



DECEMBER 2021

# Anti-Money Laundering and Countering Financing of Terrorism

## Sector Risk Assessment 2021

# Contents

---

<b>Executive summary</b>	<b>4</b>
Background	4
Purpose of this Sector Risk Assessment	5
Key changes between the SRA 2017 and the SRA 2021	5
Comments on the risk ratings	5
How REs should use the SRA	6
<b>Section 1: Money laundering and terrorism financing risks in New Zealand</b>	<b>7</b>
The Anti-Money Laundering and Countering Financing of Terrorism Act 2009	7
<b>Section 2: Methodology</b>	<b>9</b>
<b>Section 3: Risk key</b>	<b>11</b>
Virtual assets	13
<b>Section 4: Potential red flags</b>	<b>14</b>
<b>Section 5: Money laundering the proceeds of crime</b>	<b>15</b>
Stages of money laundering	15
Predicate offences	15
The use of cash in money laundering	16

This copyright work is licensed under the Creative Commons Attribution 3.0 New Zealand licence. You are free to copy, distribute and adapt the work, as long as you attribute the work to the Financial Markets Authority and abide by the licence terms. To view a copy of this licence, visit [creativecommons.org](https://creativecommons.org)

<b>Section 6: Terrorism financing</b>	<b>17</b>
Overview	17
Terrorism financing risk in our supervised sectors	17
Key indicators and red flags for terrorism financing	18
Emerging terrorism financing risk	18
Proliferation	18
<b>Section 7: How to interpret the data in this report</b>	<b>20</b>
<b>Section 8: Sector risks</b>	<b>21</b>
Derivatives issuers	22
Providers of client money or property service (Brokers and custodians)	26
Equity crowdfunding platforms	32
Financial Advice Providers	36
Managed investment scheme (MIS) managers	40
Peer-to-peer lending providers	44
Discretionary investment management services (DIMS)	48
Licensed supervisors	52
Issuers of securities	55
<b>Appendix : Glossary</b>	<b>56</b>

# Executive summary

## Background

The FMA supervises reporting entities (REs) in ten sectors under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the Act).

Our Sector Risk Assessment (SRA) helps us and the REs we supervise understand the risks of money-laundering (ML) and terrorism financing (TF) in each sector. This SRA replaces our SRA published in 2017. See page 5 for details about the differences between the two reports.

This SRA takes into account information from the Financial Intelligence Unit's current and past National Risk Assessments, and the current SRAs of the Reserve Bank of New Zealand (RBNZ) and the Department of Internal Affairs (DIA), which are the other supervisors of the Act. We have also considered guidance documentation from other jurisdictions and international organisations such as the Asia Pacific Group (APG) and the FATF (Financial Action Task Force), and typology reports. Information gathered in the course of the FMA's functions and activities as a supervisor of the Act has also been

considered. The SRA also takes into account the implementation of the Financial Services Legislation Amendment Act 2019 (FSLAA) and the impact on the original financial adviser sector (page 36) and the brokers and custodians sector (page 26).

Each of the ten sectors has been given one of the four risk ratings below. The rating is based on the assessment of the inherent risk of ML/TF. These ratings do not factor in the controls REs put in place to reduce ML/TF risks.

Low	Medium-low	Medium-high	High
-----	------------	-------------	------

The rating is based on a risk key, which has been applied to the data REs provided in their annual regulatory return, together with other information obtained for the sectors. The FMA has also observed an increase in the quality of the data provided in the annual returns. The overall sector ratings have not changed from the 2017 version.

Here is a snapshot of risk ratings for the ten sectors we supervise:

Sector	Sector risk 2021	Sector risk 2017
Derivatives issuers	High	High
Virtual Asset Service Providers	High	N/A
Provider of client money or property service (previously brokers and custodians)	Medium-high	Medium-high
Equity crowd funding platforms	Medium-low	Medium-low
Financial advice providers (FAPs)	Medium-low	Medium-low
Managed investment scheme managers	Medium-low	Medium-low
Peer-to-peer lending providers	Medium-low	Medium-low
Discretionary investment management services	Medium-low	Medium-low
Licensed supervisors	Low	Low
Issuers of securities	Low	Low

#### Our expectation is that REs:

- Review the updated SRA and information for their relevant sector
- Review their risk assessment
- Incorporate any new risks and findings into their assessment.

## Purpose of this Sector Risk Assessment

The purpose of this SRA is to identify and communicate the ML/TF risks faced by REs in the ten sectors we supervise. Identifying the risks is the first step towards combatting ML/ TF. This step is integral to putting a risk-based approach in place and allocating compliance resources effectively.

This SRA is for the following audiences:

#### REs

REs should review and consider this SRA when they prepare or update their risk assessments

#### Government, Financial Intelligence Unit, and other Supervisors

To contribute to the New Zealand Financial Intelligence Unit's National Risk Assessment and inform other supervisors – the Reserve Bank of New Zealand and Department of Internal Affairs

#### The FMA

Assessing the risks within each supervised sector enables the FMA to efficiently allocate our limited resources

#### Other organisations

Countries must ensure they have adequate anti-money laundering and countering financing of terrorism supervision in place, as recommended by the Financial Action Taskforce. This SRA contributes towards meeting these obligations.

## Key changes between the SRA 2017 and the SRA 2021

This SRA replaces the SRA 2017; however, the inherent sector risks identified in 2017 remain the same.

The main changes in the SRA 2021 methodology are:

- More detailed analysis of TF including material released by the FIU to reporting entities during 2019
- Considering amendments to the updated 2019 National Risk Assessment (NRA)
- The inclusion of virtual assets and virtual asset providers (VASPs)
- Considering the effect of increased use of online investment platforms

## Comments on the risk ratings

- Risk ratings in the SRA 2021 have not changed since the SRA 2017. The climate for REs, including customer base and methods of payment and delivery, has not changed significantly.
- FMA only supervises a small number of VASPs, and with the DIA being the primary supervisor for VASPs the risk rating as determined by the DIA in their VASP SRA is used in this SRA.
- Also, the FMA has access to considerably more information on REs, including through monitoring activity and reviews of audits REs must obtain under section 59(2) of the Act.
- Detail contained in the 2019 NRA has not increased or decreased the risk of ML/TF in any of the sectors supervised by the FMA.
- Providers of client money and property services continue to be rated as medium-high risk. Further

details around how some aspects of risk might differ between these two business types have been provided in the 2021 SRA to reflect the different functions between the businesses.

## How REs should use the SRA

- Review sections 1 to 7
- Review the section assessing your sector
- Review and update your own risk assessment.

### Review sections 1 to 7

All REs would find it helpful to read sections 1 to 7 on pages 7 to 20. This will help you understand the scope of the SRA, its limitations and any additions and changes to the findings since the 2011 and 2017 SRAs were published.

### Review your sector specific assessment

Each sector has a dedicated assessment (in section 8) covering specific risks, red flags and industry characteristics for you to review. We provide a list of common red flags that apply to all sectors, as well as specific red flags for each sector.

The ML/TF risks associated with individual REs may vary from the average risk rating for that RE's sector, and we provide a number of factors which play a part in lowering or raising the risks for entities in specific sectors. This should help you to understand where the FMA has identified higher-risk areas within the sector, and will help inform your own risk assessment (which must be tailored to your specific circumstances). For more detail, see Section 7 titled "How to interpret the data in this report" on page 20.

If you operate in more than one sector, you should review and apply all relevant risk assessments. The overall risk

will depend on a number of factors such as the ML/TF risk present and how much activity is carried out in each category.

Ultimately, REs will understand their business better than anyone else. You are best placed to identify and determine the risks your business faces from ML and TF, and whether your individual risk factors correspond to the factors identified in this SRA, and to develop adequate and effective procedures, policies, and controls to manage these risks.

### Review and update your own risk assessment

We expect you to review and update your own risk assessment with a view to incorporating any new risks identified in this SRA. For example, this can be incorporated into the annual review of the risk assessment or carried out as a standalone activity.

In our monitoring, we will look to see if you considered the SRA content, and then factored it into your risk assessment, as required by section 58(2)(g) of the Act. We will also review whether you have included references to new and/or updated supervisor guidelines – including the Explanatory Note: Electronic Identity Verification Guideline - For Part 3 - Amended Identity Verification Code of Practice 2013 - July 2021 – as well as the updated NRA published by the FIU in 2019.

You need to look at your policies, procedures and controls to examine if you are managing potential ML/TF adequately.

**It should be noted that the FMA risk rates each individual RE using data from the annual AML/CFT reports and other internal sources, for example monitoring activity and licensing.**

# Section 1 - Money laundering and terrorism financing risks in New Zealand

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

The Act came into full legal effect in June 2013. Its main purposes are:

- To detect and deter money laundering and the financing of terrorism.
- To maintain and enhance New Zealand's international reputation by adopting, where appropriate in the New Zealand context, recommendations issued by the Financial Action Task Force.
- To contribute to public confidence in the financial system.

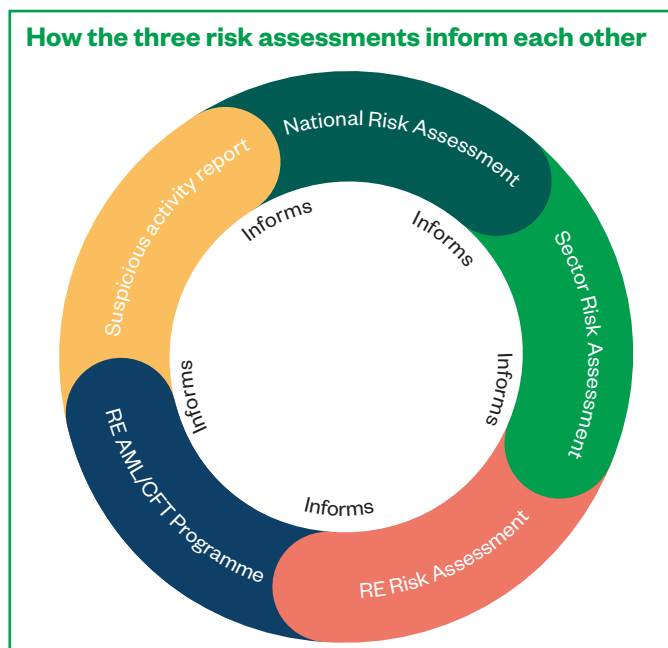
Under section 131 of the Act, each anti-money laundering and countering financing of terrorism supervisor has to assess the level of risk across all of the REs it supervises.

New Zealand has three levels of risk assessment, which review ML/TF risks from different perspectives. Together, the three assessments inform Government, supervisors and REs of potential risks, to help combat ML/TF. The three risk assessments combined provide a picture of the ML/TF risks New Zealand faces. See the diagram on the right for more detail on how the three assessments inform each other.

The three levels of risk assessment are:

### National Risk Assessment (NRA)

The NRA reviews ML/TF issues affecting the whole of New Zealand. It is based on information from suspicious activity reports (SARs) including suspicious transaction reports (STRs) and proceeds of crime asset recovery



data. Information from government organisations, both domestic and international, also contributes to the NRA. It provides a comprehensive overview of threats, vulnerabilities and crime trends.

We encourage REs to use the NRA to stay informed about emerging threats and trends. We suggest they share relevant case studies and predicate offences in staff anti-money laundering and countering financing of terrorism training. We have found that staff who understand the underlying crimes which lead to ML/TF have a greater desire to detect and deter ML/TF.

### Sector Risk Assessment

The three AML/CFT supervisors produce a risk assessment for their sectors. Our ongoing work aims to improve REs' understanding of the ML/TF sector risks, and to inform them of the risk indicators, trends and

emerging issues. This SRA will be reviewed from time to time to check how ML/TF risks affect the ten sectors we supervise.

### **Risk assessments by REs**

REs must carry out a risk assessment of ML/TF in their business. Section 58 of the Act sets out what is required in a risk assessment. This risk assessment must also take into account guidance material from their AML/CFT supervisor and the Financial Intelligence Unit. The SRA is part of our anti-money laundering and countering financing of terrorism guidance materials. We also encourage REs to access international anti-money laundering and countering financing of terrorism guidance – specifically the material produced by the Financial Action Taskforce and the Asia Pacific Group on Money Laundering.



## Section 2 - Methodology

---

This section sets out the type of information we considered, and the scope and limitations of this SRA. Understanding the methodology will help REs review and apply the findings of the SRA to their own risk assessment.

### Background information in the SRA

The following information helped inform our SRA:

- The National Risk Assessment 2019
- Other supervisors' risk assessments (Reserve Bank of New Zealand, Department of Internal Affairs)
- National and international guidance documentation, including publications from the Financial Action Task Force (FATF) and the Asia Pacific Group on Money Laundering (APG)
- FIU guidance on terrorism financing emailed to reporting entities in 2019
- Typology reports
- Annual AML/CFT regulatory reporting
- FMA monitoring and expertise
- REs' risk assessment data
- Discussions with industry representatives and consultants.

Each sector has been assessed against the variables set out in section 58(2) of the Act. This requires REs to assess:

- The nature, size and complexity of their business
- Product and services
- Delivery channels for products and services
- Customer types
- Country risk
- Institutions they deal with.

### Scope

We supervise ten sectors under the Act. These are:

- Derivatives issuers (DI)
- Virtual asset service providers (VASPs)
- Providers of client money or property service (previously brokers and custodians)
- Equity crowdfunding platforms
- Financial advice providers (FAPs)
- Managed investment scheme (MIS) managers
- Peer-to-peer lending providers
- Licensed supervisors
- Discretionary Investment Management Services (DIMS)
- Issuers of securities.

### Limitation

For consistency, when comparing sectors, we aimed to determine the likely inherent ML/TF risk. The risks faced by individual REs will vary from the sector average due to business-specific characteristics. The SRA does not assess residual risk – the assessed ML/TF risk after any controls or mitigations have been put in place. Reporting entities are responsible for determining the individual level of inherent ML/TF risk they face in their business and then applying the appropriate AML/CFT controls and determining their residual risk.

The SRA only rates the ML/TF risk by sector. However, the FMA does risk rate individual reporting entities within sectors using a “red flag” model. This is used for internal monitoring priorities.

## Risk scale

We applied the risk scale below to all variables set out in section 58(2) of the Act. We have not included a 'medium' risk category to ensure a clear position on the risk rating. For each sector we have rated the ML/TF risk as:



## Inherent risk

The risk that an activity would pose if no controls or other mitigating factors were in place.

The SRA evaluates inherent ML/TF risks.

Inherent risk disregards any controls an RE might have in place. This is deliberate, as these will vary significantly from RE to RE, and depend on their available resources and their commitment to reducing ML/TF risks.

## Vulnerability

This is described as a weakness that can be exploited for the purposes of ML/TF.

We have considered the key vulnerabilities across the sectors we supervise. This helps identify the sector risk(s).

These are:

- Complexity
- Liquidity
- Anonymity.

To see the full list of vulnerabilities, view the risk key on pages 11 to 12.

We assessed each sector individually by breaking it down into the variables in section 58(2) of the Act to determine the level of exposure to ML/TF risks.

The variables do not have an equal weighting. The overall rating assesses the importance of higher risk factors in the sector. We assumed areas showing a number of vulnerabilities, or a particularly strong vulnerability, will have a higher ML/TF risk.

## Exclusion of customer statistical information




We have excluded customer statistical information relating to FMA sector customers that are included in Designated Business Group (DBGs) which are supervised by the DIA or RBNZ.




## Section 3 – Risk key

The risk key below helps determine the main ML/TF vulnerability for each variable set out in section 58(2) of the Act.

The vulnerabilities are grouped into factors that may either increase or decrease a particular risk. This helps REs determine if their risk is higher or lower than the overall risk estimate for their sector. The effectiveness of an RE's policies, procedures and controls will also impact the overall risk.

REs need to keep this risk key top of mind when they review the individual sectors outlined in sector risk sections from page 21 onwards.

Variable	What increases the risk?	What decreases the risk?
 <p><b>Nature, size and complexity of business</b></p>	<ul style="list-style-type: none"> <li>• Large transactions</li> <li>• High volumes of transactions</li> <li>• Complex transactions</li> <li>• Large entity size can make implementing AML/CFT measures difficult</li> <li>• Rely on outsource service providers to perform key functions on behalf of RE</li> <li>• Small-sized entities may have less awareness of ML/TF</li> <li>• Insufficient staff</li> <li>• High staff turnover</li> </ul>	<ul style="list-style-type: none"> <li>• Low value of transactions</li> <li>• Low volume of transactions</li> <li>• Simple and transparent transactions</li> </ul>
 <p><b>Products / services</b></p>	<ul style="list-style-type: none"> <li>• High complexity</li> <li>• Highly liquid products/services</li> <li>• Large volume of products sold</li> <li>• High value products</li> <li>• Third-party payments</li> <li>• Commission-based selling, leading to conflicts of interest</li> <li>• Cash-based products and services</li> <li>• New payment technologies</li> </ul>	<ul style="list-style-type: none"> <li>• Low complexity</li> <li>• Low liquidity</li> <li>• Lock in periods</li> <li>• Low volume of products sold</li> <li>• Low value</li> </ul>
 <p><b>Delivery channel for products and services</b></p>	<ul style="list-style-type: none"> <li>• Anonymity</li> <li>• No face-to-face identity verification</li> <li>• No direct customer interaction</li> <li>• Due diligence carried out by other institutions</li> <li>• Due diligence carried out by offshore agents</li> <li>• Transactions carried out remotely</li> <li>• Digital advice</li> </ul>	<ul style="list-style-type: none"> <li>• Regular face-to-face contact</li> <li>• RE carries out customer due diligence – know your customer and your customer's business</li> </ul>

Variable	What increases the risk?	What decreases the risk?
 <b>Customer types</b>	<ul style="list-style-type: none"> <li>• Trusts and companies with complex structures</li> <li>• High net worth individuals</li> <li>• Foreign Politically Exposed Person (PEPs)</li> <li>• Individuals and entities that are subject to sanctions</li> </ul>	<ul style="list-style-type: none"> <li>• Stable well-known customer base with ongoing customer due diligence</li> <li>• Simple customer type (mainly individuals)</li> </ul>
 <b>Country risk</b>	<ul style="list-style-type: none"> <li>• Customers based in, controlled or owned by persons based in high-risk jurisdictions</li> <li>• Transactions designed for (or coming from) high-risk jurisdictions</li> <li>• Jurisdictions which have sanctions in place against them</li> <li>• Large overseas customer base</li> </ul>	<ul style="list-style-type: none"> <li>• Customers based in countries with robust AML/CFT systems</li> <li>• Transactions carried out in and/or with countries with sound AML/CFT systems</li> </ul>
 <b>Institutions dealt with</b>	<ul style="list-style-type: none"> <li>• Institutions with weak anti-money laundering and countering financing of terrorism controls</li> <li>• Overseas institutions with unknown anti-money laundering and countering financing of terrorism measures</li> </ul>	<ul style="list-style-type: none"> <li>• Domestic or overseas institutions with robust anti-money laundering and countering financing of terrorism measures</li> </ul>

## Virtual assets

Since the 2017 SRA was published, ML/TF risks associated with virtual assets (VAs, also known as cryptocurrencies, tokens, or crypto-assets) and virtual asset service providers (VASPs) have become more prominent. VAs are vulnerable to misuse by criminals to launder money and fund terrorism as they allow greater levels of anonymity and have global reach, making it easier for cross-border payments to be made, and can be traded easily. This has led to the inherent ML/TF risk of VASPs being assessed as high.

If you are providing financial services in relation to virtual assets in New Zealand, you will likely be classed as a 'VASP' and captured as a 'financial institution' under the AML/CFT Act. Obligations under the Act will apply. The [DIA has prepared detailed guidance](#) to help businesses determine whether they are a VASP, and how the obligations under the AML/CFT Act apply.

The primary supervisor of VASPs is the DIA; the FMA supervises a very small number of VASPs. The supervisor of a VASP is dependent on the specific activities undertaken by that VASP. VASPs that are unsure of who their supervisor is should contact the DIA in the first instance.

**We expect all REs to familiarise themselves with the risks and vulnerabilities associated with VASPs and virtual assets, and incorporate this into your risk assessments where appropriate. At a minimum, REs should closely read the DIA's sector risk assessment and guidance on VASPs.**

The FMA also recommends reporting entities review the following:

- [Guidance produced by FATF related to VASPs](#), and the steps regulators may take to ensure ML/TF risks are mitigated through the adoption of FATF standards.
- The FMA's [guidance on virtual assets](#), which also includes information about registration on the Financial Service Providers Register and other obligations that may apply.

## Section 4 – Potential red flags

---

Red flags indicate unusual customer activity and should prompt an RE to carry out further investigation. The following red flags come from different sources and could occur in the sectors we regulate.

### At the start of the customer relationship

- Customer is nervous and reluctant to provide identity documents
- No connection between customer's place of residence and the financial institution
- The information a customer provided does not align with information from other sources
- Customer has unexplained wealth inconsistent with their economic situation
- A wholesale customer who is an inexperienced investor
- Customer has complex trust or other legal arrangements which aim to hide beneficial ownership
- Customer resides in a high-risk country rated by international sources such as Financial Action Task Force or Transparency International; and has no logical geographic connection to New Zealand
- Customer seems to be acting for an undisclosed third party

### During the customer relationship

- Unusual or unexplained lump sums added to an account which do not align with the customer's known wealth
- Unusual settlements – such as third-party cheques sent for no apparent reason
- Transactions that lack economic sense such as buy and sell orders with little gain or loss to give the impression of account activity
- Investments are quickly followed by sales or transfer of assets

- Customer who keeps losing money and replenishes the account in excess of their known wealth
- Customer's investments are inconsistent with their investment profile
- Previously dormant accounts suddenly have unexplained wire transfer activities
- A new customer who introduces other high-net worth customers shortly after onboarding
- Cash is added to an account and withdrawn shortly after, with no trading
- Customer age does not align with the investment or trading behaviour – they could be used as a mule (very young or older customer)
- Customer's wealth is not aligned with their known background
- Customer makes large or structured cash deposits into the RE bank account to facilitate investment.

### Ending a customer relationship

- An account is only used for one transaction, contrary to its normal use
- Customer closes their account after being asked to provide additional customer due diligence documents (like source of funds)
- Customer requests funds to be sent to a third-party account with no apparent connection, or to an overseas account

## Section 5 – Money laundering the proceeds of crime

---

### Stages of money laundering

Money laundering (ML) involves concealing the origins of funds or assets. There are three recognised stages of ML:

- **Placement:** Criminals introduce proceeds of crime into the financial system
- **Layering:** This occurs when the proceeds of crime are in the financial system. It can involve numerous transactions designed to confuse the tracing of funds to their original source
- **Integration:** This occurs when the funds become legitimate.

The sectors we supervise are most likely to be used in the layering and integration stages of ML.

### Predicate offences

Every ML offence is preceded by a criminal offence. This is called a predicate offence. Money laundering transactions will be structured to seem like legitimate transactions, even though the origin of the funds comes from criminal activity. Taking direction from overseas experience and the findings of the 2019 NRA, it is important that REs are aware of the full range of criminal offending that can lead to ML/TF activity.

#### Common predicate offences

The Financial Intelligence Unit publishes a list of predicate offences both domestically and internationally. The full list can be found in the FIU's Quarterly Typology Report – Predicate Offence.

The 2019 NRA identifies three common predicate offences:

- **Fraud:** This includes fraud in the wider economy and in the capital market sector (market manipulation)
- **Tax evasion:** REs need to send a suspicious activity

report (SAR) to the Financial Intelligence Unit for suspected tax evasion

- Drug offences.

Offences can be carried out either domestically or internationally, or both. In its Quarterly Typology Report on predicate offences, the FIU estimates that each year \$1.35 billion of proceeds generated from domestic predicate offences are laundered in New Zealand.

Three key overseas threat areas identified by the FIU are:

- Specific transnational organised crime groups where the group is linked to New Zealand. Offending of this sort is closely associated with overseas-based networks entering the New Zealand domestic 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 money 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.

REs do not have to identify or investigate the predicate offence when reporting a SAR. If an RE suspects a predicate offence is the source of the funds, this is enough to file a SAR.

## White collar crime

The sectors we supervise are generally expected to be the target of more sophisticated money launderers.

These criminals are often familiar with capital markets and their products, involved in elaborate fraud, or could be employees of financial institutions. Even though the criminal offending is more elaborate in these cases, the illegally obtained funds still require layering to appear legitimate.

Potential white collar crime indicators which warrant further investigation by REs are:

- The known source of income contrasts with the person's known lifestyle.
- Unusual 'lump sum' payments described as bonuses.
- Businesses succeeding in sectors which are declining or not scalable.

## The use of cash in money laundering

Many believe the offence of ML requires cash to be put into the financial system. However, depending on the stage of the process (placement, layering or integration) the proceeds of crime are often already in electronic form. Examples of this would be market manipulation, tax evasion and fraud.

The absence of cash does not lead to a lower ML risk. Some REs may see receiving funds electronically as low risk because the funds would originate from another financial institution such as a bank which will deposit the funds into the bank account of the RE or their custodian.

When they receive funds electronically, REs cannot rely on other financial institutions to carry out their customer due diligence, unless an explicit arrangement was agreed.

We expect our RE types would be used in the layering and integration stages of ML, where there was no placement of cash.

<b>Predicate offence</b>	<b>Placement</b>	<b>Layering</b>	<b>Integration</b>
Drug offences	Cash proceeds	Non-cash	Non-cash
Fraud	Non-cash	Non-cash	Non-cash
Tax evasion	Non-cash	Non-cash	Non-cash
Other	Cash and non-cash	Non-cash	Non-cash



## Section 6 – Terrorism financing

---

### Overview

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 this time. Even though a second terror attack occurred at LynnMall Auckland in September 2021, it does not significantly change the TF risk for New Zealand, which remains at 'medium'.

The 2019 NRA notes that while New Zealand is not considered a 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 FMA 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 the 2019 NRA.

Following the Christchurch Terror Attack, the FIU produced a guidance document titled "Terrorism Financing Indicators: Lone Actors and Small Cells". This was subsequently emailed to all reporting entities and should be considered when reviewing your own TF risks.

Terrorists require funding to achieve their goal of carrying out terrorist acts, and to fund their operations. These activities can be as simple as food or rental payments for terrorist fighters. The characteristics of terrorist financing are similar to ML in many respects. However, REs' focus in respect of TF has a different focus – preventing the criminal activity from occurring.

#### It is a criminal offence in New Zealand under the Terrorism Suppression Act 2002 to:

- Provide or collect funds to use in a terrorist act or give to an entity carrying out terrorist acts.
- Provide material support for use in a terrorist act or to an entity carrying out terrorist acts
- Knowingly deal with any property owned or controlled by a terrorist entity.
- Make financial services available to a designated terrorist entity.

TF, by its nature, can be difficult to identify. The source of funds can be both from legitimate and criminal sources, and often involves a low value of transactions. TF is therefore concerned with concealing the origin and the nature of the funded activity.

### Terrorism financing risk in our supervised sectors

The TF threat faced by New Zealand is rated 'medium' by international standards (see above for further information). The 2019 NRA reports that from 30 June 2013 (when the AML/CFT Act commenced), there has been a total of 330 Suspicious Activity Reports (SARs) received by the FIU that indicated a possible relation to terrorism financing. This is 0.46% of all SARs received. However, we expect our REs to stay vigilant to ensure they don't unwittingly fund terrorism.

The FIU has covered a number of TF typologies in its Quarterly Typology Report. The two main threats identified in the report are:

- Financiers of overseas groups in New Zealand
- Overseas-based groups seeking to use New Zealand as a conduit for funds.

Furthermore, the FIU directly communicated with REs in regard to other potential TF risks.

## Key indicators and red flags for terrorism financing

Below we identify some of the red flags that could indicate a link to TF. This list is not exhaustive and as part of their risk assessment we encourage REs to identify any other red flags they see in their business.

- A customer making fund transfers to multiple beneficiaries located in high-risk jurisdictions
- Individuals and/or businesses transferring funds to known terrorist entities or entities suspected of having links to terrorism or TF
- Multiple customers using the same address/telephone number to conduct account activity
- REs or individuals with connections to terrorist groups
- Setting up a New Zealand account with false identification
- Customers in or returning from conflict zones
- A sudden increase in account activity which is inconsistent with the customer profile, or transactional activity inconsistent with the nature and purpose of the customer's account
- Multiple low-value domestic transfers to one account
- Prescribed 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

## Emerging terrorism financing risk

The Financial Action Task Force recommends a forward-looking analysis for TF because the risks change rapidly.

Areas of potential risk are:

- Foreign terrorist fighters, defined by the United Nations Security Council Resolution 2178 as: "Individuals who travel to a state other than their states of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict."
- Foreign terrorist supporters – an entity or individual who provides financial assistance to, or otherwise supports, terrorists
- Fundraising using social media and new payment products and services
- New payment products and services

REs need to ensure their AML/CFT measures both adequately and effectively cover emerging TF. Their AML/CFT documentation should reflect this and include regular testing and validation.

## Proliferation

The FATF Proliferation Financing Report (2008) notes that proliferation has many guises, but ultimately involves the transfer and export of technology, goods, software, services or expertise that could be used in nuclear, chemical or biological weapon-related programmes, including delivery systems. If appropriate safeguards are not established, maintained, and enforced for sensitive materials, technology, services and expertise, they can become accessible to individuals and entities seeking to

profit from the acquisition and resale, or for intended use in weapons of mass destruction programmes. The FATF report 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 weapons 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.

The risk of proliferation and proliferation financing in New Zealand is low. However, REs should understand the role that proliferation and proliferation financing plays in ML/TF and ensure that their risk assessment has adequately addressed this where relevant.

## Section 7 – How to interpret the data in this report

---

### Inherent risk tables

Individual REs will vary to some degree from the sector, due to them having differing exposure to the factors set out in section 58(2) of the Act.

To allow REs to be flexible with how they apply the sector risk rating to their own business, we have provided a number of factors we think lower or heighten the risk of ML/TF for individual REs. This should provide REs with an understanding where we have identified potential higher or lower risk areas within the sector. It is important for REs to evaluate where their business differs from the sector generally, and rate their risks accordingly.

*For example: An RE has a large number of non-resident customers from higher-risk jurisdictions and the sector in general has little exposure to non-resident customers. Therefore the risk to the specific RE would be heightened in this area and the overall risk rating of the RE could be above the sector rating.*

### Timeframe

REs are required to file annual AML/CFT reports by 31 August each year, for the year ending 30 June. In this SRA we have used 2019/20 data provided to us by 31 August 2020. SAR information used is for the period 1 January to 31 December 2020. During that period, FMA reporting entities filed 233 STRs covering 1,102 transactions with a total value of \$155 million. SARs filed totalled 104.

Data collected from previous years has not been taken into account. This is due to our expectation that the sectors supervised by us now understand their filing obligations better than in previous years.

### Dataset

The total number of reporting entities in the data set used for this SRA is 764. Included in this are 74 designated business groups containing a total of 276 reporting entities.

A number of larger entities licensed under the Financial Markets Conduct Act 2013 (FMC Act) are naturally excluded from the data as they are supervised by the Reserve Bank of New Zealand. A number of entities are also excluded as they are members of designated business groups and based on their core business activities are supervised by the Department of Internal Affairs. The data in this report is therefore **not to be taken to represent the size of the licensed sector**, but the size of the FMA's AML/CFT supervised portion of the licensed sector.

A number of REs operate in multiple sectors that we supervise, such as DIMS providers that also offer MIS and broker services. Where REs operate in multiple sectors their information was taken into account in each sector, unless specified otherwise. **The total values contained in this report will therefore exceed the actual total values of the sectors supervised by us.**

Where we found sector data did not align with the other information we hold about REs, such as licensing, we questioned the analysis or in some cases decided to override the data, given our knowledge of the sector.

While we have made an effort to identify where REs have misinterpreted the filing requirements, the data has not been analysed for its validity and we have mostly taken REs to have filed a true representation of their businesses.

For presentation purposes the numbers have been rounded.

## Section 8 – Sector risks

---

## Derivatives issuers

### Introduction

At the date of this publication, New Zealand has 25 derivatives issuers licensed to offer derivatives to retail investors. Five are registered banks and are supervised by the Reserve Bank of New Zealand for AML/CFT; four are money remitters/foreign exchange entities and are supervised by the Department of Internal Affairs, two currently have their licences suspended by the FMA and two requested that FMA cancel their licences. We supervise the remaining 12 REs.

REs describe their business in their licence applications, which helps us group DIs into the following categories:

- Banks – not supervised for AML/CFT by us; not included in this report
- Trade related – REs who transact foreign currency or options
- Speculative – REs who trade derivatives.

The derivatives market is highly attractive to money launderers as it offers:

- High liquidity
- High frequency of trading
- Easy access to the market via online account opening and online trading and
- A global marketplace.

In July 2020, the FMA published a [DI Sector Risk Assessment](#). This identifies key risks in the DI sector that REs should consider. There was nothing in this report that would impact our risk rating of this sector.

This sector filed 136 STRs covering 188 transactions and 10 SARs for the year ending 31 December 2020 – a significant increase from the 2017 SRA.

### Red flags

The following red flags are a starting point for REs to consider in their risk assessment and compliance programme. It should not be seen as an exhaustive list of unusual customer activity. Red flags should trigger an RE to investigate its customer activities further, and where appropriate file a SAR.

These are:

- Frequent trading in and out of positions with little gain/loss
- Using cash accounts to ‘park’ money (adding funds into an account without trading)
- Adding cash to an account and withdrawing it soon after without trading
- Dormant accounts that become active
- A customer who keeps losing money and replenishes their account, where the amount and frequency is inconsistent with the known wealth of the customer
- Third-party payments or deposits
- The age of the customer is not in line with their trading behaviour and could be an indication of someone being used as a mule (very young or older customer)
- Multiple customers signed up from, or registered at, the same IP address.
- Use of cryptocurrency to disguise origin of funds or to maintain anonymity of customer.

# 25



**Derivatives issuers**  
(12 supervised by the FMA)

**29,000**  
customers

**\$309 billion**  
total transaction value

## Inherent risk summary

Variable	Factors increasing risk	Factors decreasing risk
<p><b>Nature, size and complexity of business</b></p>	<ul style="list-style-type: none"> <li>REs aimed at speculative online based trading.</li> </ul>	<ul style="list-style-type: none"> <li>REs offering derivatives for risk management purposes only and to a known customer base.</li> </ul>
<p><b>Products / services</b></p>	<ul style="list-style-type: none"> <li>Online accounts for speculative trading.</li> <li>Third party deposits or payments.</li> <li>Acceptance of credit cards for payments.</li> </ul>	<ul style="list-style-type: none"> <li>Fit-for-purpose information technology systems.</li> </ul>
<p><b>Delivery channel for products and services</b></p>	<ul style="list-style-type: none"> <li>No face-to-face onboarding of customers.</li> </ul>	<ul style="list-style-type: none"> <li>Customer relationship model with regular customer contact.</li> </ul>
<p><b>Customer types</b></p>	<ul style="list-style-type: none"> <li>REs with large customer base compared to the size of the RE.</li> <li>Foreign PEPs.</li> </ul>	
<p><b>Country risk</b></p>	<ul style="list-style-type: none"> <li>Customers based in high-risk countries, or customers who are controlled by or owned by people in high-risk jurisdictions.</li> <li>REs with large non-resident proportion of their customer base.</li> </ul>	
<p><b>Institutions dealt with</b></p>	<ul style="list-style-type: none"> <li>Unregulated institutions in high-risk countries.</li> </ul>	<ul style="list-style-type: none"> <li>Subject to effective regulation.</li> <li>Located in low-risk countries.</li> </ul>
<p><b>Overall risk</b></p>	<p>The ML/TF risk of the sector has been rated as high, based on:</p> <ul style="list-style-type: none"> <li>The high liquidity of the products offered</li> <li>The ease of opening accounts</li> <li>Limited face-to-face customer onboarding</li> <li>Large number of non-resident customers in higher-risk jurisdictions.</li> </ul>	

## Sector-specific risks



### Nature, size and complexity of business

**Risk rating: High**

DIs who make regulated offers of derivatives to New Zealand retail investors are required to be licensed under the FMC Act, which has improved the information and oversight we have of the sector. REs in this sector vary greatly in size, from small entities to those with a global footprint. Their ownership is often concentrated in a small number of offshore-based individuals or entities.

Derivatives markets are characterised by fast-paced transactions with a global reach. The REs we supervise carry out large volumes of transactions per year, but this is dominated by just four REs.

The sector relies heavily on advanced information technology, which is changing rapidly each year. This brings challenges for REs to maintain their compliance capabilities in line with changes to their trading platforms.



### Products and services

**Risk rating: High**

DIs offer their customers a range of derivative products, which are highly complex and often involve leverage.

From licence applications, we see the DI sector we supervise falls into two distinct categories:

- REs offering speculative trading, often online with no customer interaction or contact

- REs facilitating risk management for businesses that mostly have a need to hedge against currency movements.

In our view, allowing speculative trading increases the risk an RE faces, because a customer's trading patterns can be unknown and unusual.

The average trading amount appears to be low when taking into account minimum trade size as well as the use of leverage in this sector. This could be a reflection of a higher involvement of retail investors in the sector than previously estimated, which could make it more attractive for ML.

The overall transaction value of \$323 billion is high, but this is dominated by one RE that accounts for 68% of the transactional value.

DI trading requires at least one account holding cash as collateral. Customers can add or withdraw funds from these accounts, while maintaining the required balance. This presents a heightened risk of ML.




### Delivery channel for products and services

**Risk rating: High**

Only one RE indicated that they on-board more than 50% customers face-to-face, with the remaining REs indicating they on-board customers using channels other than face-to-face. Only one RE told us they use overseas intermediaries. REs with a larger customer base and high transaction volume use electronic transaction monitoring methods and small REs use a mixture of electronic and manual.




Trading is frequently carried out through online platforms, which customers access anywhere in the world. We understand that trade-related derivative trading follows a more traditional relationship model and frequent phone contact with customers is common.



**Customer types**

**Risk rating: High**

The DI sector mainly transacts with individuals who often engage in speculative trading. The number of trust and other legal arrangements is relatively low at just over 1%. Only two REs indicated they have a PEP as a customer; one with 1 PEP and the other with 2 PEPs.



**Country risk**

**Risk rating: High**

The DI sector has 49% non-resident customers, the highest percentage of any of the sectors we supervise – with one RE accounting for 85% of these. The sector ranges between REs with no non-resident customers and one that has close to 100% non-resident customers. The bulk of the non-resident customers are with three REs.

Information on country risk ratings comes from a number of information sources including the Financial Action Task Force, Transparency International, the United Nations Office on Drugs and Crime, and open source media.



**Institutions dealt with**

**Risk rating: Low**

The DI sector deals with institutions based largely in low-risk countries.

## Providers of client money or property service (Brokers and custodians)

### Introduction

The FMC Act, as amended by FSLAA, now defines “brokers and custodians” as “providers of client money or property services”. The definition states that a “client money or property service”:

- a. Is the receipt of client money or client property by a person and the holding, payment, or transfer of that client property; and
- b. Includes a custodial service.

### Providers of client money or property services (as a provider of services under (a) above)

These REs, previously referred to as brokers, are financial service providers that hold, transfer or make payments with client money or property for their customers.

Providers are not licensed under the FMC Act. Their business activity itself defines them as brokers.

Providers can include NZX market participants, providers of portfolio administration services, and financial advisers who receive property or money from customers.

The obligations of providers apply whether they have retail or wholesale customers; and also apply custodians of client money and client property.

NZX market participants are a subset of providers. An NZX market participant is a business accredited by New Zealand’s main licensed market operator, NZX Limited, to participate in, and trade listed financial products on, the markets NZX operates. NZX participant types include NZX trading and advising firms, and NZX clearing and

depository participants. There are currently 32 NZX market participants which are, in addition to general obligations under the FMC Act and other laws, subject to the NZX rules (which include requirements around ‘good broking practice’) and to supervision by the NZX. Only eight of these firms are accredited to trade on the NZX. The balance can place securities trades through the eight trading participants. A number are accredited for other activities that do not involve direct securities trading.

Four NZX accredited firms are banks and supervised by the Reserve Bank for AML/CFT obligations.

The nature of the sector is often fast paced, and includes share trading, initial public offers, bond issues and other financial products. Most providers appear to offer a mixture of trade execution services, as well as a more traditional portfolio management model through Financial Advice Providers (FAPs).

This sector filed 27 STRs, covering 436 transactions, and 111 SARs for the year ending 31 December 2020. Due to the highly liquid products providers deal with and the fast-paced nature of the business, we see a heightened risk for ML/TF in this sector.

There has been a rapid increase in the use of online investment platforms that enable customers to trade shares and other financial products online. These platforms generally onboard large numbers of customers through non-face-to-face methods, which can favour anonymity and therefore increase the risk of ML and TF. Online investment platforms often have technology solutions in place to conduct account monitoring. However, to ensure these are effective in identifying ML

and TF the platform must collect sufficient information regarding the nature and purpose of the investment, and ensure appropriate trigger levels and volumes of alerts are in place for the customer base. The platforms give customers access to products that are generally highly liquid, allowing for high volumes of trading to take place without suspicion, increasing the risk of ML and TF. The rapid growth of these platforms may also increase risk of ML and TF due to a potential lack of compliance and operational resources for AML/CFT purposes. The risk of ML with use of online investment platforms to launder stolen funds has also been identified in the United States - see [Fraudsters are laundering millions in Covid relief funds through online investment platforms](#).

### **Providers of custodial services**

Providers of custodial services, previously referred to as custodians, hold money or property on trust for their customers and perform a key function in safeguarding investors' assets. Many also deliver other services such as administration, reporting and record keeping.

The FMC Act prescribes a segregation of duties in relation to retail managed investment schemes that are covered by the FMC Act. Generally, while the manager of the scheme is responsible for the investment strategy, the provider of custodial services is responsible for holding and safeguarding the scheme assets (segregation of legal ownership) and for keeping records on the scheme assets. Under the FMC Act, licensed supervisors (covered later in this SRA) are responsible for custody. Depending on the scheme's governing documents, a licensed supervisor

may appoint another appropriate independent person as custodian.

The FMC Act and Regulations do not apply to wholesale funds. Wholesale funds are investment funds that do not offer investment services to retail clients.

Factors that reduce the ML/TF risk for providers of custodial services:

- Providers hold the assets of a fund or other form of investment in trust on behalf of the investors
- Providers generally do not have direct interaction with customers
- Providers act on instructions from the fund manager, such as to invest the funds into various assets or to pay out a customer on redemption, e.g. for KiwiSaver and superannuation schemes.

Where a provider of custodial services acts on instruction from another financial institution, we see little ML risk. Providers who take instructions from customers who are not financial institutions have the same ML/TF risk as providers of client money or property services.

In December 2019, the FMA released a [findings paper on MIS custody](#). While this paper did not change our risk rating of the sector, it gives a good understanding of the custodian responsibilities.

For the year ending 31 December 2020, this sector filed 1 STR covering 17 transactions, and no SARs.

Overall we would rate providers of custodial services as lower risk than other providers in this sector.

## Red flags

The following red flags are a starting point for REs to consider in their risk assessment and compliance programme. It should not be seen as an exhaustive list of unusual customer activity. Red flags should trigger an RE to investigate its customer activities further, and file a SAR where appropriate.

These are:

- Unusual settlements, for example, payments requested to third parties with no apparent connection to the customer
- Funds deposited into a customer account by a financial adviser and paid back to the customer on the same day or the following day, occurring multiple times over a period of time
- Funds deposited into provider's account followed immediately by requests for repayment
- Frequent changes to customer details
- Securities accounts opened to trade in shares of only one listed company
- Transaction patterns resembling market manipulation or insider trading
- Intra-day trading with no economic benefit
- Transactions outside of settlement systems
- Shares bought with one provider of money or property services and sold through a different provider of money or property services
- Off-market share transfers.

# 81

**Providers of client money  
or property service**



**975,000**  
customers



**\$582 billion**  
total transaction value

## Inherent risk summary

Variable	Factors increasing risk	Factors decreasing risk
<b>Nature, size and complexity of business</b>	<ul style="list-style-type: none"> <li>Over-reliance on third parties for customer due diligence.</li> </ul>	
<b>Products / services</b>	<ul style="list-style-type: none"> <li>Third-party deposits or payments.</li> </ul>	<ul style="list-style-type: none"> <li>Custody for other financial institutions.</li> </ul>
<b>Delivery channel for products and services</b>	<ul style="list-style-type: none"> <li>Non face-to-face onboarding of customer.</li> </ul>	<ul style="list-style-type: none"> <li>Face-to-face onboarding of customers.</li> </ul>
<b>Customer types</b>	<ul style="list-style-type: none"> <li>PEPs.</li> <li>Trust and other legal arrangements</li> </ul>	<ul style="list-style-type: none"> <li>Financial institutions.</li> <li>Nature of trust e.g. small family trust</li> </ul>
<b>Country risk</b>	<ul style="list-style-type: none"> <li>Non-resident customers.</li> </ul>	<ul style="list-style-type: none"> <li>Domestic customer base.</li> </ul>
<b>Institutions dealt with</b>	<ul style="list-style-type: none"> <li>Unregulated institutions.</li> </ul>	
<b>Overall risk</b>	<p>The ML/TF risk of the sector has been rated as medium-high. This reflects the liquidity of the products, the anonymity that no face-to-face onboarding brings, and the high concentration of trust and other legal arrangements, and non-resident customers.</p>	

## Sector-specific risks



### Nature, size and complexity of business

**Risk rating: Medium-high**

The size and complexity of the sector ranges from small FAP businesses to entities operating on a global scale. Most larger entities will be licensed for some other FMC Act activity e.g. DIMS or MIS.

The transactional volume of the sector is significant, at \$582 billion for the year ended June 2020. Transaction volumes in this sector are high, which we attribute mainly to providers of custodial services. Overall transactions per customer are high, especially with providers, which supports our understanding of the fast-paced nature of the sector.

Transaction monitoring is carried out manually by four entities only, which is a reduction since the 2017 SRA.



### Products and services

**Risk rating: High**

Products and services offered by providers of client money or property services are generally highly liquid, such as shares, bonds, foreign exchange, managed funds and distribution of initial public offers. The high liquidity possibility of frequent trading without raising suspicion makes the sector vulnerable to ML. Individual products or entire portfolios in this sector can be transferred to other institutions both on- and off-shore, which can hinder efforts to trace the source of the funds.



### Delivery channel for products and services

**Risk rating: Medium-low**

The sector uses both face-to-face and non-face-to-face onboarding. A larger proportion of REs use a combination of both face-to-face and non-face-to-face onboarding methods. We understand that providers with a customer relationship model are more likely to onboard customers face-to-face. The use of online trading systems has become more common, which has decreased face-to-face onboarding over time, as seen in other sectors that are based entirely online.

Two REs in the sector have indicated using overseas intermediaries to onboard customers, with around 20% of entities utilising domestic intermediaries for onboarding.



### Customer types

**Risk rating: Medium-high**

The sector has a relatively high percentage of trust and other legal arrangements, though sector feedback and observations from onsite monitoring of providers by the FMA indicates that a large portion of New Zealand established trusts are small family trusts with beneficiaries who are family members e.g. children or grandchildren. Non-residents make up around 17% of the customer base, and while 32% of REs have reported having one or two foreign PEPs on their books, two of these have reported 11 and 13 PEPs respectively. One-off transactions are not uncommon in the provider sector and are a higher risk for ML/TF.



### Country risk

**Risk rating: Medium-high**

The reported 17% of non-resident customers come from a variety of countries. These include Australia, China, United Kingdom, United States, United Arab Emirates, Fiji, Israel, Singapore, Hong Kong, Russian Federation, and Swaziland.

Information on country risk ratings can be found from a number of information sources, including the Financial Action Task Force, Transparency International, the United Nations Office on Drugs and Crime, and open source media.



### Institutions dealt with

**Risk rating: Low**

Providers of client money or property services mainly deal with institutions and intermediaries based in low-risk countries that are regulated by their home jurisdiction.

## Equity crowdfunding platforms

---

### Introduction

An equity crowdfunding service is an RE acting as an intermediary between companies issuing shares and potential investors. The crowdfunding service provides the facility (such as a website) for the offer to go public. Charitable or philanthropic fundraising, with no shares involved, is not equity crowdfunding. Crowdfunding has now been operating for a number of years, and has increased in customer numbers and value of transactions since the 2017 SRA.

For most companies there is currently no secondary market for these shares. This means that liquidity after the initial purchase is close to zero. This feature makes it unattractive to money launderers.

Equity crowdfunding platforms have been used to raise a portion of capital in New Zealand for ASX initial public offers by overseas companies. In this situation there is a secondary market, which significantly increases the ML risk.

There were no STRs or SARs filed in the year ending 31 December 2020.

### Red flags

The following red flags are a starting point for REs to consider in their risk assessment and compliance programme. It should not be seen as an exhaustive list of unusual customer activity. Red flags should trigger an RE to investigate its customer activities further, and, where appropriate, file a SAR.

These are:

- Borrower and lender share the same address or are somehow closely linked
- Issuers cancel a share issue and return funds to investors
- Browser cookies indicate a customer with a New Zealand address is arranging transactions from overseas
- Many customers sign up from one IP address



# 6

**Licensed equity crowdfunding services**



**19,847**  
customers



**\$45.6 million**  
total transaction value

## Inherent risk summary

Variable	Factors increasing risk	Factors decreasing risk
<p>Nature, size and complexity of business</p>		
<p>Products / services</p>	<ul style="list-style-type: none"> <li>Offer with short-term exit strategy (initial public offers).</li> </ul>	
<p>Delivery channel for products and services</p>		
<p>Customer types</p>	<ul style="list-style-type: none"> <li>Foreign PEPs.</li> </ul>	
<p>Country risk</p>	<ul style="list-style-type: none"> <li>Non-resident issuers/investors.</li> <li>Customers from high-risk jurisdictions.</li> </ul>	
<p>Institutions dealt with</p>	n/a	n/a
<b>Overall risk</b>	The ML/TF risk of the sector has been rated as medium-low. For most share issues in the sector there is no liquidity after the initial purchase, making it unattractive for ML/TF.	

## Sector-specific risks



### Nature, size and complexity of business

**Risk rating: Low**

Transaction volumes are still relatively low, as was identified in the 2017 SRA. Transaction monitoring is carried out manually by one RE; the remainder of REs have indicated they utilise a combination of both manual and electronic transaction monitoring. This seems to align with the nature of the sector, which is generally a customer making a single investment into an offer. Generally, monitoring would mainly be for customers who make multiple investments into different offers.



### Products and services

**Risk rating: Medium-low**

Equity crowdfunding platforms offer a single service, which is to match buyers with entities aiming to raise funds. Customers appear to only transact once, with an average investment value of \$12,000, a slight increase from 2017. As set out earlier, we see little opportunity to utilise the sector for ML/TF due to its illiquid nature, except in the offers which raise funds for an exchange such as the NZX or ASX.



### Delivery channel for products and services

**Risk rating: Medium-high**

Crowdfunding services only accept customers via non face-to-face methods, as the service is based online. Based on the information provided from the sector, we understand that no third-party channels are used and all customers interact directly with the REs. While non-face-to-face onboarding facilitates anonymity, in the context of the equity crowdfunding sector and its lack of liquidity, we consider this to only moderately increase the risk of ML/TF.



### Customer types

**Risk rating: Low**

The sector has less than 1% exposure to trusts and other legal arrangements, and no REs reporting PEP customers.



### Country risk

**Risk rating: Low**

The sector reports 57% of its customers are non-residents, but it should be noted that 56% of non-resident customers are with one RE. These customers come from Australia, United Kingdom, Singapore, China, Netherlands, Canada, India and United States of America.

More information on country risk ratings can be found from a number of information sources, including the Financial Action Task Force, Transparency International, the United Nations Office on Drugs and Crime, and open source media.

	<b>Institutions dealt with</b>
<b>Risk rating: n/a</b>	

Not applicable.

# Financial Advice Providers

---

## Introduction

This section has been updated to include the changes to the financial advice sector following the implementation of the new financial advice regime on 15 March 2021.

The Financial Advisers Act 2008 was repealed and the Financial Markets Conduct Act 2013 (as amended by the Financial Services Legislation Amendment Act) now sets out the requirements that apply to providers and individuals. Among the changes, the new regime removes the previous terms of Authorised Financial Adviser, Registered Financial Adviser and Qualifying Financial Entity, and introduces licensed Financial Advice Providers (FAPs), as well as financial advisers, authorised bodies, and nominated representatives, which may provide advice on behalf of a FAP.

For the purposes of this SRA, a FAP is considered to be a reporting entity if it arranges relevant services and products for their customers. Changes to the FMC Act also introduced Authorised Bodies (ABs), which might be REs. This type of entity has not been specifically considered in this version of the SRA. RE should familiarise themselves with Regulation 16 of the Anti-Money Laundering and Countering Financing of Terrorism (Definitions) Amendment Regulations 2020, which updates Regulation 16 of the 2011 (Definitions) Regulations. [See our FAQs](#) for more detail about when a FAP is a reporting entity.

As of 15 March 2021, 1,765 transitional FAP licences had been approved by the FMA.

At this stage, we do not consider that these changes affect the overall risk rating for the sector. This section will be updated within the next 12 to 18 months when there is a

clearer overall picture of the number and type of FAPs and ABs that will be reporting entities for AML/CFT purposes.

There were 7 STRs covering 40 transactions, and 8 SARs filed for this sector for the year ending 31 December 2020.







## Red flags

The following red flags are a starting point for REs to consider in their risk assessment and compliance programme. It should not be seen as an exhaustive list of unusual customer activity. Red flags should trigger an RE to investigate its customer activities further, and, where appropriate, file a SAR.

These are:

- Reluctance to provide customer due diligence documentation
- Customer investments are inconsistent with the investment profile
- Lump sum additions out of alignment with known source of income
- Structuring to achieve anonymity without clear reasons
- Rapid change of products
- Withdrawals are made shortly after deposits
- Customer seems to be indifferent to losses
- A new customer who introduces other high net worth customers shortly after onboarding
- No logical geographic connection between where the customer lives and where the adviser is based
- The investor wants to be 'wholesale' but the amount or wealth does not meet the wholesale investor classification.

## Inherent risk summary

Variable	Factors increasing risk	Factors decreasing risk
 <b>Nature, size and complexity of business</b>	<ul style="list-style-type: none"> <li>• Dependency on one or several high-value customers.</li> <li>• Small entity size leading to lack of ML/TF awareness.</li> </ul>	<ul style="list-style-type: none"> <li>• Low volume or value of transactions.</li> <li>• Trading through large product providers or investment platforms that have an additional layer of AML/CFT requirements.</li> </ul>
 <b>Products / services</b>	<ul style="list-style-type: none"> <li>• Commission-based remuneration.</li> <li>• Emergence of digital (robo) advice allowing for anonymity.</li> <li>• High net worth customers demanding complex products.</li> <li>• Third-party payments.</li> </ul>	<ul style="list-style-type: none"> <li>• Providing products with lock-in periods and additional identity verification requirements</li> </ul>
 <b>Delivery channel for products and services</b>	<ul style="list-style-type: none"> <li>• Customers accepted via non face-to-face channels.</li> <li>• Emergence of digital (robo) advice allowing for anonymity.</li> </ul>	<ul style="list-style-type: none"> <li>• Most customer interactions are face-to-face.</li> <li>• Stable customer base with customers personally known to the adviser.</li> </ul>
 <b>Customer types</b>	<ul style="list-style-type: none"> <li>• Trusts and other legal arrangements. Foreign PEPs.</li> </ul>	
 <b>Country risk</b>	<ul style="list-style-type: none"> <li>• Large number of trusts and other legal arrangements.</li> <li>• Non-resident customers in jurisdictions with weak AML/CFT frameworks.</li> <li>• Offshore customers combined with trusts and other legal arrangements.</li> </ul>	<ul style="list-style-type: none"> <li>• Local customer base with known wealth management requirements.</li> </ul>
 <b>Institutions dealt with</b>	<ul style="list-style-type: none"> <li>• Unregulated institutions.</li> </ul>	<ul style="list-style-type: none"> <li>• Products are provided through licensed (regulated) financial institutions</li> </ul>
<b>Overall risk</b>	<p>The ML/TF risk of the sector has been rated as medium-low. The sector has a number of vulnerabilities which make it susceptible to ML/TF. These risks are mitigated as FAPs and ABs have enduring and in-depth relationships with their customers. This is helped by the information FAPs and ABs gather when they onboard their customers.</p>	

## Sector-specific risks



### Nature, size and complexity of business

**Risk rating: Low**

A large number of REs represented in this sector are small businesses, often sole traders, with the number of customers limited by the size of the business. The lack of resources of both time and funds can lead to reduced awareness of emerging ML/TF risks within the sector, which increases the ML/TF risk and could also be reflected in the low volume of STRs and SARs filed.

We note the transaction volume is relatively low, with an average number of eight transactions per customer. This is in line with the long-term nature of the products offered by the sector.



### Products and services

**Risk rating: Medium-high**

FAPs and ABs provide advice generally aimed at long-term wealth accumulation and retirement savings. The products sold are shares, bonds or funds purchased through investment platform providers or brokers. These products are generally liquid, and therefore increase the risk of ML. A number of FAPs will also be licensed DIMS providers, covered in a separate section in the SRA.



### Delivery channel for products and services

**Risk rating: Low**

Most REs onboard new customers face-to-face, which lowers anonymity and therefore reduces the ML/TF risks. Robo-advice is a factor which could significantly change the way advice is delivered.



### Customer types

**Risk rating: Medium-high**

FAP customers are often high net worth individuals. The reported number of trusts and other legal arrangements as customers is still relatively low, given the overall number of trusts established in New Zealand.

In the June 2020 annual returns, only 7% of REs told us they have PEP customers. This is lower than we expected from international guidance material, but still in line with the low number of non-resident customers.



### Country risk

**Risk rating: Low**

Customers in this sector are based mainly in New Zealand, with less than 1% being non-residents. These appear to be mostly New Zealanders who moved offshore

and who have chosen to retain their financial affairs with their New Zealand-based FAP, with the most common countries being Australia, United Kingdom, United States, and Singapore. These offshore customers appear to be concentrated in a number of firms that have specialised in servicing offshore customers.

Information on country risk ratings can be found from a number of information sources including the Financial Action Task Force, Transparency International, the United Nations Office on Drugs and Crime, and open source media.



**Institutions dealt with**

**Risk rating: Low**

FAPs and ABs generally invest through licensed fund managers, NZX-brokers and investment platforms based in New Zealand.

## Managed investment scheme (MIS) managers

### Introduction

There are currently 69 MIS managers licensed to offer funds to retail investors, four of which are supervised for AML/CFT by the Reserve Bank of New Zealand. From the 2020 annual returns, a further 68 identified as wholesale MIS. Both retail and wholesale MIS managers are REs.

A MIS manager pools money from a number of investors, who rely on the investment expertise of the scheme manager. These schemes can be structured in different ways, and may invest in a wide range of investments.

They can be open-ended (offered continuously) or close-ended (more equity-like).

Examples include:

- Open-ended – open-ended unit trusts, KiwiSaver, superannuation, workplace savings schemes, and other schemes that invest in relatively liquid assets.
- Closed-ended – forestry partnerships and property syndicates that invest in a single asset class.

The population is dominated by a few large entities, particularly in the unit trust and KiwiSaver categories.

It should be noted however that some of the larger MIS managers providing KiwiSaver are registered banks. These entities are supervised by the Reserve Bank of New Zealand and therefore not included in this analysis.

MIS managers filed 58 STRs covering 416 transactions, and 7 SARs for the year ending 31 December 2020, an increase from the 2017 SRA. We see this as a reflection of the higher sophistication of REs as well as the way in which SARs are identified and reported. Sectors that have a higher number of REs that operate across multiple sectors are more likely to have an increased share of the overall SAR filings. While it could also be a sign of a higher ML/TF risk, we are of the view that it is more likely attributable to the amount of resources MIS managers

have dedicated to their AML/CFT efforts, and the access to worldwide databases this provides. The FMA and FIU have also been proactive in educating this sector.

### Red flags

The following red flags are a starting point for REs to consider in their risk assessment and compliance programme. It should not be seen as an exhaustive list of unusual customer activity. Red flags should trigger an RE to investigate its customer activities further, and where appropriate file a SAR.

These are:

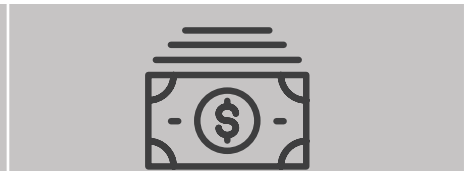
- Buying and selling units in quick succession that do not align with customers' stated investment purpose
- Large KiwiSaver contributions shortly before reaching retirement age
- Lump sum payments which don't match the customer's profile
- Customer transfers fund balance to another provider when asked for additional customer due diligence information
- Funds introduced from offshore
- Increase of fund contributions, particularly lump-sum contributions, out of alignment with known customer profile
- Spouse appears to be unaware of an account in their name
- Account in children's names (excluding KiwiSaver)
- Gifting of units
- Third-party payments
- Holding a large portion of funds in long-term cash portfolios/accounts and/or withdrawal prior to investment.



**69** Licensed MIS



**1,300,000**  
customers



**\$80 billion**  
total transaction value

**68** MIS considered wholesale

**34,500**  
customers

**\$10.6 billion**  
total transaction value

### Inherent risk summary

Variable	Factors increasing risk	Factors decreasing risk
<p>Nature, size and complexity of business</p>	<ul style="list-style-type: none"> <li>Asia-Pacific Funds Passport</li> </ul>	<ul style="list-style-type: none"> <li>No cash contributions accepted or no cash withdrawals permitted.</li> </ul>
<p>Products / services</p>	<ul style="list-style-type: none"> <li>Self-managed products.</li> <li>The products can be assigned.</li> </ul>	<ul style="list-style-type: none"> <li>Products with long lock-in periods such as KiwiSaver or private equity funds.</li> <li>Employer-offered schemes.</li> </ul>
<p>Delivery channel for products and services</p>	<ul style="list-style-type: none"> <li>Use of third-party agents.</li> <li>Use of overseas intermediaries.</li> <li>Third-party payments permitted.</li> </ul>	<ul style="list-style-type: none"> <li>Face-to-face onboarding.</li> </ul>
<p>Customer types</p>	<ul style="list-style-type: none"> <li>High net worth customers.</li> <li>Foreign PEPs.</li> </ul>	
<p>Country risk</p>	<ul style="list-style-type: none"> <li>Customer based in, controlled by or owned by persons in high-risk jurisdictions.</li> </ul>	
<p>Institutions dealt with</p>	<ul style="list-style-type: none"> <li>Unregulated institutions.</li> </ul>	
<p><b>Overall risk</b></p>	<p>The ML/TF risk of the sector has been rated as medium-low. Funds where no lock-in period applies offer high liquidity, which makes them attractive to money launderers.</p> <p>The sector has a low number of trusts and other legal arrangements. It also has a low number of non-resident customers.</p>	

## Sector-specific risks



### Nature, size and complexity of business

**Risk rating: Medium-low**

This sector's RE population is split into wholesale and retail funds, with MIS managers requiring an FMC Act licence when offering funds to retail investors.

The licensed (retail) MIS sector reported \$80 billion worth of transactions and 1.33 million customers for the year ending 30 June 2020, and the wholesale sector \$10.62 billion worth of transactions and 34,458 customers.

A large proportion of REs monitor transactions both manually and electronically, with only a few REs indicating a purely manual monitoring of transactions. We expect this to be REs offering niche products with a low number of transactions.



### Products and services

**Risk rating: Medium-low**

The sector ranges from REs offering multiple products to single-product providers. Similarly, the services offered by the sector vary greatly, from fund managers with sales staff to wholesale fund managers who only engage with one or two customers. Most funds are easy to buy and sell, and offer daily liquidity, making them an attractive proposition for ML. This is in contrast to superannuation products such as KiwiSaver, which is inaccessible until retirement age (with exceptions for situations such as first home withdrawals and hardship claims).



### Delivery channel for products and services

**Risk rating: Medium-high**

The number of MIS managers on-boarding customers face-to-face (40%) has increased compared with the 2017 data, but could be attributed to REs including customers on-boarded through financial advisers. This could also be due to REs providing an increase in other services such as DIMS.

Approximately 30% of REs onboard between half and all of their customers through domestic intermediaries.

Only 1% of REs on-board customers through the use of international intermediaries.



### Customer types

**Risk rating: Medium-low**

Within the sector, REs have indicated similar numbers of trusts and other legal structures (2%), and a low number of non-resident customers (2%). 19% of retail MIS REs report having foreign PEPs and 7% of wholesale MIS. Given the low number of non-resident customers, we see this as a possible indicator of the sector's more sophisticated screening mechanisms compared to other sectors. Nevertheless, PEPs present a higher risk for ML and we expect REs to reflect this in their dealings with these customers.



### Country risk

**Risk rating: Low**

The sector has just 2% non-resident customers. The top five countries for both retail and wholesale MIS are Australia, US, UK, Canada and Singapore (as was the case with the 2017 SRA). Information on country risk ratings can be found from a number of information sources including the Financial Action Task Force, Transparency International, the United Nations Office on Drugs and Crime, and open source media.



### Institutions dealt with

**Risk rating: Low**

Fund managers mostly deal with other licensed entities, investment platform providers, custodians and registered New Zealand banks, which all have their own AML processes.

## Peer-to-peer lending providers

---

### Introduction

Peer-to-peer lending is a financial market service covered by the FMC Act. The FMC Act enables borrowers to raise up to \$2 million in any 12-month period, without having to issue a product disclosure statement.

Currently there are eight licensed peer-to-peer platforms operating in New Zealand. They offer different types of lending such as secured and unsecured, business or consumer lending. One platform has provided 62% of lending in the year ended 30 June 2020

The business model of peer-to-peer REs is a simple 'self-service' online model. The information we gather through the licensing process tells us these platforms are well resourced to ensure they meet their compliance obligations.

This sector has filed 1 STR covering 1 transaction, and 7 SARs for the year to 31 December 2020.

There are some risks of ML in this sector due to it being based online. Additionally, the description of what the lending is used for, such as 'wedding', or 'holiday' can be difficult for REs to verify.

We see the risk of collusion by borrowers and lenders, for example through lending facilitated by the platform to legitimise sources of funds, and cash payments changing hands between borrowers and lenders outside the platform. However, the amounts involved in this sector are still relatively small.

This means it does not lend itself to laundering large sums of money.

### Red flags

The following red flags are a starting point for REs to consider in their risk assessment and compliance programme. It should not be seen as an exhaustive list of unusual customer activity. Red flags should trigger an RE to investigate its customer activities further, and where appropriate file a SAR.

These are:

- Two customers that have the same address/bank account who are on opposite ends of the transaction
- A loan is cancelled within seven days or multiple times within that seven-day period by a customer
- Customer with an excellent credit score seeks repeated loans which do not fit their profile
- Early repayments or repetitive early repayments of loans
- Cookies indicating customer with New Zealand address is arranging transactions from overseas
- Many customers signing up from one IP address.

# 8

**Licensed peer-to-peer lending providers**



**33,400**  
customers



**\$555 million**  
total transaction value

### Inherent risk summary

Variable	Factors increasing risk	Factors decreasing risk
<p><b>Nature, size and complexity of business</b></p>	<ul style="list-style-type: none"> <li>Lending growth higher than the RE's staffing availability to maintain good levels of compliance.</li> </ul>	
<p><b>Products / services</b></p>	<ul style="list-style-type: none"> <li>Third parties allowed to repay loans on behalf of customers.</li> </ul>	
<p><b>Delivery channel for products and services</b></p>		
<p><b>Customer types</b></p>	<ul style="list-style-type: none"> <li>PEPs.</li> </ul>	
<p><b>Country risk</b></p>	<ul style="list-style-type: none"> <li>Customer based in, controlled by or owned by persons in high-risk jurisdictions.</li> </ul>	
<p><b>Institutions dealt with</b></p>	n/a	n/a
<b>Overall risk</b>	The ML/TF risk of the sector has been rated as medium-low. This rating is because there are small sums of money involved, few non-resident customers and a low number of trusts and other legal arrangements.	

## Sector-specific risks



### Nature, size and complexity of business

**Risk rating: Medium-low**

REs are required to be licensed under the FMC Act. This provides good quality information of the activities within the sector and regulatory oversight. The sector has a relatively simple business model, matching lenders and borrowers through an online based platform. REs in the sector are sufficiently well-resourced to carry out the activities to meet their compliance obligations.

In line with its online business model, 17% of REs carried out electronic transaction monitoring only; the remaining 83% use a mixture of online and manual monitoring. Electronic transaction monitoring provides the advantage of monitoring volume and patterns. However, it does depend on continual improvement of the monitoring parameters, which represents a risk to REs if the parameters are not reviewed on a regular basis.



### Products and services

**Risk rating: Medium-low**

This sector is involved in peer-to-peer lending services only. We see two types of 'products' in the sector:

- Lending through the platform
- Borrowing through the platform.

The average transaction value is still relatively low

per customer, which reduces the likelihood of large sums of money being laundered through the platforms undetected.



### Delivery channel for products and services

**Risk rating: Medium-high**


This sector, being entirely based around online delivery, only accepts customers via non face-to-face methods. From the information provided by the sector we understand that one RE utilises domestic intermediaries to accept new customers. Online on-boarding increases anonymity and is therefore rated a higher risk for ML/TF.



### Customer types

**Risk rating: Low**

Peer-to-peer lenders appear to cater mostly to domestic individuals, with non-resident customers being very low at 0.2%, which has not increased since the 2017 SRA. Trusts and other legal arrangements, which are considered higher risk for ML, make up about 1% of customers. No PEPs have been reported for this period.



**Country risk**

**Risk rating: Low**

The sector has a low exposure to non-resident customers at only 0.2%. Countries in this sector include China, Australia, Malaysia, Singapore, Germany, Switzerland, United Kingdom and the United States of America.

Information on country risk ratings can be found from a number of information sources including the Financial Action Task Force, Transparency International, the United Nations Office on Drugs and Crime, and open source media.



**Institutions dealt with**

**Risk rating: n/a**

Not applicable.

## Discretionary investment management services (DIMS)

### Introduction

There are currently 52 licensed DIMS providers, four of which are registered banks and therefore supervised for AML/CFT purposes by the Reserve Bank of New Zealand and not included in this analysis.

DIMS providers differ significantly in size, ranging from large REs with significant funds under management to small FAPs. From 15 March 2021, DIMS can only be provided under the FMC Act.

A number of DIMS providers also hold licences in other areas such as MIS, are providers of client money and asset services (previously brokers), or employ a large number of financial advisers who sell DIMS. This overlap is reflected in the data, because the regulatory reporting requires REs to provide information on their entire business rather than separating out activities. However, the data does provide valuable insights into RE businesses that provide DIMS and their exposure to ML/TF risks.

What all DIMS providers have in common is that the nature of the service is to make decisions on behalf of a customer, in line with an agreed strategy. This requires in-depth knowledge of a customer's personal and financial situation and is generally a long-term relationship.

The requirement for customers to disclose detailed information to an adviser, as well as the involved process to initially enter into a DIMS arrangement, means DIMS appears unlikely to be an attractive proposition for money launderers.

FIU records indicate that no STRs or SARs have been filed under this sector – though this may be misleading, as they may have been identified under the broker/custodian sector filings.

While the sector has been given a medium-low rating, there are factors which would significantly increase an RE's risk rating, such as a high number of PEPs. These factors appear to be relevant only to specific DIMS REs, so we classed them as factors increasing the risk, rather than changing the sector's overall risk rating. We do not consider PEPs as customers to be an issue at this stage (see customer section below).

### Red flags

The following red flags are a starting point for REs to consider in their risk assessment and compliance programme. It should not be seen as an exhaustive list of unusual customer activity. Red flags should trigger an RE to investigate its customer activities further, and where appropriate file a SAR.

These are:

- A customer requests a transfer of assets or account closure shortly after entering into a DIMS facility
- Lump sum additions out of alignment with known source of income
- Withdrawals are made shortly after deposits
- A customer who seems to be indifferent to losses
- A new customer who introduces other high net worth customers shortly after onboarding
- No logical geographic connection between where the customer lives and where the adviser is based.



# 52

**Licensed DIMS**  
(48 supervised by the FMA)



**614,000**  
customers



**\$184 billion**  
total transaction value

### Inherent risk summary

Variable	Factors increasing risk	Factors decreasing risk
<b>Nature, size and complexity of business</b>		<ul style="list-style-type: none"> <li>Small customer base personally known to adviser.</li> </ul>
<b>Products / services</b>	<ul style="list-style-type: none"> <li>Commission-based adviser remuneration.</li> </ul>	
<b>Delivery channel for products and services</b>	<ul style="list-style-type: none"> <li>Non face-to-face onboarding of customers.</li> </ul>	
<b>Customer types</b>	<ul style="list-style-type: none"> <li>Foreign PEPs.</li> <li>High net worth individuals.</li> </ul>	
<b>Country risk</b>	<ul style="list-style-type: none"> <li>Customer based in, controlled by, or owned by persons in high-risk jurisdictions.</li> </ul>	
<b>Institutions dealt with</b>		
<b>Overall risk</b>	<p>The ML/TF risk of the sector has been rated as medium-low. This is mainly due to the ease of entering and exiting the product, which is similar to a MIS.</p> <p>Additions and withdrawals of funds that do not align with the known wealth of the customer should be able to be identified quickly and a SAR raised accordingly.</p>	

## Sector-specific risks



### Nature, size and complexity of business

**Risk rating: Medium-high**

The transaction volume of \$184 billion for the year to 30 June 2020 is significantly higher than 2017. We consider that this is due to the way reporting entities had previously reported their activity, i.e. it may have previously been reported under providers of client money and property services (previously broker/custodian), or financial adviser.

Around 15% of REs rely solely on electronic transaction monitoring, but from AML/CFT supervisor monitoring activity we know that most REs rely on electronic transaction monitoring with a minimal amount of manual transaction monitoring. The 5% of REs carrying out manual transaction monitoring only are assumed to be at the lower end of the DIMS scale (FAPs), as solely manual monitoring would be difficult for larger providers.



### Products and services

**Risk rating: Medium-low**

DIMS can be offered either as a service that closely resembles a managed fund, or as a personalised service which will take into account a customer's preferences and personal circumstances. We think DIMS services that do not involve a personal adviser pose a higher risk of ML, because there is less requirement for customers to interact with an actual adviser.

DIMS products are generally comprised of products with high liquidity such as shares, funds and bonds. To exit the service a customer can either ask for liquidation of the underlying assets or request a transfer of assets to their name.

We expect unusual lump sums or withdrawals would quickly raise suspicion by advisers due to the detailed information about the customer's financial situation on hand from the account opening stage.



### Delivery channel for products and services

**Risk rating: Low**

A large proportion of REs (67%) onboard more than 90% of customers via face-to-face methods. This is in line with the expectation that advisers need to know their customers circumstances in detail to be able to offer a DIMS service. Of the remaining 33%, nearly all onboard 80%+ of their customers non face-to-face. Only three REs reported on-boarding their customers using mainly non-face-to-face methods such as electronic, phone or post, which could be a reflection of entities engaged in other sectors.



### Customer types

**Risk rating: Low**

The sector has a low rate of trusts and other legal arrangements of around 2%. Six REs in this sector have reported having one foreign PEP as a customer, and one

RE reported having two PEPs as customers. We believe that this is very low compared with the overall number of customers in this sector, therefore we have not included it as a risk which increases the overall sector risk.



**Country risk**

**Risk rating: Low**

The number of non-resident customers is still low at 1.5%. The top countries REs are exposed to are Australia, United States of America, United Kingdom, Canada and Singapore, which is the same as in 2017. However, 19 REs did record having customers in two or more countries they have assessed as “high risk”.

Information on country risk ratings can be found from a number of information sources including the Financial Action Task Force, Transparency International, the United Nations Office on Drugs and Crime, and open source media.



**Institutions dealt with**

**Risk rating: Low**

From information obtained during monitoring activity, we understand that DIMS providers deal with institutions largely based in New Zealand.

## Licensed supervisors

### Introduction

There are currently five licensed supervisors. A supervisor can be licensed to provide supervision of one, a combination of, or all of the following:

- Debt securities
- Managed investment schemes (including KiwiSaver schemes)
- Retirement villages.

Supervisors are generally not involved in the day-to-day activities of debt issuers and managed investment schemes – as the name suggests, their role is to supervise the activities of their customers.

We rate the supervisory activity as low risk for being subject to ML, as there is no discretion for supervisors to act outside their supervisory role and because of the insights supervisors have into their customers' affairs.

Historically, Statutory Trustee Companies were supervised by the FMA, and trust and company service providers were supervised by the DIA. Changes were made to the Act for non-anti-money laundering and countering financing of terrorism purposes. One of those changes was removing trustee companies as a sector, effectively replacing it with licensed supervisors. However, all trustee companies supervised by the FMA for AML/CFT purposes are licensed supervisors.

Trustee companies offer their customers a wide range of services in addition to administering estates, for which they were initially set up. This ranges from ad-hoc transactions to managing their customer's financial affairs entirely.

Some of the activities carried out are:

- Providing client money and property services (previously broking and custody)
- Financial advice (often provided by FAPs)
- Establishing trusts and other legal arrangements.

Our analysis focuses on the activities of a licensed supervisor. Activities carried out by REs outside of their supervisory function must be considered by referring to the relevant sectors in this report, such as providing client money and property services (previously broking and custody), financial advice and where applicable, the SRAs of one of the other AML/CFT supervisors, e.g. the Trust and Company Service Providers risk assessment published by the DIA.

This sector filed 3 STRs covering 4 transactions, and 1 SAR for the year ended 31 December 2020.

### Red flags

The following red flags are a starting point for REs to consider in their risk assessment and compliance programme. It should not be seen as an exhaustive list of unusual customer activity. Red flags should trigger an RE to investigate its customer activities further, and where appropriate file a SAR.

#### Debt securities

- Raised debt funds are co-mingled with other funds for investment. There is either no reasonable explanation, or there are concerns about the source of the equity funding
- Debt is retired, with no reasonable explanation for the source of the new funding
- Debt issuer is making unusually high profits relative to its peers or historical profit levels
- Retirement village occupation right agreement deposits
- An individual purchases an occupation right agreement for a retirement village and departs soon after. There is no reasonable explanation, and the individual is prepared to accept the lower capital repayment sum.

#### MIS

- Unusual related-party transactions
- Investments appear to be made outside of a fund's mandate.

# 5

**Licensed supervisors**



**426,000**  
customers



**\$146.5 billion**  
total transaction value

### Inherent risk summary

Variable	Factors increasing risk	Factors decreasing risk
<p><b>Nature, size and complexity of business</b></p>	<ul style="list-style-type: none"> <li>• Insufficient compliance resources.</li> <li>• Related party transactions between trust structures, companies and other entities.</li> <li>• Poor record keeping.</li> </ul>	<ul style="list-style-type: none"> <li>• Information technology systems that are fit for purpose.</li> </ul>
<p><b>Products / services</b></p>	<ul style="list-style-type: none"> <li>• Escrow accounts. MIS custody.</li> </ul>	
<p><b>Delivery channel for products and services</b></p>		
<p><b>Customer types</b></p>		
<p><b>Country risk</b></p>		
<p><b>Institutions dealt with</b></p>		
<p><b>Overall risk</b></p>	<p>We rate licensed supervisors who only provide supervisory functions as low risk. There is no discretion for supervisors to act outside their supervisory role and they are not involved in the day-to-day activities of the schemes they supervise.</p>	

## Sector-specific risks



### Nature, size and complexity of business

**Risk rating: Medium-low**

Following the FMC Act licensing requirements, obligations have been placed on supervisors. This has the potential to put some strain on both human capital and infrastructure, which increases the risk of ML due to human or system errors. We have also seen a consolidation of services provided in this sector, with one licensed supervisor accounting for 86% of the total transaction value.



### Products and services

**Risk rating: Low**

There are two main products/services offered by licensed supervisors:

- Acting as a supervisor
- MIS custody

As set out earlier, we rate the supervisory activity as low risk due to the nature of the activity. Supervisors who also act as a MIS custodian have a heightened risk profile, which is in line with the providers of client money and property services (previously broking and custody) sector for this activity. REs who offer MIS custody should refer to the MIS section to ensure a full understanding of their ML risks.



### Delivery channel for products and services

**Risk rating: Low**

Onboarding of customers is carried out face-to-face and is part of commercial negotiations with each MIS manager.



### Customer types

**Risk rating: Low**

Customers of REs in this sector, MIS managers, are REs in their own right. The risk rating of low is a reflection of the risk rating assigned to this sector.



### Country risk

**Risk rating: Low**

There is no indication that REs in this sector interact or deal with institutions in high-risk jurisdictions or with low AML/CFT standards.



### Institutions dealt with

**Risk rating: Low**

## Issuers of securities

---

Issuers of securities captured by the Act are considered to be 'participating in securities issues and the provision of financial services related to those issues'. From the 2020 annual return data, 36 REs identified as issuers of securities. This sector's RE population is split into wholesale and retail funds, with MIS managers requiring an FMC Act licence when offering funds to retail investors. This has not changed for the 2021 update. Some "issuers" will be identified in other categories, as this will be where their predominant activity is captured.

Before the FMC Act, the types of securities covered by the sector were:

- Equity securities
- Debt securities
- Interests in unit trusts
- Interests in KiwiSaver schemes
- Interests in contributory mortgages
- Participatory securities such as bloodstock schemes
- Interests in registered superannuation schemes and life insurance policies.

With the introduction of the FMC Act, all types of securities mentioned above have been included in other sectors, except for issuers of debt securities that are neither banks nor non-bank deposit takers and also provide financial services in relation to the debt securities issued.

## Appendix: Glossary

---

AB	Authorised Body
AML/CFT	Anti-Money Laundering and Countering Financing of Terrorism
DI	Derivatives issuer
DIMS	Discretionary Investment Management Service
FAP	Financial Advice Provider
FMC Act	Financial Markets Conduct Act 2013 (as amended by the Financial Services Legislation Amendment Act)
FMC Regulations	Financial Markets Conduct Regulations 2014
MIS Manager	Managed Investment Scheme Manager
ML/TF	Money Laundering and Terrorism Financing
NRA	National Risk Assessment
PEP	Politically exposed person
RE	Reporting entity for the purposes of the Anti-Money Laundering and Countering of Financing of Terrorism Act
RA	Risk Assessment
SAR	Suspicious Activity Report
SRA	Sector Risk Assessment
SRA 2017	The FMA's Sector Risk Assessment prepared in 2017
STR	Suspicious Transaction Report
The Act	Anti-Money Laundering and Countering Financing of Terrorism Act 2009
VASP	Virtual Asset Service Provider





---

**AUCKLAND** – Level 5, Ernst & Young Building | 2 Takutai Square, Britomart | PO Box 106 672 | Auckland 1143

**WELLINGTON** – Level 2 | 1 Grey Street | PO Box 1179 | Wellington 6140

**fma.govt.nz**