April 2019

Anti-money laundering and countering financing of terrorism

Monitoring report 1 July 2016 - 30 June 2018

FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TATAI HOKOHOKO - NEW ZEALAND

Purpose

The purpose of this report is to help reporting entities (REs) better understand our expectations, and what they can do to improve their systems and processes to comply with the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the Act) and its supporting regulations.

This report summarises our monitoring activities from the period from 1 July 2016 to 30 June 2018, which marked our fifth year of monitoring compliance with the Act. We focused on:

- risk assessments being up to date and well maintained
- adequacy and effectiveness of policies, procedures and controls as per the AML/CFT programme
- customer due diligence, ongoing customer due diligence and enhanced due diligence
- governance and management oversight.

We chose to focus on these areas based on our observations from ongoing monitoring and analysis of annual return information.

Contents

Executive summary

Our role

Under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the Act), the three AML/CFT supervisors are the Financial Markets Authority (FMA) the Reserve Bank of New Zealand (RBNZ) and the Department of Internal Affairs (DIA).

The FMA supervises approximately 800 reporting entities (REs). Approximately two-thirds are financial advisers, and the remainder are derivatives issuers, brokers and custodians, fund managers, providers of discretionary investment management services, equity crowdfunding and peer-to-peer lending platform providers, licensed supervisors and issuers of securities. This population has remained largely unchanged since December 2016 when we issued our previous report.

Our role as supervisors includes:

- monitoring and assessing the level of ML/TF risk that exists across all supervised REs
- monitoring REs for compliance with the Act and regulations
- providing guidance to REs to help them comply with the Act and regulations
- investigating REs for non-compliance with the Act and regulations.

To ensure a consistent supervisory approach across all New Zealand REs, the FMA frequently interacts and coordinates with the other supervisors.

We also:

- cooperate with various committees and agencies both domestically and internationally, including the Department of Justice (MOJ), New Zealand Police Financial Intelligence Unit (FIU), Customs, Inland Revenue, MFAT and the Ministry of Business, Innovation and Employment
- engage internationally as members of the International Supervisor Forum (ISF), the Financial Action Task Force (FATF) and the Asia/Pacific Group on Money Laundering (APG).

Findings

The Act came into full effect on 30 June 2013. We therefore expect REs to be fully aware of their obligations, and to have implemented adequate and effective policies, procedures and controls to ensure compliance with the Act and regulations. Although REs have made good progress in meeting their AML/CFT obligations, there are still a number of areas that require attention.

During our interactions with REs the following issues were highlighted, and should be addressed by management and boards:

- **AML/CFT programmes** that have not been reviewed and updated to align with the business's current practices, have not been updated for two years, do not include politically exposed person (PEP) check processes, refer to other jurisdictions' legislation, do not specify how customer activities and or transactions are monitored, do not provide staff with specific criteria to consider when reviewing potential suspicious transactions, etc.
- **AML/CFT risk assessments** that are not updated when changes in risks occur (including country risk changes, new products being added, substantial new client databases being added), are too complex for the size and nature of business, refer to outdated legislation, do not consider the likelihood of business being used for ML/TF, etc.
- **Customer due diligence (CDD) including enhanced CDD (ECDD) and ongoing CDD and account monitoring** remains problematic for REs. More and

more REs are using electronic identity verification to verify customers, but we noted a number of deficiencies with their AML/CFT programmes in this regard. REs are also not conducting ECDD when required and account monitoring systems are still not fit for purpose.

Enforcement actions

During the review period, 18 formal warnings (including one public warning) were issued under section 80 of the Act, for significant breaches of the Act. Warnings are made public to deter other REs from engaging in similar activity. The determination of whether to make a warning public is largely driven by the number and severity of the RE's breaches.

Reasons for the warnings included the following:

- Not meeting key obligations in risk assessments and/or the AML/CFT programme.
- Failing to take reasonable steps to determine whether a customer or any beneficial owner is a politically exposed person.
- Only performing account monitoring on accounts in excess of US$100,000.
- Failing to report suspicious transactions to the FIU.
- Failing to have independent audits of risk assessment and AML/CFT programmes performed every two years.
- Failing to submit an annual AML/CFT report to the FMA by the 31 August deadline.
- Failing to provide the FMA with copies of independent audit reports when requested.

Where REs engage in conduct that constitutes a civil liability act, or do not take appropriate corrective action, civil or criminal enforcement action may be taken under the Act. This may result in (but not be limited to) the imposition of:

- civil penalties of up to $200,000 in the case of an individual, or $2 million, in the case of a body corporate; and
- criminal penalties of imprisonment for up to two years or a fine of up to $300,000 in the case of an individual, or
  $5 million in the case of a body corporate.

Future focus

REs have had more than five years to familiarise themselves with their obligations in terms of the Act, and we expect to see more mature policies, procedures and controls in place.

Our future monitoring activities with REs will therefore include more desk-based and on-site monitoring visits, and an increased focus on reviewing independent audit reports. This will result in more in-depth reviews of areas such as client on-boarding and account monitoring processes. To assist us in performing these operational reviews we will interact more with the frontline staff who perform these tasks, to assess their understanding of their obligations.

We expect REs to consider the findings and observations in this report and, where required, update their AML/CFT policies, procedures and controls to ensure compliance with their obligations. We will continue to investigate suspected non-compliance and take appropriate enforcement action consistent with the FMA's enforcement policy. This will include giving more consideration to publishing the outcomes of formal warnings we issue.

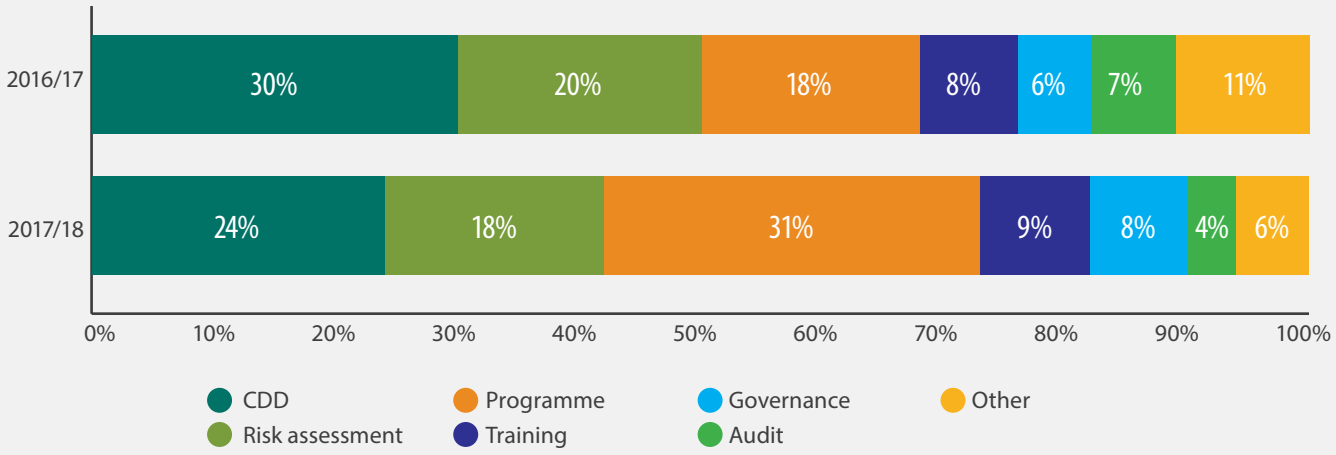
Our findings and observations

Summary of findings

During the period 1 July 2016 to 30 June 2018, we did 44 onsite visits and 24 desk-based reviews. From this we found 89 issues in 2017 and 175 issues in 2018 requiring remedial action by REs.

The top three themes for both years related to AML/CFT programmes, AML/CFT Risk Assessments and CCD (which included ECDD and Ongoing CDD).

Issues identified by theme



AML/CFT programmes

Section 57 of the Act requires REs to have adequate and effective policies, procedures and controls in place to assist with managing compliance. During monitoring activities with REs in 2018, 31% of our findings related to the AML/CFT programmes (18% in 2017). We are therefore concerned with the adequacy and effectiveness of procedures, policies and controls REs have in place.

In November 2017, we issued a formal public warning to Fullerton Markets Limited (Fullerton) for failing in terms of section 56 of the Act to establish a compliance programme based on their risk assessment, including adequate and effective procedures, policies and controls.

Fullerton could only produce a draft compliance programme, which was not approved by their board even though it had been operational for over a year at the time of our monitoring visit.

We also issued a formal private warning to a RE for failing to have adequate and effective procedures, policies and controls included in their AML/CFT programme as required per section 57 of the Act.

Our expectations

Programmes must align with current processes, business structures, products and services. The Act came into effect in June 2013, so we expect REs to have appropriately mature practices that meet the minimum requirements for:

- vetting and training of senior managers, AML/CFT compliance officers and any other staff with AML/CFT duties

- complying with CDD requirements, including ongoing CDD and account monitoring
- reporting suspicious activities to the FIU
- reporting prescribed transaction reports (PTRs) to the FIU
- record-keeping
- managing and mitigating the risk of ML/TF
- identifying when ECDD is required, and ensuring it is based on current and relevant information and source documents.

REs must also consider guidance material produced by AML/CFT supervisors and the FIU.

Examples of good practice

- Programme is updated at least annually (or more regularly when legislative changes occur, such as the requirement to report PTRs), or when the RE introduces new products, does business in new jurisdictions, etc.

Examples of unsatisfactory practice

- Programme is not updated or aligned with current business practices.
- Programme has not been reviewed and updated for more than two years.
- Programme does not require that PEP checks are done, and there is no indication of how often PEP screening is conducted on existing customers.
- Programme and training material includes references to Australian AML/CFT legislation.
- Programme does not specify the frequency of customer activity monitoring.
- Programme does not specify what criteria staff should consider when reviewing a transaction as potentially suspicious.

AML/CFT risk assessment

Under section 58 of the Act, REs are obliged to assess the risk of ML/TF that they could reasonably expect to experience during the course of their business. REs understand their business better than anyone else and must consider any changes in their operations that could affect the level of ML/TF risk they face.

The formal public warning issued to Fullerton in November 2017 also related to a breach of section 58 of the Act, which requires REs to have a risk assessment. Fullerton twice presented the FMA with draft risk assessments that were not compliant.

A formal private warning was also issued to a RE for not considering in their risk assessment the nature, size and complexity of their business, and the countries and institutions they deal with.

Our expectations

Risk assessments must be kept up to date and reviewed as and when changes in the business's circumstances occur that might be material to the level of ML/TF risk faced by the RE. Examples of such changes include the addition of new products or services, new methods of delivery, and doing business in new countries.

REs must consider the:

- nature, size and complexity of their business
- types of products and services they provide
- methods of delivery of products and services
- types of customers they deal with
- countries they do business in
- institutions dealt with
- guidance material produced by AML/CFT supervisors and the FIU.

Our findings

- REs tend to be one end or the other of the compliance spectrum. We saw well-documented risk assessments with well-defined rationale as to why certain levels of risk had been assigned to different aspects considered in the risk assessment. We also saw REs using off-the-shelf templates to complete the risk assessment, but failing to make it fit for purpose for the size and nature of their business.
- REs are not updating risk assessments when changes occur that could affect the level of ML/TF risk they face. This includes country risk ratings not being updated, and no consideration of risk when adding new products, services or substantial new client databases to their business.

Examples of good practice

- Risk assessment is updated at least annually, or more regularly when the RE introduces new products, does business with new jurisdictions, etc.
- Risk assessment clearly considers the likelihood that the business will be used for ML/TF.
- Risk assessment is appropriate for the size and nature of the business.
- RE demonstrates a dynamic risk rating for each client that adjusts according to the investing behaviour of the customer, and is built into the core IT infrastructure.

Examples of unsatisfactory practice

- Risk assessment is too complex for the nature and size of business.
- Risk assessment has not been reviewed and updated for more than two years.
- Ineffective use of FMA's Sector Risk Assessment 2017 when performing RE risk assessment.
- Risk assessment is not reviewed and updated and therefore refers to outdated legislation and terminology, does not include version history or includes references to the Australian AML/CFT legislation.
- Risk assessment does not give regard to trade-based ML even though the RE client base includes importers to New Zealand, which increases the risk of this.
- Risk assessment does not adequately consider the likelihood that the business may be used for ML/TF.

Customer due diligence (CDD)

REs are required to conduct CDD, including enhanced CDD (ECDD) and ongoing CDD, and to monitor the accounts of new and existing customers.

The FMA warned Fullerton for failing to take reasonable steps to determine whether their customers or any beneficial owners are PEPs as soon as practicable after establishing a business relationship or conducting an occasional transaction, as required by section 26 of the Act. They also failed to carry out checks on PEPs and relied on self-declarations by customers. We required Fullerton to undertake a review of all customers to ascertain if they were PEPs by using an internationally recognised search tool, and to take appropriate steps where there was a positive match.

Fullerton also failed to conduct ongoing CDD and undertake account monitoring to ensure that the business relationship and the transactions relating to that business relationship were consistent with the RE's knowledge of the customer and the customer's business and risk profile. Only accounts in excess of US$100,000 were monitored, which does not comply with the requirements of section 31 (2) of the Act.

We required Fullerton to develop a more appropriate level of transaction monitoring and undertake a review of all customer transactions since commencing business in New Zealand, and to file SARs with the FIU where suspicious activities were identified.

A formal private warning was also issued to a RE for failing to take reasonable steps, according to the level of risk involved, to verify the identity of any beneficial owners. The RE also failed to take reasonable steps to identify persons acting on behalf of customers and their authority to act in this capacity. This is relevant for customers who are trusts and companies. In many of the trust and company files we reviewed we noted that CDD was not adequately performed by the RE.

The formal private warning also related to the RE failing to undertake ongoing CDD, which includes the requirement for a RE to regularly review the information it holds on customers, including those that were on-boarded prior to 30 June 2013.

Our expectations

- REs must conduct CDD on all customers, any beneficial owner of a customer or any person acting on behalf of a customer.
- REs must conduct CDD based on the level of risk involved. Section 12 of the Act requires a RE to rely on its AML/CFT programme and risk assessment to determine the level of ML/TF risk for customers.
- PEP checks must be performed when establishing a business relationship or conducting an occasional transaction or activity.
- Where a PEP is identified, the RE must obtain senior management approval to continue with the relationship, and performs ECDD on the customer.
- REs must have an appropriate account monitoring system that can identify potential suspicious activity or transactions.
- Where account monitoring systems identify unusual customer activity or transactions, these red flags must be investigated. If activity is determined to be suspicious it should be reported to the FIU.

Our findings

- More REs use electronic identity verification to identify and verify customers, but we have noted a number of deficiencies related to this, including:
  - REs not clearly describing how all the relevant required criteria are satisfied.
  - REs using two electronic sources to electronically identify clients, but this process is not described in the RE's programme.
  - The electronic verification process set out in the AML/CFT programme is not aligned with Part 3 of the IDVCOP (Identity Verification Code of Practice) and the updated IDVCOP – EN (Exploratory Note).
- REs don't have processes for assessing and recording exceptions to the CDD process, e.g. where clients present expired passports or driver licences.
- REs not conducting ECDD when situations require it, and the source of funds or source of wealth not being verified or being determined as not requiring verification.
- As we reported previously, monitoring systems are still not fit for purpose, and include inadequate frequencies and transaction values.

Examples of good practice

- RE uses a dynamic risk rating of each client that adjusts according to the investing behavior of the customer, and is built into the core IT infrastructure.
- RE maintains a robust transaction monitoring system with monitoring done at appropriate intervals.

Examples of unsatisfactory practice

- No PEP checks done during on-boarding.
- Credit or debit cards used for CDD not having important details redacted.
- Checks not undertaken on documents obtained during CDD.
- The nature and purpose of the business relationship not being consistently recorded.
- Monitoring only done for deposits over a specific monetary value.
- Monitoring only performed monthly even though large transactions are conducted daily.

Electronic identity verification

Part 3 of the IDVCOP allows for electronic identity verification. To assist REs that are considering the use of electronic identity verification systems, an Exploratory Note was prepared by supervisors and published in December 2017.

Where REs decide to use electronic verification methods it is important they ensure the system they use satisfies requirements as per IDVCOP and IDVCOP-EN. If they rely on a single electronic source it must verify an individual's identity to a high level of confidence. Only an electronic source that incorporates biometric information (or information that provides an equal level of confidence) enables an individual's identity to be verified to a high level of confidence.

Otherwise, REs must verify an individual's identity from at least two electronic sources, which must be reliable and independent. Results must match each other.

REs must clearly describe in their AML/CFT programme how they have determined that the electronic sources they use meet the requirements of being reliable and independent. REs must also update their policies, procedures and controls to indicate they are using electronic verification methods to do CDD.

Politically exposed persons and sanction checking

REs must ensure they perform PEP checks when on-boarding new customers, and thereafter from time to time on an ongoing basis depending on the level of ML/TF risk – with high risk customers being checked more frequently. We have noted REs do PEP checks at on-boarding, but no further PEP checks are performed. In some instances REs don't have appropriate systems to perform PEP checks.

REs must also ensure that sanction checks are performed and that this process is clearly described in policies, procedures and controls. We have noted instances where REs don't do sanction checks (e.g. UN country and individual lists) and don't include this in their policies, procedures and controls.

Financial Intelligence Unit and suspicious activity reports

goAML

All REs must register with goAML so they can submit SARs and receive relevant information from the FIU. The FIU provides goAML system training, which all users should attend. REs can contact the FIU to arrange training.

All goAML-related questions and issues must be directed to the FIU.

Suspicious activity reports (SARs)

REs are required by section 40 of the Act to report suspicious activities to the FIU by submitting SARs through the goAML portal. The following table shows the number of SARs received by the FIU since the Act came into effect in June 2013.

Period	Total SARs submitted to FIU	SARs submitted by our REs
2013/14	10,585	38
2014/15	11,684	33
2015/16	8,415	47
2016/17	9,139	56
2017/18	10,048	128

In 2015/16 we noted that our REs submitted only a fraction of the total number of SARs filed. We decided to provide targeted training jointly with the FIU for REs on filing SARs when required. Eleven training sessions were held in various locations across New Zealand, which were attended by a total of 173 AML compliance officers and RE staff. The number of SARs being filed by our REs increased by 20% in 2016/17 and 128% in 2017/18.

The FMA and FIU are planning to deliver more training in 2019 in various locations. REs will be invited and are encouraged to participate. The training includes practical examples and discussions of actual case scenarios. It will help those responsible for on-boarding new customers and performing account monitoring activities to be more alert to suspicious activities and transactions.

Engaging with your supervisor

REs are encouraged to build good working relationships with us on a formal or informal basis. We can provide general comments and guidance, but not advice on specific issues. For all AML/CFT-related queries email aml@fma.govt.nz

Reminder to REs

- **Addition and removal of REs**

  REs need to notify the FMA of any changes within their business that may require us to update the AML/CFT RE list on our website. When changes occur, email us with a brief explanation of the proposed changes. We aim to keep this list up to date as our RE population changes.

- **AML/CFT compliance officer changes**

  We expect all REs to email us the details of changes to their AML/CFT compliance officer. Before appointing compliance officers, REs must ensure the person is adequately experienced to effectively administer and maintain the AML/CFT programme.

Appendix: How we engaged with the sector

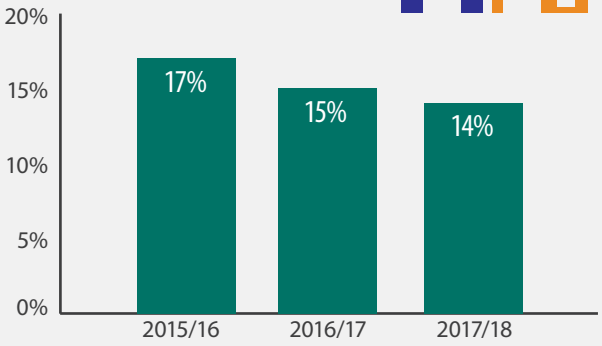
AML/CFT annual reports

REs are required to file annual reports by 31 August each year, for the year ending 30 June. This data helps in our risk-based approach to monitoring, allowing us to better understand where our REs are located and what business activities they carry out.

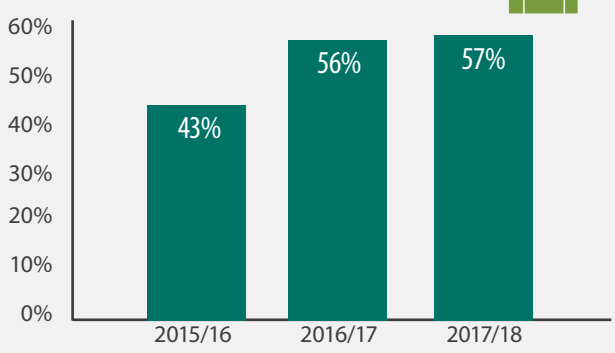
There has been a reduction in the number of late filings of annual reports from previous reporting periods. Late filing is a breach of regulatory obligations, and we have issued warnings to late filers and those who fail to file their annual reports.

From the annual reports we have noted the information and trends.

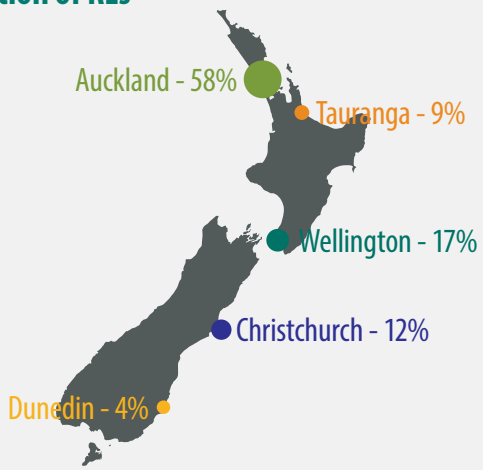
Percentage of REs that are members of a designated business group



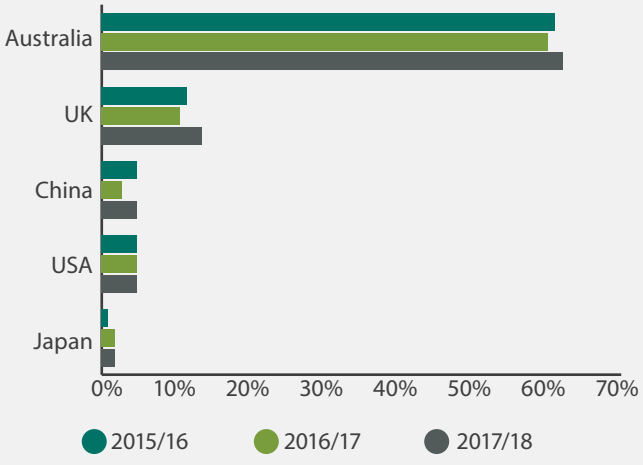
Percentage of REs with 100% face-to-face on-boarding of new customers



Location of REs



Location of non-resident customers



Monitoring activity

We focus our monitoring on areas with the potential to cause the greatest ML/TF harm. We select REs for monitoring based on a range of factors that includes:

- assessment of risk
- information collected from sources such as the annual AML/CFT reports
- tactical intelligence
- the size and nature of the business
- the industry sub-sector
- compliance history
- complaints.

During the review period, we did 44 on-site monitoring visits and 24 desk-based reviews. Each visit and review was followed up with a feedback letter and other action as required. We also examined 145 independent AML/CFT audit reports, as well as information that must be included in annual AML/CFT reports.

During the review period, 18 formal warnings (including one public warning) were issued under section 80 of the Act, for significant breaches of the Act.

The table below summarises our direct engagement (including monitoring reviews) with REs in each sub-sector.

Sub-sector	SRA 2017 Risk Rating	On-site		Desk-based		Section 59 audit reports		Enforcement action taken	
		2016/17	2017/18	2016/17	2017/18	2016/17	2017/18	2016/17	2017/18
Derivatives issuers	H	4	6						1
Brokers and custodians	M-H	3	5	1	1		6		
Fund managers	M-L	5	8		6		6		2
Financial advisers	M-L	4	5	1		55	47	10	5
Equity crowdfunding platforms	M-L								
Peer-to-peer lending providers	M-L	1			1				
Providers of discretionary investment management services	M-L	2	1		8		7		
Licensed supervisors	L								
Issuers of securities	L				1		1		
Total		**19**	**25**	**2**	**22**	**55**	**67**	**10**	**8**

The desk-based reviews were a result of an initial examination of section 59 audit reports, which indicated further follow-up action was required with the RE. In most cases, this was following up on matters identified in the audit reports and ensuring the RE had taken the recommended or suggested actions.

Glossary

AML/CFT	Anti-money laundering and countering financing of terrorism
CDD	Customer due diligence, as defined in section 11 of the Act
DBG	Designated business group, as defined in section 5 of the Act. A DBG is a group of two or more persons where there is a written agreement between the persons that make up the group. An entity that elects to join a DBG may rely on another member of the DBG to carry out some of its obligations under the AML/CFT Act, provided certain conditions are met.
ECDD	Enhanced customer due diligence, as defined in sections 22-30 of the Act
Existing customer	A person who was in a business relationship with the reporting entity immediately before the commencement of Part 2 of the Act in 30 June 2013, or who has subsequently entered into a business relationship with the RE
FIU	Financial Intelligence Unit of the New Zealand Police
goAML	A reporting tool that allows the rapid and secure exchange of information between reporting entities and the Financial Intelligence Unit relating to suspicious activity reports
IDVCOP	Identity Verification Code of Practice
IDVCOP – EN	Identity Verification Code of Practice – Explanatory Note (updated December 2017)
ML/TF	Money laundering and terrorism financing
PEP	Politically exposed person
PTR	Prescribed transaction report – a report made under section 48a
RE	Reporting entity – a firm or individual as defined in section 5 of the Act
Risk(s)	Risk of money laundering and terrorist financing
SAR	Suspicious activity report – made under section 40 of the Act through goAML
SRA 2017 Risk Rating	FMA's Sector Risk Assessment (SRA) 2017 assigned risk ratings for each sector we supervise. The ratings are High (H), Medium-High (M-H), Medium-Low (M-L) and Low (L). For further detail as to how we assessed and assigned the risk ratings please refer to the FMA SRA 2017.
the Act	The Anti-Money Laundering and Countering Financing of Terrorism Act 2009 and its regulations

AUCKLAND

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

Phone: +64 9 300 0400

WELLINGTON

Level 2, 1 Grey Street
PO Box 1179, Wellington 6140

Phone: +64 4 472 9830