FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TATAI HOKOHOKO - NEW ZEALAND

February 2016

Anti-Money Laundering and Countering Financing of Terrorism

1 July 2014 to 30 June 2015

www.fma.govt.nz

AUCKLAND OFFICE | Level 5, Ernst & Young Building | 2 Takutai Square, Britomart | PO Box 106 672 | Auckland 1143
WELLINGTON OFFICE | Level 2 | 1 Grey Street | PO Box 1179 | Wellington 6140

Contents

Executive summary

Our role

The Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the Act), and associated regulations, came into full effect on 30 June 2013. The Act's purpose is to deter and detect money laundering and terrorist financing, and our role includes monitoring certain people and organisations for compliance, and to provide them with guidance.

We are one of three supervisors under the Act, along with the Reserve Bank of New Zealand and Department of Internal Affairs. We also work closely with the other supervisors and other government agencies, including Customs, Inland Revenue, the Ministry of Justice, New Zealand Police, the Ministry of Foreign Affairs and Trade, and the Ministry for Business, Innovation and Employment. We are part of the International Supervisors Forum, and participate in the meetings of the Financial Action Task Force (FATF) and the Asia/Pacific Group on Money Laundering.

We currently supervise around 800 firms and individuals (known as reporting entities) who are required to comply with the Act. Roughly two-thirds define themselves as financial advisers, but they also include issuers of securities, licensed supervisors, derivatives issuers, providers of discretionary investment management services, fund managers, brokers and custodians, equity crowdfunders, and peer-to-peer lenders.

Purpose of this report

The aim of this report is to summarise our monitoring to help firms and individuals better understand our expectations, and therefore improve their systems and processes, and ensure compliance with the Act.

This report covers the period from 1 July 2014 to 30 June 2015. It was our second year of monitoring compliance with the Act, and we focused particularly on:

- customer due diligence (CDD)
- transaction and account monitoring (as part of ongoing CDD obligations)
- management reporting and oversight (including governance).

The reasons for focusing on these areas were outlined in our 2014 monitoring report. They are core obligations and results from our early monitoring were not satisfactory in these areas.

During the year, we did 12 on-site monitoring visits and four desk-based reviews. Each visit and review was followed up with feedback reports and other action as required. We also examined 112 independent AML/CFT audit reports, as well as information required to be supplied to us in the 2014 and 2015 annual AML/CFT reports.

Our findings

We recognise the efforts firms and individuals have made since our last monitoring report to ensure they are complying with the Act. Most have had their risk assessments and compliance programmes independently audited, and the audits have shown broad compliance. Many of the queries we now receive are technical issues, rather than general requests for help. However, we are still seeing some common issues, including:

- A lack of senior management oversight (including governance), and a lack of regular AML/CFT reporting to senior management.
- A lack of clear AML/CFT controls in procedures. Some businesses have plenty of policies and procedures, but are light on controls. Policies, procedures and controls should be tailored to the size and nature of the business and the risks outlined in its risk assessment. In our monitoring, we are looking for appropriate systems and controls, not one-size-fits-all.
- Insufficient ongoing CDD and account monitoring. Many businesses understand their obligations, and have processes to monitor transactions, but some do not regularly review accounts.
- Insufficient or unclear information on both the nature and the purpose of the business relationship with their customers.

Three formal warnings under section 80 of the Act were issued during the year (including one public warning), for significant breaches of the Act. The warnings included not meeting key obligations in a risk assessment and/or compliance programme, and failing to provide us with an independent audit report.

Future focus

Much of our time during our initial monitoring was spent reviewing the design of internal controls. Now that firms and individuals appear to be more familiar with their obligations under the Act, we will focus on reviewing how well these internal controls are working.

Consistent with our strategic priorities, we will also examine governance systems to understand how they have established the right culture in AML/CFT practices from the top of the organisation.

We will also look at the potential for conflicted conduct. Organisations must find a balance between mitigating and managing the risk of money laundering and terrorist financing, compliance concerns, and sales culture and other drivers.

We will also focus on:

- senior management and board oversight of AML/CFT policies, procedures and controls including reporting to senior management
- ongoing CDD and account monitoring
- unusual transactions and how decisions are made about whether a suspicious transaction report should be filed with the financial intelligence unit of the New Zealand Police (FIU).

We will also consider how firms and individuals are treating the class exemption for managing intermediaries which came into effect in July this year. We will be particularly interested in the two classes of managing intermediaries that it relates to (‘licensed’ and ‘specified’ managing intermediaries) as there are conditions that apply, and different levels of information required for the exemption.

Our findings and observations

Risk assessments

Under section 58 of the Act, each reporting entity must assess the risk of money laundering and financing of terrorism it may reasonably expect to face. The Act calls this a risk assessment.

What we expect:

- Ongoing improvement in the quality of risk assessments, with risks clearly identified and documented.
- An understanding of the importance of a risk assessment and how it will help identify risks.
- Firms and individuals able to demonstrate they have considered all the items listed in section 58(2) of the Act.
- All risk assessments should clearly detail how they will remain current.

What we found:

- Evidence for the conclusions in the risk assessments was often inadequate.
- The conclusions were not always reflected in compliance programmes and operating procedures.
- Lack of clarity as to whether the risks documented were inherent or residual.

Examples of good practice	Examples of unsatisfactory practice
• Some firms and individuals have clear triggers for when their risk assessment should be reviewed. For one business, this included development of new products, publications from regulators (such as this report or FIU typology reports), and after AML/CFT compliance officer training. This business was also able to show a direct link between a 'trigger' occurring, and how this was considered in their risk assessment. • One business had received training from the FIU on 'what is suspicious'. It had one of the clearest views we've seen of the possible risks.	• We have observed several businesses that do not clearly define the risks for different types of customers, products and countries (such as simply defining all customers as low risk). This could result in the wrong areas being targeted for prevention. • Risk assessments that had not been reviewed since they were completed. Firms explained that their business had not changed since the assessments were initially prepared so they did not see the need to revisit them. Our general view was their criteria for review were likely set too high.

Customer due diligence

Under section 57(c) of the Act, compliance with CDD obligations is a minimum requirement for AML/CFT programmes. It is also an area we focus on strongly in our monitoring. Since our 2014 monitoring report, we have noticed an improvement in the quality of documented evidence for CDD, and in the verification of documents.

If AML/CFT functions such as CDD are outsourced, there must be robust oversight of the outsourced service providers. Compliance obligations remain with the firm or individual doing the outsourcing. We have seen examples of no oversight and, in one case, no agreement with the provider.

Firms or individuals considering outsourcing to another country must be familiar with section 33 of the Act, which details the required conditions. We have seen that where there is a strong, established business relationship, there are service agreements that include strong oversight provisions.

What we expect:

- Those who outsource CDD need to be aware they are not outsourcing their CDD obligations.
- Procedures and controls for CDD must be adequate, effective and reflect relevant provisions in the Act and/or the Amended Identity Verification Code of Practice 2013 (IDVCOP).

Actual procedures should match documented procedures and/or IDVCOP.

What we found:

- Where there were good internal controls over CDD, the collection of required documents was generally of a higher standard, and any exceptions were identified at an early stage.
- Some firms and individuals have not been able to demonstrate the relevant nature and details of the contractual relationship with the CDD provider. This includes demonstrating how they can be confident the provider is complying with the Act and IDVCOP (if applicable).

Examples of good practice	Examples of unsatisfactory practice
• A business relying on a third party to perform CDD (in this case, a financial adviser business) had an agreement which clearly detailed responsibilities and had robust monitoring controls. This included internally checking all client application forms and, in some cases, having this peer-reviewed before the applicant was accepted as a new customer. • One business provided us with clear IDVCOP exception-handling procedures. Every exception was documented with an explanation supporting the conclusion and decision made.	• One business had no controls or checking of new customers where CDD was undertaken by third parties. This resulted in a number of breaches of CDD, including verification requirements. • In some businesses, when new customers are non-natural persons (such as a company or trust), CDD is not adequately conducted on, among others, any person with effective control over the customer and any person acting on behalf of the customer.

Ongoing customer due diligence and account monitoring

Under section 31 of the Act, reporting entities are obliged to conduct ongoing CDD and account monitoring on new and existing customers. This extends to regularly reviewing any information already held about an existing customer. These are basic requirements for any AML/CFT compliance framework, since they play a key role in identifying potentially suspicious transactions, and an area we strongly focus on in our monitoring.

What we expect:

- To be able to demonstrate an understanding of the rules for the automated account and transaction monitoring system.
- Rules for the automated account and transaction monitoring system reflect the areas of higher risk identified in the risk assessment.
- Alerts are raised for appropriate transactions. Businesses are familiar with transaction monitoring requirements and adjust the rules to produce more meaningful results.
- To be able to demonstrate how alerts are dealt with.
- Transaction and account monitoring for all customers, including existing customers.
- Although there is no requirement to get previously obtained identity information unless there are 'reasonable grounds' to doubt its adequacy or veracity, ongoing CDD will not be as effective if information on existing customers is poor quality. We would like to see more firms and individuals regularly reviewing and updating this information.
- It should be clear in a firm's policies who finally decides whether the account is terminated if the customer is slow to respond or is unhelpful in providing requested CDD information within a reasonable time. Management needs to monitor such situations, and take action where needed, with evidence to back their decisions.
- Where issues around CDD arise, they need to be escalated and resolved to the satisfaction of the AML/CFT compliance officer.
- Where customers delay or resist providing required information within a reasonable period, there should be active follow-up and monitoring, including escalation to senior management or governance committees, and timely decision to terminate relationships where required.

What we found:

- Monitoring systems not fit for purpose, such as too manual or infrequent.
- Irregular transaction monitoring and, in some cases, no account activity monitoring.
- No written process for investigating alerts. Sometimes, no audit trail of investigations.
- A lack of reports on suspicious transactions.
- Some businesses did not:
  - know what information they had for existing customers
  - have a plan or process to review information on existing customers
  - risk-rate existing customers. This is especially concerning for customers who would be assessed as high risk or where enhanced due diligence would now be required (per their current CDD policy).

Examples of good practice	Examples of unsatisfactory practice
• Prior to 30 June 2013, a business risk-rated all existing customers. It has since reviewed its existing documents and identity information and updated those it considered inadequate. Other businesses have taken similar steps to review their pre-30 June 2013 customer files and are progressively updating customer information.	• A manual transaction monitoring system that was inadequate for the volume of transactions. This included setting transaction thresholds too high. An example we have seen is a threshold of $1m for all transactions. • No process for updating existing customer files or not being aware of ongoing CDD obligations in certain circumstances.

• Electronic transaction monitoring systems were established with rules that applied to the local New Zealand business. Alerts are reviewed daily with a full record retained of what actions are taken on each alert.	• Businesses being unable to demonstrate that the rules for the automated systems have been appropriately tailored to their business.

Suspicious transaction reports

Section 40 of the Act requires suspicious transactions to be reported. These obligations are essential for compliance with the Act. They are a basic requirement for any AML/CFT framework, as suspicious transaction reports (STRs) are a key part of the FIU's intelligence. It is an area we strongly focus on in our monitoring.

Every transaction monitoring system (manual or automated) generates alerts for transactions that may be suspicious. Alerts must be analysed and/or investigated to determine whether they should be closed, investigated further, or reported to the FIU.

The FIU offers training for those who would like help, such as training in 'what is suspicious' and 'how to enter STRs'. See their website for more information (http://www.police.govt.nz/advice/businesses-and-organisations/fiu).

What we expect:

- A better understanding of what transaction or account monitoring system works best, and how to determine 'unusual' transactions.
- An increase in suspicious transaction reporting.
- Reporting entities to be registered for the FIU's goAML facility and to have been trained by the FIU.

What we found:

- The reporting of suspicious transactions to the FIU has traditionally been low in the sectors we supervise. This concerns both us and the FIU. We believe some firms and individuals are not fully aware of what constitutes a suspicious transaction or are not appropriately monitoring customer transactions or accounts. We will be examining on monitoring visits how decisions are made about whether a suspicious transaction report should be filed with the FIU.
- Those who have filed STRs generally have robust transaction monitoring systems and processes, including a sound process for investigating alerts.

Examples of good practice	Examples of unsatisfactory practice
• A recently updated process for investigating suspicious transactions, including confidentiality considerations and good documentation on outcomes. • Businesses following up on STRs rejected by goAML to correct deficiencies (usually formatting issues) and resubmitting them.	• Alerts reviewed but insufficient detail recorded about what the alert related to, what was investigated, what was decided, and the reasons for the decision. • Poor record-keeping which made it difficult to determine the date when a particular suspicion arose.

Nature and purpose of the business relationship

Under sections 17, 21 and 25 of the Act, reporting entities are required to get information on the nature and purpose of the proposed business relationship with their customers. This information should be collected as part of accepting a customer. It includes understanding what the customer is trying to achieve, how much business (volume and value) is expected, and how regular their interactions will be. If the customer follows the given profile, there is no need to conduct CDD for every transaction. However, it would be prudent to request more information if the customer's behaviour changes significantly.

What we expect:

- Policies and procedures should clearly define what would be a material change in the nature and purpose of a business relationship.
- Information on the nature and purpose of the business relationship is collected when a new customer signs up, or if CDD is required on an existing customer.
- Nature and purpose are two separate items. Requesting information on them separately on an application form is likely to provide better quality information.
- Customer-declared changes to the nature and purpose of the business relationship should be monitored, as they could indicate AML/CFT information.
- Being able to explain how the information collected about the nature and purpose of the business relationship complies with the obligations under sections14(c) and 31(2)(a) of the Act.

What we found:

- Many firms and individuals do not distinguish clearly enough between the nature of a business relationship (what the customer is bringing to the business relationship) and purpose of the business relationship (why they want this particular product or service).

Examples of good practice	Examples of unsatisfactory practice
• Businesses able to link nature and purpose information directly to their transaction and account monitoring procedures. • Businesses that have substituted 'nature and purpose' wording in application forms for other questions and phrases such as 'how much do you intend to invest' and 'how often do you plan to invest with us'. This wording can often be clearer for customers and can provide more consistent information.	• Customer application forms that collect poor quality or generic information that is inadequate to determine both the nature and the purpose of the business relationship.

Governance and management oversight

Section 57 of the Act requires reporting entities to have adequate and effective procedures, policies and controls for, among other things, monitoring and managing compliance with their procedures, policies and controls. Management oversight (including governance) of AML/CFT obligations was covered in our previous AML/CFT monitoring report. However, we are still seeing a few examples of poor AML/CFT oversight by senior management and boards. In some cases, management are getting no information, or very limited information, on ongoing compliance with the Act.

What we expect:

- Adequate reporting structures (such as a risk committee or board) for regular AML/CFT reporting, and processes for escalating material matters to senior management or governance committees, with clear responsibility for decision-making.
- Transparent reporting and scrutiny of recommendations made by AML/CFT compliance officers, including escalation where management differs from recommendations.

Examples of good practice	Examples of unsatisfactory practice
• Regular reports submitted to a risk and compliance committee, including instances where there has been a compliance investigation into an unusual or suspicious transaction. This is followed by regular updates or progress into any investigations that could result in an STR being filed.	• No AML/CFT reporting to senior management or the board, and no requests from the board. This is likely to hinder compliance with AML/CFT obligations. • AML/CFT reports that regularly use stock phrases such as 'no suspicious transactions reported', without reporting information such as the number of unusual transactions examined, the number of accounts examined, the length of investigations, and emerging themes.

Electronic customer due diligence

Part 3 of the IDVCOP allows for electronic identity verification. More businesses are starting to consider electronically verifying the CDD information they get from customers, to improve the customer experience and reduce time and cost. However, some are concerned about the risk of someone's identity being stolen and used to open an account. Fraud risk should not be a barrier to using electronic identity verification, as you should have controls to reduce the risk of fraud as part of your overall controls.

- Identify theft is a different risk to money laundering or terrorist financing. We expect controls and robust procedures for detecting and decreasing the risk of fraud. However, this doesn't have to be part of an AML/CFT programme.
- Identity theft is more likely to be used to try to withdraw funds, than make deposits (and open new accounts).
- Paper-based verification can also be used for fraud.
- Controls to reduce fraud risk (some of which also help to support verification of identity) could include:
  - contacting a new customer either during the sign-up process or once the account is approved to confirm their identity and/or address

- not releasing funds until customers have verbally confirmed their instructions (by phoning the customer using the contact details on their file)
- only making payments to customers' documented bank accounts
- requiring a bank slip for changes to customer bank accounts.

Source of customer funds or wealth

Under sections 23(a) and 24(1)(b) of the Act, reporting entities are required to take reasonable steps, depending on risk, to verify information on the source of funds or wealth of the customer. We have noted that some businesses are not always getting and/or verifying this information, when an obligation for enhanced due diligence (EDD) is triggered.

A bank account or statement is unlikely to be sufficient evidence of the source of funds. The source is not where the money is being transferred from (which is likely to be a bank account). Source and wealth both point to where the funds originated. It is also insufficient to simply say 'inheritance', for example. An explanation of who the inheritance came from, when, how much, and where will the funds transfer from, would be needed. This information would need to be verified.

The extent of verification is based on the customer's risk. Verifying evidence is similar to verifying identity documents, such as sighting originals and getting original certified copies. Firms and individuals must be able to explain the risk they assign to an EDD customer, with documented conclusions.

AML/CFT audits

Under section 59 of the Act, a reporting entity must ensure its risk assessment and AML/CFT programme are independently audited every two years, or at any other time at our request. We may also request a copy of any audit report. For many firms and individuals, this was the first year they were required to get an audit.

Since the Act came into force, we have been provided with about 160 audit reports by firms and individuals we supervise, including about 112 audit reports reviewed in the year to 30 June 2015. For some, we brought forward the completion date for their audit. Others volunteered copies of their audit reports. Each audit report is reviewed and, where material issues are identified, a full desk-based review is completed.

The auditors' findings were similar to those we identified on our monitoring visits, and similar to the previous period's. Most firms and individuals have some remediation work to do post-audit. However, we noted an improvement that we believe is partly due to the guide attached to last year's monitoring report, and partly due to increased learning and understanding by auditors.

Around 20% of the audit reports we requested identified issues that were significant enough for us to contact the firm or individual to discuss further, and in some cases required further action.

We will continue to focus on auditor independence. We hope that many businesses establish and benefit from a trusted relationship with their auditor. Many auditors also offer consulting and other AML/CFT services, and businesses need to determine whether these extra services, if used, could jeopardise the auditor's independence.

Staff training

Under section 57 of the Act certain staff must be trained on AML/CFT matters. Staff training should be an ongoing process. Some businesses provided training pre-30 June 2013, but have not continued it. It is important that

appropriate, targeted training is given at regular intervals. This is especially important for frontline and compliance staff, but should also include senior management and board members. Good practice we have seen is a scheduled training programme with a required pass mark. At the very least, businesses should regularly test the AML/CFT competency of appropriate staff. If staff do not perform well in these tests, extra training is required.

Breach reporting

This year we have seen instances of businesses self-reporting breaches of their obligations under the Act. This usually follows an independent audit, when the breach is considered serious enough to report to the relevant supervisor. The breach report has been accompanied by a timeline of remedial action to rectify the breach. We encourage this and will follow up progress on this with the business.

Businesses that engage with us positively in this manner may reduce the likelihood that we will need to carry out a direct supervisory visit in the future.

Directors of a trustee company

We are aware through our monitoring activities, and from queries we have received during the year, that there is still some confusion about how far CDD should extend with corporate trustees.

We would expect CDD for a director of trustee company if:

- the individual had effective control over the trustee of a trust, as they would be a beneficial owner of the customer – section 11(1)(b) of the Act; or
- the individual was authorised to act on behalf of the trustee of a trust, as they would be acting on behalf of the customer – section 11(1)(c) of the Act.

We would expect the reporting entity to establish which director(s) of the trustee company satisfy those characteristics. We would not expect CDD for a director of a trustee company who does not satisfy either of the above characteristics. We acknowledge that it can be difficult to establish that a director of a trustee company does not satisfy either of these characteristics.

Appendix 1: Snapshot of the AML/CFT sector

800 approximate number of firms and individuals required to file annual AML/CFT returns

60% are located in Auckland, Christchurch and Wellington

7% have overseas owners

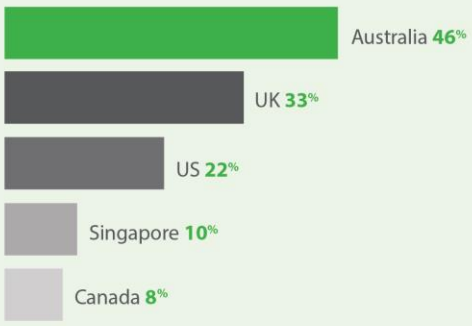
12.5% are members of a designated business group

7.9% have identified politically exposed people

59% have at least one non-resident customer

5% have more than 500 non-resident customers

Non-resident customers



49% sign-up new customers face-to-face

25% do not meet face-to-face to sign up 90% of their customers

Around 800 firms and individuals are required to submit an annual AML/CFT report to us on their risk assessment and AML/CFT programme. These are due by 31 August each year, and cover the year to the end of June. Data collected from these reports helps us:

- understand the risk in each reporting entity and the sectors we supervise
- ensure our information about these reporting entities is accurate and up-to-date
- determine the best use of our resources.

The following data covers the year to the end of June 2015.

Location

- 83% were concentrated in the main cities.
- 40% were located in Auckland.
- 10% were located in Christchurch and 10% in Wellington.
- Excluding adviser businesses, 90% were based in Auckland, Christchurch or Wellington.
- There was a higher concentration in Auckland of collective investment schemes (77%), brokers (60%), issuers (58%) and futures dealers/derivative issuers (63%).

Location is one of the factors we consider when allocating our monitoring resources.

Ownership

- 93% had New Zealand owners.
- 7% had overseas owners.
- Of those owned overseas, 23 were owned in Australia, six in the UK, four in Switzerland and four in the United States. Other overseas locations included China, France, Barbados, Guernsey, Hong Kong, Japan, Malaysia, Singapore, Turks and Caicos Islands, United Arab Emirates, and the British Virgin Islands.

We have observed that businesses with an overseas owner often model their risk assessments and compliance programmes on foreign requirements or group documentation. It is often difficult for them to comply with New Zealand requirements as our Act is unique. We recommend these businesses pay particular attention to the obligations in our Act and ensure there is no confusion in their documentation.

Designated business groups

- 12.5% were members of a designated business group. This is similar to the percentage in 2014.

Under section 5 of the Act, a designated business group (DBG) is essentially a written agreement between two or more related people to form such a group. Members of a DBG may rely on another member to carry out some of its obligations under the Act, such as sharing an AML/CFT compliance officer, having one audit performed across the group, and a maintaining a common AML/CFT compliance programme. Some members also rely on other members to perform CDD obligations for them.

Given the potential benefits, we are slightly surprised at the relatively low number of eligible businesses forming a DBG. Some appear to think that DBGs are only suitable for larger companies with multiple legal entities. The process of forming a DBG is relatively straightforward and we encourage businesses to review their eligibility to do this.

More information is available on our website.

Politically exposed people

- 7.9% identified politically exposed people (PEPs) they have a business relationship with. This is up from 5.7% the previous year.

Under section 5 of the Act, PEPs are individuals who, due to their position in public life, may be vulnerable to corruption. The Act currently limits this concept to foreign PEPs. Reporting entities are required to consider the risks involved with PEPs and should:

- have procedures to determine whether a customer, or a beneficial owner of a customer, is a PEP or a close associate of a PEP
- get senior management approval for establishing or maintaining business relationships with PEPs
- take reasonable measures to establish the source of wealth and source of funds of PEPs
- regularly monitor the business relationship.

We believe the higher number of PEPs could be due to better processes that allow easier identification of PEPs, and more examination of existing customers, rather than more PEPs transacting in New Zealand.

Non-resident customers

- More than half (59%) had at least one non-resident customer, 21% had more than 10 non-resident customers, and 5% had more than 500 non-resident customers.
- Just under half (46%) had a customer in Australia, 33% had a customer in the UK, 22% had a customer in the USA, 10% had a customer in Singapore, and 8% had a customer in Canada.
- Less than 2% of reporting entities also had customers in countries that could be considered high risk (such as those identified by FATF as lacking adequate AML/CFT controls).

We recognise that for many businesses, non-resident customers are often expatriate New Zealanders who may have originally been accepted in New Zealand and subsequently moved abroad. A customer from a country that is considered high risk may require greater monitoring.

Channels used to identify new customers

- Nearly half accept new customers by meeting them face-to-face.
- About two-thirds meet more than 90% of their new customers face-to-face.
- About a quarter do not meet face-to-face with more than 90% of their new customers.
- Less than 5% use domestic intermediaries, and less than 2% use overseas intermediaries.

The way a business delivers its products and services affects its susceptibility to money laundering or the financing of terrorism. Not meeting face-to-face with new customers may make it more difficult to verify their identity.

Appendix 2: How we engaged with the sector

Who we choose for monitoring is based on our 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, their compliance history, and complaints. Our monitoring is focused on what we believe are the potential areas of greatest harm.

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

	Monitoring		AML/CFT audit reports reviewed			
Sub-sector	On-site	Desk-based	No follow-up engagement	Direct follow up engagement	FMC Act licensing	Total
Derivatives issuers	3	1	3	4	14	25
Fund managers	6	3	25	8	7	49
Brokers and custodians	1		9	2		12
Financial advisers	2		40	12		54
Issuers of securities			1	5		6
Licensed supervisors and trustee companies			1	1		2
DIMS providers			1		5	6
Equity crowdfunders					6	6
Peer-to-peer lenders					2	2
Total	**12**	**4**	**80**	**32**	**34**	**162**

It should also be noted:

- In a small number of cases, a firm or individual may have been counted twice in this table, as they would have been examined as part of our monitoring, as well as during a licence assessment.
- We perform many more on-site and desk-based reviews of financial advisers for compliance with the *Financial Advisers Act 2008*. Many of these are also reporting entities for AML/CFT. Although we discuss their compliance with AML/CFT obligations, we do not do detailed testing. We have therefore excluded these engagements from this table.
- Although we did not specifically target issuers, some of the businesses we engaged with are also issuers. We partly base our monitoring on sector risk assessment. As part of this assessment, issuers came out the lowest risk.
- The *Financial Markets Conduct Act 2013* (FMC Act) introduced licensing for many of our reporting entities including derivatives issuers, fund managers, equity crowdfunders, peer-to-peer lenders and DIMS providers. As part of assessing FMC Act licence applications, we examine AML/CFT documentation provided.

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.
EDD	Enhanced due diligence, as defined in sections 23-30 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 (30 June 2013).
goAML	A reporting tool that allows the rapid and secure exchange of information relating to STRs between reporting entities and the Financial Intelligence Unit.
PEP	Politically exposed person, as defined in section 5 of the Act.
Reporting entity	A firm or individual as defined in section 5 of the Act.
Risk(s)	Risk of money laundering and terrorist financing.
STR	Suspicious transaction report, made under section 40 of the Act through goAML.
the Act	The *Anti-Money Laundering and Countering Financing of Terrorism Act 2009* and its regulations.