency and sensitivity.**

360. The FIU has identified three main TF threats in the NRA 2019:

i. Domestic terrorism – given the low level of domestic support for terrorist causes and absence of terrorist networks, it is more likely financiers of domestic terrorism would manifest in New Zealand as isolated disaffected individuals or small groups.

ii. Overseas groups able to inspire support through ideology - Individuals may be inspired to contribute to overseas terrorist groups by travelling to conflict zones, which requires self or third-party funding. Radicalised individuals may also choose to contribute to terrorism by raising and contributing funds.

iii. Well-resourced groups with established networks – This may involve the movement of larger sums of money for terrorism, in particular for or by state-sponsored groups. This may occur through New Zealand vulnerabilities such as legal persons and alternative banking platforms, or New Zealand address services without transactions moving through New Zealand. This form of TF may not have a domestic NZ connection beyond an address or legal entity.

Nature of TF

361. The characteristics of TF can make it difficult to identify. Transactions can be of low value, they may appear as normal patterns of behaviour, and funding can come from legitimate as well as illicit sources. However, the methods used to monitor ML can also be used for TF, as the movement of those funds often relies on similar methods to ML. Internationally the TF process is considered to typically involve three stages:
    - Raising funds (through donations, legitimate wages, selling items, criminal activity)
    - Transferring funds (to a terrorist network, to a neighbouring country for later pick up, to an organisational hub or cell)
    - Using funds (to purchase weapons or bomb-making equipment, for logistics, for compensation to families, for covering living expenses)

362. The risks associated with TF are highly dynamic. As such, reporting entities need to ensure that their CFT measures are current, regularly reviewed and flexible. It is important that reporting entities maintain situational awareness and effective transaction monitoring systems. CFT measures should incorporate dynamic TF risks, as well as the more static risks associated with ML.

363. The value of funds moved through New Zealand connected to TF is likely to be much lower than other forms of illicit capital flows. However, if funds connected to TF were to be associated with New Zealand reporting entities, it would likely have a disproportionate effect on New Zealand's reputation. Outside of the obvious harm caused by TF, any New Zealand reporting entity associated with this activity could see their reputation severely damaged. If their CFT measures were found to be inadequate or ineffective, they could also face civil and even criminal charges.

New Zealand as a conduit for TF

364. One of the potential consequences of transnational ML is that channels may be established that may also be exploited by terrorist financiers. Overseas groups may seek to exploit New Zealand as a source or conduit for funds to capitalise on New Zealand's reputation as being a lower risk jurisdiction for TF. For instance, funds originating in or passing through New Zealand may be less likely to attract suspicion internationally.

365. TF through the Financial Institution sectors could be small-scale and indistinguishable from legitimate transactions. TF could involve structured deposits of cash into bank accounts followed by wire transfers out of New Zealand. It could also involve money remitters sending funds overseas. More complex methods could see New Zealand businesses, professional services, non-profit organisations and charity accounts being used as fronts for sending funds offshore. The NRA 2019 specifically highlights the use of NZ structures as a risk for TF – for example, in 2014 a website associated with Da'esh/Islamic State was reported to have used a New Zealand virtual office address.

TF indicators and warnings

366. ML and TF share many indicators and warnings, or red flags. The following indicators and warnings may help reporting entities in the difficult task of drawing a link between unusual or suspicious activity and TF:
    - International funds transfers to and from high-risk jurisdictions, potentially at multiple branches of the same reporting entity
    - Multiple customers and/or occasional transactions by non-customers conducting international funds transfers to the same beneficiary located in a high-risk jurisdiction
    - A customer transferring funds to multiple beneficiaries in high-risk jurisdictions
    - A customer using incorrect spelling or providing variations on their name when conducting funds transfers to high-risk jurisdictions
    - Large cash deposits and withdrawals to and from non-profit organisation accounts
    - Individuals and/or businesses transferring funds to listed terrorist entities or entities reported in the media as having links to terrorism or TF
    - Funds transfers from the account of a newly established company to a company selling dual-use items (see the "Proliferation and dual-use items" section below)
    - A sudden increase in business/account activity, inconsistent with customer profile
    - Multiple cash deposits into personal account described as "donations" or "contributions to humanitarian aid" or similar terms
    - Multiple customers using the same address/ telephone number to conduct business/ account activity
    - Proscribed entities or entities suspected of terrorism using third-party accounts (e.g. a child's account or a family member's account) to conduct transfers, deposits or withdrawals
    - Use of false identification to establish New Zealand companies
    - Pre-loading credit cards, requesting multiple cards linked to common funds or purchasing cash passports/stored-value cards prior to travel
    - Customers taking out loans and overdrafts with no intention or ability to repay them or using fraudulent documents
    - Customers emptying out bank accounts and savings
    - Customers based in or returning from conflict zones
    - Customers converting small-denomination bank notes into high-denomination notes (especially US dollars, euros or sterling)

Proliferation and dual-use items

367. FATF's AML/CFT recommendations cover not only AML/CFT but also the financing of the proliferation of weapons of mass destruction. There is currently no evidence to suggest that reporting entities in New Zealand are involved in financing proliferation activities. However, included in "proliferation" are dual-use items or technologies, and New Zealand is not immune from abuse in this sector. Although the likelihood of occurrence is very low, the potential consequences, as with TF, could be catastrophic.

368. Dual-use items are also called "strategic" or "controlled goods" and can be used for both peaceful and military aims. Many of these items can be produced, sourced and manufactured in New Zealand. Such items cannot be legally exported from New Zealand without an export licence or permission from the Secretary of Foreign Affairs and Trade. A list of strategic goods is available on the Ministry of Foreign Affairs and Trade website,[76] and a booklet on the topic is available on the Security Intelligence Service website.[77] Appendix 18 contains a FATF-provided table of general dual-use items and proliferation risk factors that reporting entities may encounter.

[76] http://bit.ly/2A1piYg

[77] http://bit.ly/2Bhy8PL

Support Document for Financial Institutions SRA: Appendices

December 2019

Appendix 1: SRA methodology

This appendix outlines the methodology used for the 'Phase 1 SRA 2018'. For sectors which were included in the 2018 document no substantive changes have been made to their risk assessment in this document. The development of the risk assessment for the virtual asset service provider sector followed this same methodology. Consideration was also given to the updated National Risk Assessment.

Concept of risk

1. The Phase 1 SRA 2018 works on two distinct levels: it provides an **assessment of ML/TF risk**, and it **identifies key ML/TF vulnerabilities and high-risk factors** and how they impact each sector. Where there are specific weaknesses or typologies of note, these are also highlighted.

2. This assessment follows the NRA 2018 and FATF guidance, which suggest that ML/TF risk should be assessed as a function of threat, vulnerability and consequence. This assessment uses a range of FATF guidance on risk assessment methodology and draws on specific international advice for assessing risk in the Phase 1 sectors. Threat combined with vulnerability was expressed as likelihood and aligns with existing DIA risk assessment models where risk is a function of likelihood and consequence.

3. The Phase 1 SRA is one of the decision-making tools DIA uses to plan and focus its AML/CFT supervisory activities on the reporting entities that may present the greatest risk. These tools assist DIA to carry out its statutory functions in an effective and efficient manner. This reflects DIA's commitment to a risk-based approach to AML/CFT.

Methodology – assessment of risk

4. DIA assessed ML/TF risk for each sector using a simple model using the risk factors listed in section 58(2)(a)–(f) of the Act and in the Risk Assessment Guideline[1]. The SRA is intended to help reporting entities in their own risk assessment. The risk factors are:
   - Nature, size and complexity of business
   - Products/services
   - Methods of delivery of products/services
   - Customer types
   - Country risk
   - Institutions dealt with

5. DIA posed a number of ML/TF questions for each of these variables. The responses to these questions helped guide the assessment of inherent risk for each variable. This was done in combination with structured professional knowledge and domestic and international guidance.

6. Historically the primary focus of the Phase 1 SRA was likelihood. However, an explicit part of the risk rating process was to consider the consequences for each sector of ML/TF activity based on the potential for harm.

7. Determining consequence can be challenging and it was considered in the following context: nature and size of the sector, potential financial and reputational consequences, and wider criminal and social harms. These judgements were necessarily qualitative in nature due to the wide variance in ML/TF consequence across individual reporting entities.

8. Because DIA did not consider the adequacy or effectiveness of ML/TF controls in the risk rating process, DIA made no judgements as to whether the risks present in a sector are adequately managed or mitigated. Reporting entities may have systems and controls that address some or all the risks discussed in the risk assessment, but the Phase 1 SRA 2018 does not identify or comment on activities undertaken by individual entities within the sectors.

9. Taking all these variables into consideration, an overall assessment of **inherent** ML/TF risk was assigned to each sector using ratings of low, medium, medium-high or high in line with DIA's Enterprise Risk Management Tool. The Enterprise Risk Management Tool assesses risk in terms of "likelihood" (in the Phase 1 SRA 2018 this is a function of threat and vulnerability) and "consequence". DIA determined risk by cross-referencing the assessed likelihood of an event with its assessed consequence in the following matrix.

Likelihood scale	5 Almost certain	11	16	20	23	25
	4 Highly probable	7	12	17	21	24
	3 Possible	4	8	13	18	22
	2 Unlikely	2	5	9	14	19
	1 Improbable	1	3	6	10	15
		1 Minimal	2 Minor	3 Moderate	4 Significant	5 Severe
		Consequence scale				
Risk rating	Low	Medium	Medium-high		High	

10. For the purposes of the SRA, weightings were assigned to the risk variables and each sector's risk rating was scored and aggregated to arrive at a final overall risk rating (see Appendix 2-16). The numbering of the risk ratings assists with prioritisation. For example, if a risk is rated as 'unlikely' with 'minor' consequences (medium-5) this is less of a priority than a risk which is rated as 'possible' with 'moderate' consequences (medium-13).

Methodology – identification of vulnerabilities and high-risk factors

11. As part of the Phase 1 SRA 2018, DIA identified four key ML/TF vulnerabilities and six high-risk factors. The vulnerabilities/risk factors were selected during a series of DIA workshops using subject matter expertise, operational experience and both domestic and international guidance. They were chosen for their impact and commonality across the Phase 1 sectors and were deliberately kept few in number to help reporting entities understand the ML/TF environment in New Zealand. DIA assessed the vulnerabilities and high-risk factors (see Appendix 17 for details) using a Delphi process[2] to ensure inter-rater reliability. DIA then identified key vulnerabilities and high-risk factors for each sector during consultation.

12. This model was combined with supervisory experience, structured professional judgement, annual reports and data from the DIA Entity Risk Model.

13. The vulnerabilities and high-risk factors are based on the knowledge and experience of DIA staff in conjunction with information from the NRA 2018, SRAs from the AML/CFT supervisors in New Zealand, and international guidance from the FATF, APG and comparable jurisdictions (e.g. AUSTRAC, Financial Crimes Enforcement Network, Financial Transactions and Reports Analysis Centre of Canada, Financial Conduct Authority) in addition to other open source media.

Entity Risk Model

14. The purpose of the Entity Risk Model is to assess ML/TF risk across DIA's regulated sector. The Entity Risk Model is refreshed annually, and the results will help inform future SRAs. The Act requires reporting entities to submit AML/CFT annual reports, and the Entity Risk Model uses this quantitative data, combined with insight and information from other partners, to assign inherent risk. The Entity Risk Model is one of the decision-making tools DIA uses to focus AML/CFT supervisory programmes on reporting entities that present the greatest risk.

Consultation with other AML/CFT sector supervisors

15. DIA, as one of the three AML/CFT supervisors, is in regular contact with RBNZ and the FMA. During the production of the Phase 1 SRA 2018, DIA sought formal feedback and input from both these supervisors. This consultation was augmented by monthly National Coordination Committee meetings and fortnightly Supervisors Forum meetings.

Consultation with FIU

16. DIA consulted the FIU during the production of the Phase 1 SRA 2018. Given the key nature of the NRA, communication, feedback, input and the exchange of information between DIA and FIU was comprehensive and robust. This SRA uses FIU research throughout its assessment of ML/TF risk.

Risk appetite and risk-based approach

17. Regardless of the assessed ML/TF risk and vulnerability ratings in the Financial Institutions 2019, when reporting entities assess their own ML/TF risk, they should consider the level of risk they are willing to accept. A risk-based approach recognises that there can never be a zero-risk situation, and reporting entities must determine the level of ML/TF exposure they can tolerate. This is not a legislative requirement but may help reporting entities in their risk management.

Information sources

18. The Phase 1 SRA 2018 drew together information from a number of sources. A list of source documents is included in Appendix 18. DIA also considered other data sources available to the AML/CFT supervisors, including summary SAR data and other information provided by the FIU (including the NRA 2018, historic Quarterly Typology Reports and associated research), as well as industry expertise, knowledge and experience from internal and external resources relevant to the sectors.

Qualitative and quantitative data

19. The Phase 1 SRA 2018 used a combination of qualitative and quantitative data collected and collated from numerous sources of information. The qualitative judgements of AML/CFT professionals and key stakeholders were an essential aspect of the data collection process. Quantitative data included data from SARs (where relevant), the DIA Entity Risk Model (where relevant), Asset Recovery Unit data and criminal justice statistics. Data collection methods included expert assessments through structured questions, interviews, workshops and other assessment tools. This is in line with FATF, International Monetary Fund (IMF), World Bank, and Organization for Security and Co-operation in Europe (OSCE) methodologies.

Baseline monitoring –annual report data

20. The annual report is required by section 60 of the AML/CFT Act. The annual report applies to activities that are covered by the Act. Reporting entities need to provide details on revenue associated with products or services that are covered by the AML/CFT Act during the reporting period. Annual report data informs the DIA Entity Risk Model.

21. The information in the annual reports helps DIA, in its role as AML/CFT supervisor to get to know reporting entities better and understand the ML/TF risks they face. This helps DIA to better target resources to areas of highest risk. The process of filling in the annual report also assists reporting entities in identifying any changes to their business, and where they might need to revise their ML/TF risk assessment and AML/CFT programme. DIA recognise that annual reports may hold commercially sensitive information and treat them confidentially.

Limitations

22. The Phase 1 SRA 2018 process had the following limitations:
    - Information on ML/TF in some of the Phase 1 sectors is limited
    - Phase 1 reporting entities have various degrees of understanding of AML/CFT legislation and procedures
    - Phase 1 reporting entities have various degrees of understanding of the ML/TF risks in their business, therefore the perception of ML/TF may not be fully developed in a reporting entity's ML/TF risk assessment or AML/CFT programme
    - There is insufficient data and information to inform some risk areas

Appendix 2: Money Remittance

Variable	Assessed risk	Rationale
Nature, size and complexity of business	High	The use of agents, most of whom are not reporting entities, extends the size and complexity of the sector significantly. There are further ML/TF risks associated with the increasing use of non-face-to-face remittance systems, the practices used by some informal or 'hawala' money remitters and the difficulties faced by some money remitters in opening or maintaining bank accounts. There is also an underground remittance sector comprising of businesses providing money remittances services that are not registered on the Financial Service Providers Register. The size of the underground sector is unknown.
Products/services	High	The money remittance sector facilitates international payments of value, often in volume and with velocity. It is exposed to a number of risks and vulnerabilities including cash, currency exchange and high-risk jurisdictions.
Methods of delivery of products/services	Medium-high	Money remittance providers offer their products and services both via face-to-face and non face-to-face means. Advances in the use of the internet and online banking also pose ML/TF risk. The settlement methods used by informal or 'hawala' money remitters, sometimes involving multiple money remitters in combination and aggregating customer funds, may obfuscate the visibility of the origin and destination of a transfer of funds.
Customer types	Medium-high	Many money remittance customers are lower-risk New Zealand-based individuals. However, ML/TF risk in relation to trusts, shell companies, PEPs, criminals, organised crime groups and high-risk occupations needs to be considered.
Country risk	Medium-high	While one party to a money remittance transaction is usually New Zealand-based, the other party is an overseas jurisdiction (which may pose ML/TF risk). An increasing and dynamic international environment presents ML/TF vulnerabilities.
Institutions dealt with	Medium	As well as banks, some money remitters have exposure to dealing with institutions identified as presenting ML/TF risk such as other money remitters and currency exchanges.
Overall inherent risk	High	Both domestic and international evidence and guidance indicate significant ML/TF risks presented by the money remittance sector. The easy access and wide geographic spread of their services, use in every stage of ML/TF and presence in a number of ML/TF typologies, means this sector presents a high inherent risk of ML/TF.

Appendix 3: Currency exchange

Variable	Assessed risk	Rationale
Nature, size and complexity of business	Medium-high	The currency exchange sector is a complex environment; from large international organisations to niche local providers. Access to currency exchanges (also called foreign exchange providers) is easy but geographically concentrated. Businesses may also offer money remittance services. In addition, some hotels also offer currency exchange services.
Products/services	High	The use of foreign exchange and prepaid currency cards present the highest risk for currency exchange services. The accessibility and anonymity associated with these products make them an attractive placement tool for launderers. Bank drafts and traveller's cheques can be considered lower risk. Some currency exchange providers offer other services that include money remittance.
Methods of delivery of products/services	Medium-high	Currency exchanges mostly offer their products and services face-to-face, though non-face-to-face means are increasing. Advances in the use of the internet also pose ML/TF risk.
Customer types	Medium	Currency exchange customers are generally lower-risk New Zealand-based individuals. However, ML/TF risk in relation to trusts, shell companies, PEPs, criminals, organised crime groups and high-risk occupations needs to be considered.
Country risk	Medium	The currency exchange sector is predominantly New Zealand-based but is also exposed to higher-risk jurisdictions. An increasing and dynamic international ML/TF risk environment presents ML/TF vulnerabilities.
Institutions dealt with	Medium	Currency exchange businesses have exposure to dealing with institutions identified as presenting ML/TF risk such as money remitters and banks.
Overall inherent risk	Medium-high	Both domestic and international evidence and guidance highlight the significant ML/TF risks presented by the currency exchange sector, especially when overlapped with money remittance functions. The high-risk services/products of this sector combined with ease of access, global spread and the ability to process large cash transactions means this an inherently medium-high risk sector.

Appendix 4: Payment Provider

Variable	Assessed risk	Rationale
Nature, size and complexity of business	Medium-high	The payment providers sector is broad and includes mobile and internet-based payment systems, digital wallets and alternative banking platforms. The problem of regulating and supervising some payment providers is exacerbated by the fact that their services often require no physical presence in a jurisdiction but can be carried out from anywhere via the internet.
Products/services	Medium-high	New payment products and services are developing rapidly and increasing in functionality and use globally. Some common risks associated include: speed of transaction, difficulty in monitoring transaction activity, international movement of funds, anonymity, third party funding and insufficient AML/CFT regulation.
Methods of delivery of products/services	Medium	Payment providers predominantly offer their products and services by non-face-to-face means. Advances in the use of the internet pose ML/TF risk.
Customer types	Medium	Payment provider customers are generally lower-risk New Zealand-based companies and individuals. However, they need to consider ML/TF risk in relation to PEPs, organised crime groups and high-risk occupations.
Country risk	Medium	Payment providers can be used to transfer funds overseas and in the purchase of valuable assets. An increasing and dynamic international ML/TF risk environment presents ML/TF vulnerabilities.
Institutions dealt with	Medium	Payment providers have exposure to institutions identified as presenting ML/TF risk such as money remitters and currency exchanges.
Overall inherent risk	Medium- high	ML/TF risks presented by the payment provider sector include anonymity, use of new technology, the ease of access, lack of regulation, global reach, international transfer of funds and the ability to process large numbers of high value transactions. It is assessed this is an inherently medium-high risk sector.

Appendix 5: NBNDTLs

Variable	Assessed risk	Rationale
Nature, size and complexity of business	Medium	NBNDTLs range from very small low value lenders to nationwide providers. NBNDTLs can be considered as 'third tier' lending institutions. Social lenders are part of the social finance market where organisations offer loans in addition to grants.
Products/services	Medium - high	Personal and business lending can be exposed to higher risk ML/TF activities. Criminals can obtain a loan by fraudulent means then pay off the loan with the proceeds of crime making the loan appear legitimate. The funds from the loan may then be used however the criminal wishes. Providing funds for lending purposes also present risk.
Methods of delivery of products/services	Medium	Non-face-to-face application for, and delivery of, products/services is regarded as being more vulnerable to ML/TF activity than face-to-face delivery. Reporting entities should assess the ML/TF vulnerabilities associated with the methods of delivery.
Customer types	Low	There is typically a demand for loans from NBNDTLs from domestic customers with low incomes, cash flow problems, existing debt and/or poor credit rating, as well as home owners lacking equity in their homes. The sector focuses on domestic customers.
Country risk	Low	The NBNDTL sector is predominantly New Zealand-based but may be exposed to higher-risk jurisdictions, especially online. An increasing and dynamic international ML/TF risk environment presents ML/TF vulnerabilities.
Institutions dealt with	Low	Although wire transfers are generally completed through New Zealand banks or money remittance services, the receipt and payment of funds by wire transfer through NBNDTLs is still a risk.
Overall inherent risk	Medium	The medium risk rating for NBNDTLs recognises that despite having relatively few products, lower value transactions and a domestic customer base the sector does have moderately high levels of transactions by volume, is easily accessed across a wide geographic area and is vulnerable to ML/TF exploitation.

Appendix 6: Non-Bank Credit Cards

Variable	Assessed risk	Rationale
Nature, size and complexity of business	Medium	There are two types of non-bank credit cards, open loop and closed loop. Several of DIA's reporting entities in the non-bank credit card sector are issued by global associations and can be used at multiple retailers or to withdraw cash from ATMs.
Products/services	Medium-high	Non-bank credit cards present a number of ML/TF risks including cash loading, transfer of funds across border and the purchase of high value goods. Products and services may be accessed worldwide. Persons operating accounts can be acting on behalf of customers as nominees with multiple persons having access to cards on an account. This also provides anonymity. Some non-bank credit cards also offer other services such as international money transfer (through online platforms) and foreign exchange for individuals or business.
Methods of delivery of products/services	Medium	Non-bank credit card products and services can be accessed both via face-to-face and non-face-to-face means. Online access to a variety of functions presents ML/TF risk.
Customer types	Medium	Non-bank credit card customers are generally lower-risk New Zealand-based companies and individuals. However, providers need to consider ML/TF risk in relation to trusts, shell companies and PEPs as well as exposure to criminals and high-risk occupations.
Country risk	Medium	Non-bank credit cards can be used to transfer funds overseas via open loop global card networks and can be used overseas with cash withdrawal options and in the purchase of valuable assets. An increasing and dynamic international ML/TF risk environment presents ML/TF vulnerabilities.
Institutions dealt with	Medium	Non-bank credit card providers have exposure to dealing with institutions identified as presenting ML/TF risk such as banks.
Overall inherent risk	Medium	Non-bank credit cards present a medium ML/TF risk. The higher risk products and services offered by this sector are limited in number but can involve cross border movement of funds.

Appendix 7: Stored Value Cards

Variable	Assessed risk	Rationale
Nature, size and complexity of business	Medium- high	This sector includes prepaid gift cards, cards such as iTunes or Google Play cards and foreign currency cards/ cash passports. Access is easy and wide spread
Products/services	Medium-high	Stored value cards include closed loop cards with only limited negotiability, such as only being available for use at a particular retail chain and not allowing cash withdrawals. However, they also include open loop cards with significant levels of functionality, including being reloadable, usage overseas, the ability to withdraw cash at ATMs and the functionalities of a payment instrument tied to a payment account.
Methods of delivery of products/services	Medium	Stored value card products and services can be accessed both via face-to-face and non-face-to-face means. Stored value cards may be reloaded in structured amounts to avoid reporting thresholds. Likewise, cash withdrawals can be made worldwide in a variety of currencies in a structured manner.
Customer types	Low	Customers are generally low-risk New Zealand-based companies and individuals. Customers and non-customers can access stored value cards at banks and other non-bank distribution outlets.
Country risk	Medium	Some stored value cards can be loaded with and provide access to funds in currencies other than the NZ dollar. These may be particularly susceptible to being loaded with illicit funds and carried/sent overseas to use or trade. Multiple purchases of cards may be an indicator of this type of activity.
Institutions dealt with	Medium	It is not always necessary to have a business relationship with an institution offering stored value cards. Stored value card providers may have exposure to dealing with institutions identified as presenting ML/TF risk such as banks and currency exchanges.
Overall inherent risk	Medium	Use of stored value cards for ML/TF purposes is a recognised typology, both domestically and internationally. The ease of use, access and transport of large amounts of funds (especially across borders) mean this sector presents a medium ML/TF risk.

Appendix 8: Cash Transport

Variable	Assessed risk	Rationale
Nature, size and complexity of business	Medium	The cash transport sector (including cash storage) in New Zealand is small but 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 illicit funds through the transfer (Layering) and re-enter the financial system through the bank deposit or delivery service (Integration).
Products/services	Medium-high	The high volumes of cash being transported and (in some cases) an inability to establish source of funds make this sector vulnerable to ML. Customers can easily combine illicit funds with genuine takings in order to disguise their origin and increase their legitimacy.
Methods of delivery of products/services	Medium	The quantities of cash held and transported by cash transport companies vary depending on their insurance levels, capacity and individual client contracts. Interactions with customers can be face-to-face or online.
Customer types	Low	Cash transport business customers are generally low-risk New Zealand-based companies. However, they need to consider ML/TF risk in relation to trusts, shell companies and legal entities associated with PEPs, as well as customers associated with organised crime groups and high-risk industries.
Country risk	Low	Cash transport businesses primarily operate in New Zealand. However, the global and dynamic international ML/TF risk environment does present some ML/TF vulnerability when they are used to move cash overseas.
Institutions dealt with	Medium	Cash transport companies will have dealings with cash intensive businesses and the banking sector. Banks remain the primary avenue for ML/TF providing a high degree of value, volume and velocity for processing and moving illicit funds.
Overall inherent risk	Medium	Cash transport businesses have limited exposure to most high-risk products/services. However, the intrinsic ML/TF risk around cash, cash intensive businesses and the ability to move large amounts of funds, potentially across borders, needs to be taken into consideration. Interactions with generally lower-risk customers and institutions mean this sector presents a medium inherent risk of ML/TF.

Appendix 9: Tax Pooling

Variable	Assessed risk	Rationale
Nature, size and complexity of business	Low	There are a small number of tax pooling providers in New Zealand offering a very specific range of services. The specialised nature of this field reduces the exposure to ML/TF vulnerability.
Products/services	Low	Tax pooling provides a very specific and low risk service. However, there is potential to use this service to move significant amount of funds for ML purposes.
Methods of delivery of products/services	Low	Tax pooling providers offer their products and services via both face-to-face and non-face-to-face means.
Customer types	Low	Tax pooling provider customers are generally low-risk New Zealand-based companies and individuals. However, they need to consider ML/TF risk in relation to trusts, shell companies and legal entities associated with PEPs, as well as businesses associated with high-risk industries.
Country risk	Low	Tax pooling providers operate in New Zealand. However, the global and dynamic international ML/TF risk environment does present some ML/TF vulnerability.
Institutions dealt with	Low	Tax pooling providers have limited exposure to dealing with institutions identified as presenting ML/TF risk. However, there may be ML/TF risk present when dealing with banks and gatekeepers associated with tax pooling.
Overall inherent risk	Low	The restricted service offerings, domestic focus and lack of high risk customers and transactions in the sector justify a low risk rating. However, the potential to launder large amounts of funds, even if highly unlikely, is still a danger for this sector.

Appendix 10: Debt Collection

Variable	Assessed risk	Rationale
Nature, size and complexity of business	Low	There are a limited number of debt collection firms in New Zealand offering a very specific range of services. The specialised nature of this field reduces the exposure to ML/TF vulnerability. However, links to organised crime may be present within the sector to a limited degree.
Products/services	Medium	Debt collection firms offer a limited range of products/services with limited exposure to most high-risk products and services. Laundering money in the debt collection sector would require some level of collusion between the client and debtor in order to legitimise illicit funds.
Methods of delivery of products/services	Low	Debt collection firms offer their products and services via both face-to-face and non-face-to-face means.
Customer types	Medium	Debt collection firm customers are generally low-risk New Zealand-based companies and associated individuals. However, they need to consider ML/TF risk in relation to trusts, shell companies and legal entities associated with PEPs, as well as businesses associated with organised crime groups and high-risk industries.
Country risk	Low	Debt collection firms primarily operate in New Zealand.
Institutions dealt with	Low	Debt collection firms have limited exposure to dealing with institutions identified as presenting ML/TF risk.
Overall inherent risk	Low	Debt collection firms have limited exposure to high-risk products/services, and their interaction with generally lower-risk customers and institutions, mean this sector presents a low inherent risk of ML/TF. However, potential exposure to the ML/TF risk presented by organised crime groups needs to be considered.

Appendix 11: Factoring

Variable	Assessed risk	Rationale
Nature, size and complexity of business	Low	The factoring sector is small and highly specialised. Access and geographic spread is limited. The specialised nature of this field reduces the exposure to ML/TF vulnerability.
Products/services	Low	Laundering money 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. The ability to conceal or disguise large value transactions is a potential vulnerability.
Methods of delivery of products/services	Low	Factoring providers offer their products and services via both face-to-face and non-face-to-face means.
Customer types	Low	Factoring provider customers are generally low-risk New Zealand-based companies and individuals. However, they need to consider ML/TF risk in relation to trusts, shell companies and legal entities associated with PEPs, as well as businesses associated with organised crime groups and high-risk industries.
Country risk	Low	Factoring providers operate in New Zealand. However, the global and dynamic international ML/TF risk environment does present some ML/TF vulnerability.
Institutions dealt with	Low	Factoring providers have limited exposure to dealing with institutions identified as presenting ML/TF risk. However, there may be ML/TF risk present when dealing with banks and gatekeepers associated with factoring activity.
Overall inherent risk	Low	The low transaction number, domestic focus and lack of high risk customers and transactions in the sector justify a low risk rating. However, the potential to launder significant amounts of funds for ML purposes, even if highly unlikely, is still a danger for this sector.

Appendix 12: Financial Leasing

Variable	Assessed risk	Rationale
Nature, size and complexity of business	Low	The financial leasing sector is diverse. The specialised nature of this field reduces the exposure to ML/TF vulnerability.
Products/services	Low	Money launderers may consider the use of financial leasing as a means to legitimise money by making lease repayments using illicit funds. In addition, financial leasing can be considered a way of purchasing valuable assets (a known ML typology). However, the complexity of lease agreements and the long term nature of financial leases may make them too complicated and time consuming for money launderers.
Methods of delivery of products/services	Low	Financial leasing providers offer their products and services via both face-to-face and non-face-to-face means.
Customer types	Low	Financial leasing provider customers are generally low-risk New Zealand-based companies and associated individuals. However, consideration is required in regard to the ML/TF risk in relation to trusts, shell companies and legal entities associated with PEPs, as well as businesses associated with organised crime groups and high-risk industries. Determining beneficial ownership and executive control of customers also needs attention, as do persons acting on their behalf.
Country risk	Low	Financial leasing providers operate in New Zealand. However, the global and dynamic international ML/TF risk environment does present some ML/TF vulnerability.
Institutions dealt with	Low	Financial leasing providers have limited exposure to dealing with institutions identified as presenting ML/TF risk.
Overall inherent risk	Low	The lower transaction values, domestic focus and lack of high risk customers and transactions in the sector result in a low risk rating. However, ML through repayment of leasing arrangements is a possible typology and should not be discounted.

Appendix 13: Payroll Remittance

Variable	Assessed risk	Rationale
Nature, size and complexity of business	Low	There are a limited number of payroll remittance providers in New Zealand offering a very specific range of services. While transactions can be complex and of high value, the specialised nature of this field reduces the exposure to ML/TF vulnerability.
Products/services	Low	Payroll remittance providers offer a limited range of products/services with limited exposure to most high-risk products and services. DIA 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. ML/TF typologies are limited and difficult. For instance the use of 'ghost' or 'phantom' employees is a possible method to conduct ML.
Methods of delivery of products/services	Low	Payroll remittance providers offer their products and services via both face-to-face and non-face-to-face means.
Customer types	Low	Payroll remittance provider customers are generally low-risk New Zealand-based companies. However, they need to consider ML/TF risk in relation to trusts, shell companies and legal entities associated with PEPs, as well as businesses associated with organised crime groups and high-risk industries.
Country risk	Low	Payroll remittance providers primarily operate in New Zealand. However, global access of services and a dynamic international ML/TF risk environment can present some ML/TF vulnerability.
Institutions dealt with	Low	Payroll remittance providers have limited exposure to dealing with institutions identified as presenting ML/TF risk.
Overall inherent risk	Low	The high values and volume of payroll remittance activity exposes the sector to ML/TF vulnerabilities. However, there is a lack of evidence to suggest ML is occurring in the payroll remittance sector. In addition, there is limited exposure to cash and other high-risk products/services. Coupled with generally lower-risk customers and institutions this sector presents a low inherent risk of ML/TF.

Appendix 14: Safe Deposit Boxes

Variable	Assessed risk	Rationale
Nature, size and complexity of business	Low	There are a limited number of safe deposit box providers in New Zealand offering a very specific range of services. The specialised nature of this industry and its relative scarcity reduces the exposure to ML/TF but it is still vulnerable to criminal exploitation. Safe deposit boxes may be used to store cash whilst implementing the three stages of money laundering (Placement, Layering and Integration). The risk associated with safe deposit boxes 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.
Products/services	Medium	Safe deposit box providers offer a limited range of products/services, but they do have exposure to high-risk factors and vulnerabilities such as cash, high value commodities and anonymity. Products and services are vulnerable to criminal misuse and anonymity is highly desirable for ML/TF purposes.
Methods of delivery of products/services	Low	Safe deposit box providers offer their products and services via both face-to-face and non-face-to-face means. Access to the actual safe deposit box will be in person.
Customer types	Medium	Safe deposit box provider customers are generally New Zealand-based companies and individuals. However, they do need to consider ML/TF risk in relation to PEPs, as well as customers associated with organised crime groups and high-risk industries. Determining beneficial ownership and executive control of customers and persons acting on their behalf may present challenges.
Country risk	Low	Safe deposit box providers operate in New Zealand. However, the global and dynamic international ML/TF risk environment presents some ML/TF vulnerability and should not be discounted entirely.
Institutions dealt with	Low	Safe deposit box providers have limited exposure to dealing with institutions identified as presenting ML/TF risk.
Overall inherent risk	Low	Safe deposit box providers have limited exposure to high-risk products/services and generally lower-risk New Zealand customers. It is assessed this sector presents a low inherent risk of ML/TF. However, potential use by criminals (especially exploiting anonymity) should not be discounted.

Appendix 15: Virtual Asset Service Providers

Variable	Assessed risk	Rationale
Nature, size and complexity of business	Medium-high	VASPs face numerous risks in this sector. The nature of most VASPs lends itself to the rapid transfer of value, often with minimal oversight or controls. The complexity of a VASP business can vary, for example some exchanges may offer only a small selection of virtual assets and may not facilitate fiat currency transactions. These factors should be taken into account when assessing risks of a particular VASP.
Products/services	Medium-high	The services offered by VASPs will have varying degrees of high-risk characteristics for each service provided and can also vary depending on the nature of the virtual asset that is involved. Anonymity-enhanced cryptocurrencies (AECs), mixers, tumblers, decentralised platforms, and other products or services that enable or allow for reduced transparency and increased obfuscation of financial flows should be considered when assessing risk.
Methods of delivery of products/services	High	The internet-based nature of virtual assets lends itself to anonymity and non-face-to-face means of delivering services. Exposure to Internet Protocol (IP) anonymisers may further obfuscate transactions or activities and inhibit a VASP's ability to know their customers and implement effective AML/CFT measures.
Customer types	High	The VASP sector has a history of having a high-risk of exposure to criminals and organised crime. The sector is considered attractive to this type of customer due to its ability to reduce transparency and allow for obfuscation of financial flows. The risk of TF is also significant - terrorist organisations and their supporters and sympathisers are also constantly looking for ways to raise and transfer funds without detection or tracking by law enforcement.
Country risk	High	The VASP sector has significant exposure to higher risk jurisdictions through internet channels – it is effectively borderless. Exchanges, intermediaries, or related service providers may be located in jurisdictions which have limited or no AML/CFT obligations, and the potential for international sanctions to be avoided by countries or individuals.
Institutions dealt with	High	VASPs have exposure to other VASPs such as exchanges and wallet providers, which may have insufficient AML/CFT controls in place. Tumblers, peer-to-peer exchanges, and other methods of enhancing anonymity or obfuscating the flow of funds should be considered higher risk factors.
Overall inherent risk	High	Both domestic and international evidence and guidance points to risks presented by the VASP sector. The easy access and wide geographic spread of VASP services, coupled with their pseudo-anonymous nature and use in many different ML/TF typologies, means this sector presents a high inherent risk of ML/TF.

Appendix 16: Types of VASPs

Virtual Asset Exchanges	Virtual Asset Wallet Providers	Virtual Asset Broking	Initial Coin Offering (ICO) Providers	Providing investment opportunities in virtual assets
Issuing virtual assets such as virtual currency/digital tokens to facilitate virtual asset trading; or Providing a digital online platform facilitating virtual asset trading. Trading may occur between virtual assets or between virtual asset and fiat currency.	Providing storage for virtual assets or fiat currency on behalf of others and then facilitating exchanges between virtual assets or fiat currency.	Arranging transactions involving virtual assets.	Issuing and selling virtual assets/ digital tokens to the public (where tokens are not "financial products" under Financial Markets Conduct Act).	Providing an investment vehicle enabling investment in/ purchase of virtual assets (i.e. via a managed investment scheme or a derivatives issuer providing virtual asset options, or via a private equity vehicle that invests in virtual assets)

Appendix 17: Key ML/TF vulnerabilities and high-risk factors

Key vulnerabilities

Cash and liquidity

23. As noted in the NRA 2019, New Zealand is a relatively low-cash society. The NRA 2019 reports an increased circulation of high denomination bank notes, concurrent with declining use of cash in retail, but increased use in the hidden economy. The growth in the value of cash in circulation, in particular the value of high value notes, increases the capacity of the shadow economy to facilitate illicit transactions and store the proceeds of crime.

24. Crime such as drug dealing and converting stolen property generally generates proceeds in cash. Cash remains popular for ML/TF activity because it:
    - Is anonymous and does not require any record keeping
    - Is flexible, allowing peer-to-peer transactions
    - Can be used outside of formal financial institutions
    - Stores the value of the proceeds of crime outside of the financial sector
    - Facilitates the transfer of proceeds – between parties or geographical locations

25. Cash does have some disadvantages due to its bulk and need to be physically transported. In addition, it is likely to increase the risk of detection – either through arousing the suspicion of financial institutions (as large cash transactions are uncommon and often associated with illicit purchases) or being discovered by authorities.

26. Broadly, placement of cash criminal proceeds must occur either through deposits or co-mingling with legitimate cash, or transported offshore to where cash can be more easily placed through either deposits or co-mingling. The FIU highlighted this vulnerability in *Quarterly Typology Report Q4 2013–2014: Co-Mingling with Business Revenue*.[3]

27. The FIU reports multiple instances where individuals not involved in the predicate offending have been used to physically move cash (to act as cash couriers or money mules), particularly to transport cash internationally.

28. The use of cash-rich businesses is a well-known typology using all three stages of ML. They offer legitimacy and concealment of funds, easy methods of mixing criminal funds with legitimate income, and access to the financial sector. Cash-rich businesses include nail bars, takeaways and restaurants, bars, remitters, high value dealers and short-term loan businesses.

29. The FIU reports that offending using cash is highly visible and transactions involving cash are highly represented in historical STR reporting.

30. Criminals use cash to purchase assets, such as vehicles or real estate, and to conduct transactions through remittance channels (particularly international transactions).

31. Other ML/TF vulnerabilities presented by cash include:
    - Dispersing placement through multiple cash deposits (often called smurfing)
    - Refinement into higher-denomination notes or specific currencies
    - Being used in casinos and gaming/betting
    - Using anonymous deposit drop boxes or deposit-capable ATMs

[3] http://bit.ly/2hZZogQ

32. Customers with foreign currency accounts may conceal illegitimate funds generated overseas by depositing cash into those accounts, which allows them to easily convert, transfer and access the funds.

New payment technologies

33. New payment technologies (some more established than others) can increase the opportunities for ML/TF. In particular, they may allow criminals to exploit technological developments to break down the barriers posed by international borders, or to facilitate anonymous payments between individuals.

34. New payment technologies may exacerbate vulnerabilities in traditional channels by circumventing, hampering or defeating AML/CFT controls – for example, payments online allowing non-face-to-face transactions. Where CDD policies are unclear and reporting entities' knowledge of this topic is low, this may allow anonymity and subsequent abuse for ML/TF purposes.

35. Technology that can be accessed remotely anywhere in the world, that can move funds quickly, and that allows the quick reintegration of the proceeds of crime back into the financial system will be attractive to launderers and terrorist financiers.

36. New payment technologies may increase anonymity in other ways – for example, by allowing more person-to-person transactions outside of the regulated financial sector, or placing a layer between individuals undertaking transactions and reporting entities.

37. Money launderers and terrorist financiers may be attracted by the speed and convenience of new payment technologies. Criminals can exploit the borderless nature of the internet whereby there are difficulties regulating financial services that operate online.

38. Some new payment technology vulnerabilities are:
    - Open loop stored value instruments that may be used overseas
    - Online payment facilities offered by traditional financial sectors, such as banks and money remitters, particularly if the standard of AML/CFT compliance cannot be maintained in relation to these products
    - Online payment systems, particularly those that facilitate peer-to-peer payments or obscure purchases of valuable assets from financial institutions
    - Remitters offering money transfers to countries that provide e-wallets on phones

39. Virtual assets (e.g. Bitcoin) have not been observed in significant numbers in ML/TF cases, and where they have been used the value of funds has been relatively low. However, the products and methods of delivery associated with this typology present a dynamic ML/TF risk.

40. The FATF has produced guidance on this vulnerability – *Money Laundering Using New Payment Methods* (2010)[4] – though, by its nature, this topic is a dynamic risk environment and guidance will develop accordingly.

Anonymity and complexity (obfuscation)

41. Anonymity and complexity can be considered as part of the broader obfuscation of beneficial ownership and/or executive control. Obfuscation is highly desirable for ML/TF purposes. Any products, services, business relationships or methods of delivery that facilitate anonymity or the disguising of identity or ownership represents a high ML/TF risk.

42. Determining and verifying the identity of the individual (not legal) person(s) behind activities and transactions is one of the most important AML/CFT measures that reporting entities must undertake. Shortfalls in this area represent the highest ML/TF risk and will receive significant supervisory attention.

[4] http://bit.ly/1ewq4rq

43. The following items (not exhaustive in nature) all provide varying degrees of obfuscation. Reporting entities should carefully consider their use in the ordinary course of business and what AML/CFT measures should be deployed:
    - **Non face-to-face methods of delivery –** A lack of direct contact between reporting entities and customers makes it easier to use fraudulent or uncertified identity documents. Use of overseas documents in a non-face-to-face relationship also presents ML/TF risk.
    - **Shell companies –** New Zealand is an easy country to do business in and offers quick and simple establishment of companies. This can be abused by creating companies for criminal purposes (see the "Trusts, shell companies and other legal arrangements" section below).
    - **Trusts –** New Zealand has a large number of trusts (including family trusts), which are a well-known method of providing anonymity (see the "Trusts, shell companies and other legal arrangements" section below).
    - **Safety deposit boxes –** Though it is not a common typology in New Zealand, the use of deposit boxes has been linked in international reporting to organised crime and the hiding of the proceeds of crime.
    - **Use of electronic banking –** Where transactions occur without face-to-face contact with the reporting entity, criminals can use accounts set up by other persons, nominees or shell companies as a front for their activities. Electronic banking facilities often can be established in circumstances where it is difficult to verify the persons operating the account as distinguished from the account opener.
    - **Drop boxes/Smart ATMs –** These services provide a high degree of anonymity and an easy method to place the proceeds of crime into the banking system. The use of smart ATMs that accept deposits anonymously present ML/TF risk.

44. The use of intermediaries, such as brokers, presents a number of ML/TF vulnerabilities. The increased risk stems from the ability of intermediaries to control the arrangement and the sales environment in which they may operate.

45. Use of intermediaries may also circumvent some of the CDD effectiveness by obscuring the source of the funds from third parties. For some reporting entities, the use of intermediaries may be their sole distribution channel and for others it may account for an increasing market share, leaving them open to ML/TF risk.

46. The FIU highlighted the risks presented by intermediaries in the following reports:
    - *Quarterly Typology Report Q3 2013–2014: Money Laundering and Terrorist Financing through Professionals' Client Accounts*[5]
    - *Quarterly Typology Q2 2013–14: Money Laundering through Use of 3rd Party Intermediaries & Terrorism Financing (Intermediaries)*[6]

Lack of ML/TF awareness

47. While many reporting entities consider themselves at a low risk of ML/TF activity, their lack of awareness of the topic may make them more vulnerable to abuse by money launderers and terrorist financiers. The role of the compliance officer is key in preventing this, and DIA encourages them to explore and consider the ML/TF risk pertinent to their organisation.

48. To increase awareness, there are a number of agencies and organisations that provide open source guidance and information. Those listed below are a good place to start:
    - National Risk Assessment and Sector Risk Assessment (New Zealand)
    - Previous FIU Quarterly Typology Reports and current SAR guidance (New Zealand)
    - Sector supervisor guidance material (New Zealand)
    - APG typology reports (international)
    - FATF guidance and best practice material (international)
    - AUSTRAC guidance material (Australia)
    - UNODC guidance documents (international)

49. Establishing and maintaining an AML/CFT culture from the top down is an important part of having an effective regime. Senior management involvement is required for parts of the Act, and regular AML/CFT reporting to senior management should be business as usual.

[5] http://bit.ly/2zijNkM

[6] http://bit.ly/2jigHGE

50. Developing, maintaining, demonstrating and evidencing situational awareness is a vital responsibility of the compliance officer and the reporting entity. Keeping aware of ML/TF-related current affairs, media, typologies and research is expected from compliance officers. For instance, attending AML/CFT conferences and seminars can provide a wide range of benefits and learning opportunities as well as invaluable networking with peers.

51. Some basic awareness-raising situations from the Act are listed below:
    - **Reporting to Board and senior management –** The compliance officer is to act, where relevant, as a conduit between senior management and operational staff to ensure that AML/CFT is actioned and understood at all levels of an organisation.
    - **Training –** This is a key requirement for an adequate and effective AML/CFT programme, especially for senior managers, compliance officers and customer-facing staff. Training should include the identification of industry-specific red flags and anticipation of new and emerging risks and vulnerabilities.
    - **Audit –** Reporting entities must have their ML/TF risk assessment and AML/CFT programme audited on a regular basis. This presents an excellent opportunity to re-visit previous assessments and to incorporate the findings of the audit into existing policies, procedures and controls.
    - **Trigger events –** There is an expectation that reporting entities will develop processes and procedures that take into account dynamic risk factors, changes in legislation, advances in technology and new guidance material. These "trigger" events should prompt the reporting entity to re-visit its risk assessment and programme to ensure they are still fit for purpose.

Key high-risk factors

Trusts, shell companies and other legal arrangements

52. New Zealand company structures and trusts are attractive to money launderers because New Zealand's reputation as a well-regulated jurisdiction provides a veneer of legitimacy and credibility.

53. It is easy and inexpensive to register companies and set up trusts in New Zealand; they are essentially disposable and cheaply replaceable. In addition, registration on the Financial Service Provider Register may be misused to provide a veneer of legitimacy.

54. The attraction of trusts is their ability to hide beneficial ownership or involvement of criminals in transactions and to create a front behind which criminals may mask their activity. At the integration phase, trusts can be an effective means of dispersing assets while retaining effective control and enjoying the proceeds of criminal offending.

55. During layering, trusts and other legal entities may be used to create complex legal structures. Such legal structures obscure the involvement of the natural persons connected to the predicate offending. Trustees may be used as intermediaries in laundering transactions, which may allow especially complex and effective laundering where the trustee service is provided by professional service providers.

56. Using shell companies to conduct ML/TF transactions and activity helps criminals conceal the involvement of natural persons. The company conducts transactions while beneficial ownership or effective control of the company is hidden behind nominee directors and/or shareholders. The Act prohibits business relationships with shell banks.

57. Overseas money launderers may also use New Zealand's foreign trusts as a vehicle for international transactions, giving the appearance of a transaction involving New Zealand. This may make the transaction appear benign by trading on New Zealand's reputation, or may simply obscure the money trail by adding to the complexity of tracing money internationally.

58. Of note are New Zealand offshore finance companies, which present a very high degree of ML/TF vulnerability, especially around tax evasion, and should be subject to close attention.

59. The NRA 2018 highlights that trusts, companies and other legal persons or arrangements are extremely attractive vehicles for ML/TF purposes and are used to hide and protect the ownership of property by offenders.

60. Given the above, shell companies and trusts, including family trusts, should be considered highly vulnerable to ML/TF activity. The FIU highlighted these vulnerabilities in the following reports:
    - *Quarterly Typology Report Q2 2014–2015: Abuse of Shell Companies*[7]
    - *Quarterly Typology Report Q1 2014–2015: Abuse of Trusts*[8]

61. Legal arrangements are versatile, as they can be sold or transferred to other people along with the assets or bank accounts established in the name of the legal entity. In addition, disguising and concealing of beneficial ownership is relatively easy using deeply nested, and complex, legal arrangements across multiple jurisdictions.

62. Trusts/companies can give the appearance of legitimate business transactions and can be used at all three stages of the ML process. Trusts/companies can hinder detection and investigation of ML/TF. Trusts/companies can also be used to create complex structures that hinder law enforcement investigations.

63. There have been several high-profile international cases where New Zealand shell companies have been exploited to launder money. Currently there is no central register of trusts, and trust transparency is low, making it difficult to detect the existence of a trust, the activity of a trust, or the involvement of an individual in a trust.

64. Company structures, including complex arrangements using shell companies, limited partnerships, trusts, and other vehicles to obscure beneficial ownership, are readily available in New Zealand. These may be attractive to money launderers because:
    - Company registration can be facilitated online in one day
    - The cost of establishing a New Zealand company is low
    - There is minimal CDD – only verification of identity is required of persons involved in a company structure assessed as high risk
    - Third parties can be used as nominee shareholders and nominee directors
    - The beneficial owner of a company does not need to be declared
    - The physical location of the company does not need to be declared – the office of a lawyer, accountant, virtual office, or company formation agent can be used

International payments

65. International payments appear to be the primary means for money launderers and terrorist financiers to move illicit funds offshore. This movement of funds can constitute either layering or integration. In addition, it can constitute placement of cash proceeds of crime, especially in the case of remitters.

66. Transactions involving countries with limited or no ML/TF controls will present a higher risk. The use of wire transfers to move funds cross-border relatively quickly is recognised internationally as one of the most common methods to launder funds.

67. Wire transfers between jurisdictions can obscure the source of funds, particularly where information on the originator of the transaction is incomplete or absent. While international wire transfers are more likely to attract suspicion, domestic transfers are not free of risk.

68. Moving funds transnationally allows criminals to complicate investigations by creating a complex money trail and creates jurisdictional hurdles for law enforcement agencies. Criminals may structure their transactions, including occasional transactions, to be below reporting/identification thresholds to avoid detection.

[7] http://bit.ly/2BfP21c

[8] http://bit.ly/2A2XKC6

69. ML/TF via international payment may be easily combined with other ML/TF methods, such as the use of professional services, use of intermediaries and the use of trusts and companies.

70. Entities engaged in international payments can be involved in foreign currency exchange and may accept cash. Some entities that conduct international payments, such as brokers, may be perceived as prestigious and therefore low risk.

71. International payments may facilitate the use of "money mules" to create layers and obscure the money trail. For example, transnational payments could be made to a money mule's account, which is then followed by cash withdrawal and the remittance of that cash.

72. Payments between companies for goods or services may facilitate the flow of funds between criminals in different jurisdictions and/or create layers in laundering or terrorism financing schemes.

73. ML/TF risks may relate to the jurisdictions the wire transfer comes from or passes through as well as the parties to the transaction.

74. Transactions through New Zealand may be one of many stops in a transaction path in an effort to disguise the country of origin and give the appearance of clean funds from a lower-risk jurisdiction. Risks may include criminals deleting or substituting accompanying information to circumvent ML/TF controls.

75. Money launderers may use New Zealand businesses to move funds to escape detection in their own jurisdiction. Third parties may be based in overseas locations with reduced or no AML/CFT requirements. Some countries also have secrecy laws or conventions that prevent the underlying beneficiary or source of funds being identified.

76. Premium payments made via companies in offshore financial centres may shield the origin of the funds. Similarly, requests for redemption of products by an organisation or person in another country may cause suspicions.

77. The FIU highlighted this vulnerability (wire transfers) in *Quarterly Typology Report Q1 2013–2014: Money Laundering Typology – Wire Transfers*.[9]

High-risk customers and jurisdictions

78. Customers represent the primary source of ML/TF risk for reporting entities. Every effort should be made to ensure CDD is carried out in line with a risk-based approach and that it is both robust and proportionate. Given the importance of CDD, reporting entities need to be mindful of identify fraud and the use of uncertified or counterfeit identity documents.

79. Certain occupations or businesses are also considered high risk depending on their exposure to ML/TF vulnerabilities – for example, customers involved in arms manufacturing, extraction industries, high-value and cash-intensive businesses, and casinos. In addition to the ML/TF opportunities, money launderers may be attracted to a business because its industry provides access to other facilitators of crime. FIU research indicates that transport businesses, pharmacies and bars may all be used to facilitate the trafficking and sale of illicit drugs.

80. Businesses, particularly cash businesses, have long been identified as being vulnerable to ML/TF activity. They are a particularly attractive option for obscuring the money trail at placement and layering phases. The classic technique of co-mingling cash proceeds with cash takings from a business to place funds in a financial institution establishes a legitimate origin for the cash, and reduces suspicion and detection by a financial institution.

81. Small, cash-intensive businesses are attractive to criminals as they may also be expected to have less sophisticated AML/CFT awareness.

82. At the layering stage, criminals may move funds through business accounts to avoid suspicion or to place a layer between the financial institution and the individual involved. Use of a business controlled by a third party can effectively obscure the involvement of beneficial criminal owners in a transaction.

[9] http://bit.ly/2Asgb3N

83. When a reporting entity conducts their risk assessment, they need to assess how their business may be vulnerable to ML/TF because of the countries they deal with. There is no universally agreed definition of a high-risk country, but when undertaking a risk assessment, some variables to consider include countries that are:
    - Identified as lacking adequate AML/CFT systems/measures or controls
    - Identified as having supporters of terrorism or the financing of terrorism
    - Identified as having significant levels of corruption and/or organised crime
    - Identified by credible sources as being tax havens
    - Associated with production and/or transnational shipment of illicit drugs or people trafficking
    - Subject to sanctions, embargoes or similar measures

84. The Act does not prohibit business relationships or transactions with persons/organisations based in high-risk countries. However, reporting entities should make sure sufficient mitigation and control measures are in place. When dealing with a high-risk jurisdiction, the following ML/TF factors should be considered:
    - Is the country a conflict zone or a jurisdiction associated with terrorism?
    - Does the country have laws that make it illegal to launder money or finance terrorism?
    - Does the country's legislative framework put obligations on financial institutions for CDD, account monitoring, SARs and record keeping similar to those set out in the Act?
    - Does the country have an established and effective AML/CFT supervisory regime?
    - Is the country a member of the FATF or a FATF-style regional body (e.g. the APG)?
    - Has the country been subject to any recent independent assessment of its AML/CFT systems/measures (i.e. a FATF mutual evaluation)?
    - Are there any public concerns raised about the country's AML/CFT systems/measures?
    - Does the country have a high degree of organised crime, bribery and corruption, or human trafficking?

85. Reporting entities should consider not only high-risk countries but also their neighbouring countries, as ML/TF activity can involve the movement of funds across the border. As such, reporting entities may wish to consider "high-risk jurisdictions" to cover both high ML/TF risk countries and their neighbours.

86. For further guidance, refer to the sector supervisors' *Countries Assessment Guideline* (2012).[10]

PEPs and high net worth individuals

87. Reporting entities should establish whether the customer is a politically exposed person (PEP) or a relative/close associate (RCA) of a PEP. If they are, then enhanced CDD (most commonly known as "EDD") will be required. However, not all PEPs carry the same risks. This will depend on the country the PEP is from, where they are located (see the "High-risk customers and jurisdictions" section above) and the position of power or funds the person holds or controls.

88. For very high-risk PEPs, extra AML/CFT measures will be needed.

89. Senior management authorisation is required by the Act to establish a business relationship with a PEP. The reporting entity must also obtain information about the source of wealth or source of funds of the PEP.

90. Foreign PEPs may use financial institutions in other countries, such as New Zealand, to launder funds away from scrutiny in their home jurisdiction. The position of power of PEPs and the control they may exert in their home country means that it may be easier for them to access the proceeds of crime. Such funds may be diverted from legitimate sources or may be the result of corruption or bribery.

91. Facilities provided to higher net worth customers and heads of international organisations (HIOs), particularly those with dedicated customer representative relationships, can be misused for ML/TF. This is especially the case if transactions are rarely questioned because of the high value of the business to the reporting entity.

[10] http://bit.ly/2hOTHPk

92. High net worth individuals/HIOs may have patterns of financial activity that can be exploited to mask ML/TF. Value, volume and velocity red flags that would apply to other customers may be ignored for presumed legitimate activity.

93. The sources for the funds that a PEP/HIO may try to launder are not only bribes, illegal kickbacks and other directly corruption-related proceeds but also embezzlement, tax fraud, and theft of State assets or funds from political parties and unions. PEPs/HIOs that come from countries or regions where corruption is endemic, organised and systemic present the greatest risk. However, it should be noted that corrupt or dishonest PEPs/HIOs can be found in almost any country.

94. Transparency is an issue that goes beyond the fight against corruption and ML/TF. It also impacts tax evasion, corporate governance, and the fight against all types of criminal activity. The FATF has produced several papers on this topic, including *Specific Risk Factors in Laundering the Proceeds of Corruption: Assistance to Reporting Institutions* (2012).[11]

Gatekeepers

95. Professional 'gatekeepers' such as lawyers, accountants, trust and company service providers (TCSPs) and real estate agents have long been identified as a ML/TF high-risk factor. The NRA 2018 highlights the ML/TF risks associated with gatekeepers and details the vulnerabilities within the sector.

96. In addition, the consequences if professional services are being abused for ML/TF purposes have the potential to be very serious. Refer to the DNFBPs & Casinos SRA for more information on these risk factors.

97. The involvement of a professional gatekeeper can provide launderers with the impression of respectability, legitimacy and/or normality especially in large transactions. It also provides a further step in the laundering chain which frustrates detection and investigation.

98. Professionals may also allow launderers to access services and techniques that they would not ordinarily have access to. This may be as simple as making introductions (e.g. to open an account) or facilitating setting up structures such as trusts.

99. Vulnerabilities in the legal and accountancy profession include the use of client accounts, trust accounts, purchase of real estate (this would also apply to other purchases of large assets and businesses), creation of trusts and companies, management of trusts and companies, setting up and managing charities and managing client affairs. While each of these areas are legitimate services these services may be exploited by money launderers and/or terrorism financiers.

100. The real estate sector is a well-recognised avenue for ML/TF. Real estate is readily available in New Zealand and is a very active market. Purchasing both residential and commercial property is a reliable and profitable investment strategy. The FIU considers that the real estate sector is highly vulnerable to ML. It also considers that international exposure is significant, and there is a risk that New Zealand real estate is being abused by offshore criminals.

101. The value of the sector, the volume of sales and the low level of detection capacity make the real estate sector highly vulnerable to layering and integration of criminal proceeds. Real estate poses significant risk across many DIA sectors. Refer to the DNFBPs & Casinos SRA for more information on this specific vulnerability.

102. The use of intermediaries, such as brokers, present a number of ML/TF vulnerabilities. The increased risk stems from the ability of intermediaries to control the arrangement and the sales environment in which they may operate. Use of intermediaries may also circumvent some of the due diligence effectiveness by obscuring the source of the funds from third parties. For some reporting entities, the use of intermediaries may be their sole distribution channel and for others it may account for an increasing market share leaving them open to ML/TF risk.

103. The FIU have highlighted ML/TF through professional's client accounts and ML/TF through the use of third party intermediaries.

[11] http://bit.ly/1M0fkGo

Money Service Businesses

104. Money service businesses (MSBs) - also called money remitters, money value transfer services (MVTS) – are included in the list of high-risk factors as a typology and not as an indication of the industry as a whole. Domestic and international experience, along with FATF guidance, has highlighted this sector as presenting significant ML/TF risk. This includes alternative remittance, defined by FATF as money transfer services outside of the formal or licensed financial sector.

105. The FATF found that alternative remittance networks may be expanding internationally and are a growing concern. They have classified alternative remittance into three categories:
    - **Traditional hawala and similar service providers –** Providers may establish traditional services within emerging or existing ethnic communities.
    - **Hybrid gatekeepers and alternative remittance providers –** Gatekeepers may expand their services to offer alternative remittance.
    - **Criminal alternative remittance providers –** These are established or expanded to serve criminals and/or circumvent controls. They are by nature high risk and may be connected to complex specialised ML/TF networks managed by offshore international "controllers".

106. Currency exchange businesses are also considered to be MSBs and are vulnerable to ML/TF. Exchanging funds for an easily exchangeable and transportable currency, often at a variety of institutions, allows for funds to be moved into other countries without questions that may be raised from electronic transactions or wire transfers. Criminals may exchange low-value foreign currency notes for higher-value denominations that are more easily transportable. This is sometimes referred to as refining.

107. Despite their decline in use traveller's cheques appear in international case studies of ML. Foreign currency drafts provide an easy method of removing funds from the country and little information is generally required about the recipient.

108. An important consideration with MSBs is their role in supporting vulnerable and hard to reach populations. Financial exclusion based purely on a category of customer, product or jurisdiction is not in line with the FATF Recommendations. Reporting entities are expected to apply a risk based approach to MSBs and mitigate ML/TF risks in a proportionate manner.

109. The FATF has released a number of guidelines in relation to MSBs including 'Guidance for a Risk Based Approach – Money or Value Transfer Services' (2016)[12]', and 'Money Laundering through Money Remittance and Currency Exchange Providers (2010)[13]'.

110. For further information on MSBs refer to the money remittance section of this SRA.

[12] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-money-or-value-transfer.html

[13] http://www.fatf-gafi.org/publications/methodsandtrends/documents/

Appendix 18: Suggested reading and source documents

111. All the following are open source documents used in the production of the Financial Institutions SRA 2019. They can be located via an internet search and are freely accessible. Some documents are available on multiple sites..

International

- FATF Report – *Guidance for a Risk Based Approach – Money or Value Transfer Services* – February 2016
- FATF Report – *Terrorist Financing FATF Report to G20 Leaders – Actions Being Undertaken by the FATF* – November 2015
- FATF Report – *Emerging Terrorist Financing Risks* – October 2015
- FATF Report – *Financing of ISIL* – February 2015
- FATF Report – *Risk of Terrorist Abuse in Non-Profit Organisations* – June 2014
- FATF Report – *Virtual Currencies: Key Definitions and Potential AML/CFT Risks* – June 2014
- FATF Report - *The role of Hawala and other similar service providers in money laundering and terrorist financing* - October 2013
- FATF Report – *Guidance for a Risk Based Approach – Prepaid Cards, Mobile Payments and Internet Based Payment Services* – June 2013
- FATF Guidance – *National Money Laundering and Terrorist Financing Risk Assessment* – February 2013
- *FATF Recommendations – International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation* – February 2012
- FATF Report – *Money Laundering through Money remittance and Currency Exchange Providers* – July 2010
- FATF Report – *Money Laundering Using New Payment Methods* – October 2010
- FATF Report – *Money Laundering Using Trust and Company Service Providers* – October 2010
- FATF Report – *Vulnerabilities of Casinos and Gaming Sector* – March 2009
- FATF Report - *Guidance on the Risk Based Approach for Casinos* - October 2008
- FATF Report – *Proliferation Financing Report* – June 2008
- FATF Report – *The Misuse of Corporate Vehicles, Including Trust and Company Service Providers* – February 2007.
- APG – *APG Yearly Typologies Report 2016*
- APG – *APG Yearly Typologies Report 2015*
- APG – *APG Yearly Typologies Report 2014*
- APG – *Trade Based Money Laundering Typologies* – July 2012
- APG – *New Zealand Mutual Evaluation Report (MER)* – 2010
- UNODC – *Risk of Money Laundering through Financial Instruments – 2nd Edition* – 2013
- European Supervisory Authorities (ESA) – *Final Guidelines – Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849: Risk Factor Guidelines* – June 2017
- OSCE – *OSCE Handbook on Data Collection in support of Money Laundering and Terrorism Financing National Risk Assessments* – 2012
- HM Treasury and Home Office – *UK National Risk Assessment of Money Laundering and Terrorist Financing* – October 2015
- HM Treasury and Home Office – *Anti-money Laundering and Counter Terrorist Finance Supervision Report 2013–14* – updated March 2015
- Basel Institute on Governance – *AML Index* – accessed May 2018
- AS/NZS ISO 31000:2009 – *Risk Management – Principles and Guidelines*
- AS/NZS ISO 4360:2004 – *Risk Management*
- FINTRAC – *Guidance of the Risk Based Approach to Combating Money Laundering and Terrorist*

Financing – May 2015

- FINTRAC – *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada* – July 2015
- FINTRAC – FINTRAC Typologies and Trends Reports – (multiple)
- Department of the Treasury/Justice/Homeland Security/Federal Reserve/US Postal Service – *U.S. Money Laundering Threat Assessment* – December 2005
- AUSTRAC – *Insights from Compliance Assessments* – December 2016
- AUSTRAC – *Methodologies Brief 01 – Building a Profile: Financial Characteristics Associated with Known Foreign Terrorist Fighters and Supporters* – December 2015
- AUSTRAC – *Terrorism Financing in Australia* – 2014
- AUSTRAC – *Typologies and Case Studies Report* – various
- AUSTRAC – *Money Laundering in Australia* – 2011
- AUSTRAC – *Insights from Compliance Assessments* – December 2016
- The Egmont Group of FIUs – *100 Cases from the Egmont Group* – (date unknown)
- The Egmont Group of FIUs – *FIUs and Terrorist Financing Analysis Report* – (date unknown)

Domestic

- FIU – *National Risk Assessment of Money Laundering and Terrorist Financing 2019*
-
- FIU – *National Risk Assessment of Money Laundering and Terrorist Financing 2018*
- FIU – *National Risk Assessment of Money Laundering and Terrorist Financing 2010*
- FIU – *National Risk Assessment of Money Laundering and Terrorist Financing 2010 – Support Document*
- FIU – Quarterly Typology Reports (multiple)
- FIU – Suspicious Activity Reporting Guideline – 2018
- FIU – Terrorism Suppression Act 2002 Advisory – 2013
- FIU – Financial Action Task Force (FATF) statements and advisories (ongoing)
- FIU – PTR: Understanding the Regulations – 2017
- FIU – PTR: Reporting (Obligation) Guidance – 2017
- DIA – AML/CFT Sector Risk Assessment Guides (multiple) – April 2014
- DIA – *Internal Affairs AML/CFT Sector Risk Assessment* – March 2011
- DIA – *Phase 2 AML/CFT Sector Risk Assessment* – December 2017
- DIA – *Risk Assessment and Programme: Prompts and Notes for DIA reporting entities* – December 2017
- FMA (then Securities Commission) – *Anti-Money Laundering and Countering the Financing of Terrorism Sector Risk Assessment* – March 2011
- FMA – *Anti-Money Laundering and Countering Financing of Terrorism Sector Risk Assessment* – 2017
- RBNZ – Sector *Risk Assessment for Registered Banks, Non-Bank Deposit Takers and Life Insurers* – March 2011
- RBNZ – *Sector Risk Assessment for Registered Banks, Non-Bank Deposit Takers and Life Insurers* –

February 2017

- RBNZ, DIA and FMA – *Beneficial Ownership Guideline* – December 2012
- RBNZ, DIA and FMA – *Countries Assessment Guideline* – July 2012
- RBNZ, DIA and FMA – *AML/CFT Programme Guideline* – May 2018
- RBNZ, DIA and FMA – *Risk Assessment Guideline* – May 2018
- RBNZ, DIA and FMA – *In the Ordinary Course of Business Guideline* – December 2017

Appendix 19: Terrorism financing and dual-use items and proliferation risk factors

112. The TF environment in New Zealand is assessed by the NRA 2019 as low risk. Despite this assessment, it is prudent for **all** DIA reporting entities to consider the vulnerabilities and risk factors associated with TF and the potential red flags that may indicate TF activity. Reporting entities should consider not only high-risk countries but also their neighbouring countries, as TF often involves the movement of funds across borders.

Nature of TF

113. The characteristics of TF can make it difficult to identify. Transactions can be of low value, they may appear as normal patterns of behaviour, and funding can come from legitimate as well as illicit sources. However, the methods used to monitor ML can also be used for TF, as the movement of those funds often relies on similar methods to ML. Internationally the TF process is considered to typically involve three stages:
    - **Raising funds** (through donations, legitimate wages, selling items or criminal activity)
    - **Transferring funds** (to a terrorist network, to a neighbouring country for later pick up, to an organisational hub or cell)
    - **Using funds** (to purchase weapons or bomb-making equipment, for logistics, for compensation to families, for covering living expenses)

114. Given the global nature of TF and the constantly changing nature of international tensions and conflicts, the risks associated with TF are highly dynamic. As such, reporting entities need to ensure that their CFT measures are current, regularly reviewed and flexible. It is important that reporting entities maintain situational awareness and effective transaction monitoring systems or procedures that incorporate dynamic TF risks, as well as the more static risks associated with ML.

115. The value of funds moved through New Zealand connected to TF is likely to be much lower than other forms of illicit capital flows. However, if funds connected to TF were to be associated with New Zealand reporting entities, it would likely have a disproportionate effect on New Zealand's reputation. Outside of the obvious harm caused by TF, any New Zealand reporting entity associated with this activity could see their reputation severely damaged. If their CFT measures were found to be inadequate or ineffective, they could also face civil and even criminal charges.

New Zealand as a conduit for TF

116. One of the potential consequences of transnational ML is that channels may be established that may also be exploited by terrorist financiers. Overseas groups may seek to exploit New Zealand as a source or conduit for funds to capitalise on New Zealand's reputation as being low risk for TF. For instance, funds originating in or passing through New Zealand may be less likely to attract suspicion internationally.

117. TF through the Phase 2 sectors can be small-scale and indistinguishable from legitimate transactions. TF could involve structured deposits of cash into bank accounts followed by wire transfers out of New Zealand. It could also involve remittance agents sending funds overseas. More complex methods could see New Zealand businesses, professional services, non-profit organisations and charity accounts being used as fronts for sending funds offshore (see "TF indicators and warnings (red flags)" section below for further red flags).

118. Given the difficulty of detecting TF, reporting entities' transaction monitoring systems and procedures will play a key role, especially given PTR obligations. Furthermore, the Phase 1 sectors' knowledge of their customers and their customers' established and expected transactions and activity is vital in determining if TF activity is potentially taking place.

Remitters and alternative remitters (remitters)

119. Remitters are recognised internationally as presenting a high risk of TF, and reporting entities should be aware of the risks associated with them. To some extent remitters offer a degree of anonymity (variable levels of CDD) and an easy method of moving funds to countries that may have little or no formal banking structure, high levels of corruption and poor CFT measures. **However, many communities and countries rely on the flow of funds using remitters and AML/CFT responses to the risks they present should be proportionate and reflect a risk-based approach.**

Non-profit organisations and charities

120. The use of non-profit organisations and charities is an internationally recognised TF typology. They can be used to disguise the movement of funds to high-risk regions, and funds raised for overseas humanitarian aid can be co-mingled with funds raised for TF. Non-profit organisations can also easily and legitimately access materials, funds and networks of value to terrorist groups. In addition, funds sent overseas by charities with legitimate intentions can also be intercepted when they reach their destination country.

121. The FATF reports that the non-profit organisations most at risk of abuse are those engaged in "service" activities that are operating near an active terrorist threat. Funds sent to high-risk jurisdictions for humanitarian aid are at increased risk of being used for TF if they are sent through less-established or start-up charities and non-profit organisations. Some donors may willingly provide donations to support terrorist groups, while other donors, and the charities themselves, may be coerced, extorted or misled about the purpose of funding.

122. However, it is important to consider this TF vulnerability in the context of the lower-risk New Zealand environment, and that this will not apply to the vast majority of New Zealand charities and non-profit organisations.

Cash couriers

123. TF risk associated with cash couriers is assessed internationally as high. This method of TF may be undertaken by multiple individuals and may involve smuggling cash across porous borders to high-risk TF jurisdictions. Bulk cash smuggling can also be used. To this end, the presence of high-value bank notes (such as the 500-euro note, which facilitates the easy transportation of large amounts of funds) may be an indicator of TF (as well as ML). The 500-euro note has been removed from sale in some jurisdictions due to its overwhelming use in organised crime.

New Zealand shell companies

124. FIU research indicates that overseas groups have demonstrated a desire to use New Zealand shell companies for activities similar to TF (see examples below). As such, reporting entities should not immediately discount New Zealand companies from suspicion of TF as a matter of course.
    - 2009 – New Zealand shell companies were connected to an attempt to ship arms from North Korea in violation of UN sanctions. It is suspected that the arms in this case were enroute to Iran and potentially destined for use by one of Iran's paramilitary/insurgent clients.
    - 2014 – A New Zealand postal hosting service was apparently abused to establish a website associated with the Islamic State. The persons responsible for the website were successful in using the New Zealand address for activities that could facilitate financing.

FATF and TF

125. TF continues to be a priority issue for the FATF. They have published numerous papers on the topic, including *Terrorist Financing Typologies Report* (2008) , *Terrorist Financing in West Africa* (2013) , *Risk of Terrorist Abuse in Non-Profit Organisations* (2014) *and Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)* (2015) . This attention reflects global concern in relation to TF and signals the need for reporting entities to give TF due consideration in their ML/TF risk assessment.

TF indicators and warnings (red flags)

126. ML and TF share many indicators and warnings, or red flags. The following red flags may help reporting entities in the difficult task of drawing a link between unusual or suspicious activity and TF. The list is not exhaustive, and DIA encourages reporting entities to identify red flags that may occur in their ordinary course of business as part of their risk assessment. Red flags that may occur include:
    - International funds transfers to and from high-risk jurisdictions, potentially at multiple branches of the same reporting entity
    - Multiple customers and/or occasional transactions by non-customers conducting international funds transfers to the same beneficiary located in a high-risk jurisdiction
    - A customer conducting funds transfers to multiple beneficiaries located in high-risk jurisdictions
    - A customer using incorrect spelling or providing variations on their name when conducting funds transfers to high-risk jurisdictions
    - Large cash deposits and withdrawals to and from non-profit organisation accounts
    - Individuals and/or businesses transferring funds to listed terrorist entities or entities reported in the media as having links to terrorism or TF
    - Funds transfers from the account of a newly established company to a company selling dual-use items (see the "Proliferation and dual-use items" section below)
    - A sudden increase in business/account activity, inconsistent with customer profile
    - Multiple cash deposits into personal account described as "donations" or "contributions to humanitarian aid" or similar terms
    - Multiple customers using the same address/telephone number to conduct business/account activity
    - Proscribed entities or entities suspected of terrorism using third-party accounts (e.g. a child's account or a family member's account) to conduct transfers, deposits or withdrawals
    - Use of false identification to establish New Zealand companies
    - Pre-loading credit cards, requesting multiple cards linked to common funds or purchasing cash passports/stored-value cards prior to travel in order to courier cash overseas
    - Customers taking out loans and overdrafts with no intention or ability to repay them or using fraudulent documents
    - Customers emptying out bank accounts and savings
    - Customers based in or returning from conflict zones
    - Evidence of payments from insurance fraud simulating traffic accidents
    - Customers converting small-denomination bank notes into high-denomination notes (especially US dollars, euros or sterling)

Emerging TF risk

127. The FATF has highlighted the need for forward-looking analysis in relation to TF given the dynamic risk environment. Areas of potential risk are:
    - Foreign terrorist fighters and foreign terrorist supporters
    - Fundraising through social media
    - New payment products and services
    - Exploitation of natural resources

128. The extent to which these avenues have been exploited for TF purposes is unclear and, although these activities may not have an immediate association with reporting entities, their potential impact on TF should be noted.

129. The dynamic nature of the TF environment necessitates that reporting entities should make sure their compliance officers maintain situational awareness in relation to this topic. Reporting entities should also make sure that in the face of evolving TF risk factors their AML/CFT measures are both adequate and effective.

130. This should be reflected in relevant AML/CFT documentation and be evidenced by regular testing and validation. While the likelihood of TF in New Zealand may be low compared to other jurisdictions, the consequences are potentially catastrophic.

Proliferation and dual-use items

131. These items are taken from the FATF *Proliferation Financing Report* (2008)[14]

Nuclear	Chemical	Biological	Missile and delivery
Centrifuges	Scrubbers	Bacterial strains	Accelerometers
High-speed cameras	Mixing vessels	Fermenters	Aluminium alloys
Composites	Centrifuges	Filters	Aluminium powders
Maraging steel	Elevators	Mills	Gyroscopes
Mass spectrometers	Condensers/Coolers	Presses	Isostatic presses
Pulse generators	Connectors	Pumps	Composites
X-ray flash apparatus	Heat exchanges	Spray dryers	Maraging steel
Pressure gauges	Precursors	Tanks	Homing devices
Ignition	Pumps	Growth media	Oxidants
Vacuum pumps	Reactors		Machine tools

132. The FATF *Proliferation Financing Report* (2008) identified the following general risk factors:
- Weak AML/CFT controls and/or weak regulation of the financial sector. A weak or non-existent export control regime and/or weak enforcement of the export control regime.
- Non-party to relevant international conventions and treaties regarding the non-proliferation of weapons of mass destruction. Lack of implementation of relevant United Nations Security Council resolutions.
- The presence of industry that produces weapon of mass destruction components or dual-use goods.
- A relatively well-developed financial system or an open economy. A jurisdiction that has secondary markets for technology. The nature of the jurisdiction's export trade.
- A financial sector that provides a high number of financial services in support of international trade. Geographic proximity, significant trade facilitation capacity (e.g. trade hub or free trade zone), or other factors causing a jurisdiction to be used frequently as a trans-shipment point from countries that manufacture dual-use goods to countries of proliferation concern.
- Movement of people and funds to or from high-risk countries can provide a convenient cover for activities related to proliferation financing.

[14] http://bit.ly/2zBY0Yd

Appendix 20: AML/CFT abbreviations and acronyms

133. This table contains abbreviations and acronyms used in this document and in the wider AML/CFT environment. It is included for reference purposes.

1LOD, 2LOD etc.	first line of defence, second line of defence…
AML	anti-money laundering
AML/CFT compliance officer	compliance officer
APG	Asia Pacific Group
ATAINZ	Accountants and Tax Agents New Zealand
AUSTRAC	Australian Transaction Reports and Analysis Centre
BCR	border cash report
BO	beneficial owner
CAANZ	Chartered Accountants Australia and New Zealand
CBR	correspondent banking relationship
CDD	customer due diligence
CFT	countering financing of terrorism
CPRA	Criminal Proceeds (Recovery) Act 2009
CTR	cash transaction report (part of prescribed reporting)
DBG	designated business group
DIA	Department of Internal Affairs
DNFBP	designated non-financial business or profession/gatekeeper
EDD	enhanced customer due diligence
Egmont	Egmont group of international FIUs
FATF	Financial Action Task Force
FATF 40	FAFT 40 Recommendations for AML/CFT and proliferation
FinCEN	Financial Crimes Enforcement Network (USA)
FINTRAC	Financial Transactions and Reports Analysis of Canada
FIU	Financial Intelligence Unit (hosted by NZ Police)
FMA	Financial Markets Authority
FSRB	FATF style regional body (APG is an FSRB)
FTRA	Financial Transaction Reporting Act 1996
goAML	FIU reporting system for STRs/SARs
HIO	head of international organisation (e.g. a company president or CEO)
HVD	high-value dealer
I&W	indicators and warnings (of ML/TF)
IFT	international fund transfer (part of prescribed reporting)
IFTI	international fund transfer instruction (part of prescribed reporting)
IVCOP/IDVCOP	Identity Verification Code of Practice
LCT	large cash transaction (part of prescribed reporting)

LPP	legal professional privilege
MER	mutual evaluation report
ML	money laundering
MSB	money service business
N&P	nature and purpose
NBDT	non-bank deposit taking entity
NBNDT	non-bank non-deposit taking entity
NCC	National Coordination Committee
NRA	National Risk Assessment
NZFT	New Zealand Foreign Trusts
NZOFCs	New Zealand Offshore Finance Companies
NZRB	New Zealand Racing Board
PAOBO	person acting on behalf of
PEP	politically exposed person
Phase 2	Phase 2 of the AML/CFT Act
POWBATIC	person on whose behalf a transaction is carried out
PPCs	procedures, policies and controls
PTR	prescribed transaction report
QA	quality assurance
QTR	Quarterly Typology Report
RA	risk assessment
RBNZ	Reserve Bank of New Zealand
RCA	relative/close associate (of PEP)
RE	reporting entity
Regs	AML/CFT Regulations
SAR	suspicious activity report
SPR	suspicious property report (Terrorism Suppression Act 2002)
SRA	sector risk assessment
STR	suspicious transaction report
SVI	stored value instruments
TBML	trade-based money laundering
TCSP	trust and company service provider
TF	terrorism financing
TM	transaction monitoring
TSA	Terrorism Suppression Act 2002
UNODC	United Nations Office on Drugs and Crime