FMA

FINANCIAL MARKETS AUTHORITY

TE MANA TATAI HOKOHOKO - NEW ZEALAND

Anti-money laundering and countering financing of terrorism monitoring report

December 2016

Purpose of this report

This report summarises our monitoring activities to help firms and individuals better understand our expectations and how they can improve their systems and processes, to comply with the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the Act).

This report covers the period from 1 July 2015 to 30 June 2016. It was our third year of monitoring compliance with the Act. We focused on:

- on-going customer due diligence
- identification and monitoring of high-risk customers
- governance and management oversight.

We chose to focus on these areas based on our observations from previous monitoring and analysis of annual return information. Governance and management oversight is part of our focus and aligns with our strategic priorities.

FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TATAI HOKOHOKO - NEW ZEALAND

fma.govt.nz

AUCKLAND
Level 5, Ernst & Young Building 2 Takutai Square, Britomart PO Box 106 672, Auckland 1143
Phone: +64 9 300 0400 Fax: +64 9 300 0499

WELLINGTON
Level 2, 1 Grey Street PO Box 1179, Wellington 6140
Phone: +64 4 472 9830 Fax: +64 4 472 8076

December 2016

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. Our role includes monitoring certain people and organisations for compliance, and providing 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 a nd the Asia/Pacific Group on Money Laundering.

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

Our findings

REs have made some progress towards meeting their anti-money laundering and countering of financing of terrorism (AML/CFT) obligations.

The areas we highlight in this report are of particular interest, and should be carefully considered by management and boards.

- We are particularly concerned about the continued low level of filing of suspicious transaction reports (STR) by REs. We plan to address this in 2017 by conducting training jointly with the Financial Intelligence Unit (FIU).
- We issued one public formal warning under section 80 of the Act during the year. For more information on the nature of the warning see the **Governance and management oversight** section of this report.
- We continue to see a lack of staff training effort to detect and prevent money laundering and terrorist financing (ML/FT) activities.
- We continue to see variances in the quality and way in which REs conduct due diligence on high-risk customers.

Future focus

Coming into the fourth year of the regime, firms and individuals have had time to become familiar with their obligations under the Act. We expect that REs have internal controls in place which are working. We will focus our monitoring on the programme of work to update, and maintain AML/CFT documentation, as well as management and board oversight.

REs need to consider carefully the findings and observations set out in this report to ensure they are compliant with the Act. The legal obligations on REs under the Act have been in place now for three years. In future, the FMA will be adopting a stronger position where it sees a failure to meet these obligations.

Governance

In line with our strategic priorities, we also continue to focus on governance. This helps us understand how REs have embedded the right culture in AML/CFT practices for their organisations at a senior management level. We will also look at how REs ensure their staff are trained to a satisfactory standard, and what on-going training programmes are in place.

Next year we will be increasing our desk-based and on-site monitoring, looking for compliance with the Act.

Our findings and observations

Staff training

Under section 57 of the Act senior managers (including boards of directors), the AML/CFT compliance officer and any other employee engaged in AML/CFT related duties, must be trained on AML/CFT matters. We have outlined our expectations for training in our **2015 report.** However, we continue to see a lack of staff training within some REs.

Our expectations:

- Staff must be fully trained to be aware of their role to detect and prevent criminals from using their business as a conduit for money laundering and terrorism financing.
- Staff training is an on-going process and must be targeted to the audience. For example, frontline staff would have different training requirements to back office staff or directors.
- Staff training is an integral part of any AML/CFT programme and knowledge must be kept up to date.

Our findings:

- Some REs had provided training pre-30 June 2013, but have not continued the training or trained new staff.
- REs who have a structured training programme, generally, have a more proactive AML/CFT culture. We expect the heightened awareness of staff of AML/CFT matters should also lead to a higher number of STR filings.

Examples of good practice	Examples of unsatisfactory practice
• All new staff, where required under section 57(b) of the Act, have completed AML/CFT training as part of their induction. • We found some REs regularly test the AML/CFT competency of appropriate staff. • Tailored training was carried out for board members and more detailed training provided to front line staff. • One RE had a scheduled training programme with a required pass mark. Staff who did not pass were identified for further training.	• Some REs provided training before 30 June 2013 and have not continued to do so. • REs who do not carry out staff training on AML/CFT are breaching their obligations under the Act.

Governance and management oversight

Section 57 of the Act requires REs to have adequate and effective procedures, policies and controls to monitor and manage compliance.

In May 2016, we issued a **formal warning to Craigs Investment Partners** (Craigs) for failing to conduct adequate enhanced due diligence, and failing to terminate its business relationship with a client when it had been unable to complete the required level of customer due diligence on that client.

In our view, whilst Craigs had made efforts to update its compliance programme, there were deficiencies within the programme after the introduction of AML/CFT Act on 30 June 2013. Craigs did not have a cohesive process for escalating, monitoring and managing AML/CFT issues, and for ensuring compliance with the AML/CFT compliance programme.

We recognise the deficiencies in the operation of Craigs' AML/CFT programme existed relatively soon after the introduction of the AML/CFT regime in 2013. The warning related to conduct in 2014 and Craigs has, since 2014, taken steps to significantly improve its AML/CFT compliance programme, reducing the chances of similar breaches occurring in the future.

We consider that if the issues were to be identified in an RE now, it would likely attract a stronger regulatory response.

Our expectations:

- Senior management and boards must have oversight of AML/CFT matters.
- REs must have a documented process for escalating material matters to senior management or governance committees, including escalation procedures for instances where management views differ from the recommendations of the AML/CFT officer.
- REs must have robust structures in place to adequately record recommendations and decisions made. This ensures the RE is able to show the rationale for these decisions.

Examples of good practice	Examples of unsatisfactory practice
• Compliance staff submit reports on a regular basis to a risk and compliance committee, including details of the compliance assurance activities performed. • Examples of compliance assurance activities include: how many records have been examined, what the success rate is, what the common issues are in customer due diligence (CDD) documentation, or what actions were taken to address any issues or trends identified. • A documented process within the AML/CFT programme for terminating relationships when a client's CDD fails.	• Reporting by exception. • Reports containing phrases such as "there were no suspicious transactions reported" or "sampling of CDD records carried out".

Due diligence on high-risk customers

Under section 57(c) of the Act, compliance with CDD obligations is a minimum requirement for AML/CFT programmes.

After the release of the *Panama Papers*, we carried out a number of targeted visits. Our visits focused on how REs were meeting their obligations in the following areas:

- Policies and processes for identifying higher-risk customers and customers who are subject to enhanced due diligence.
- Processes for identifying whether the RE has had any business relationship with Mossack Fonseca and its affiliates.
- Policies and processes for on-going monitoring, including identifying pre-30 June 2013 high-risk customers; and carrying out appropriate due diligence of these customers.
- How REs gain assurance that their policies, procedures and controls can identify high-risk customers, and that appropriate due diligence is carried out.

Our findings:

REs tend to be on either end of the compliance spectrum. At one end, we saw good written policies and procedures with well-documented reasons for escalating processes to senior management.

At the other end, we found organisations with informal structures in place with little or no documentation.

Our expectations:

- High-risk customers must be reviewed more frequently than low-risk customers; they should also be flagged for on-going CDD and targeted transaction monitoring.
- The on-boarding of all high-risk customers must be signed off by management. A written process must be in place to ensure issues are appropriately escalated to senior management and fully documented, including the outcome.
- A robust and transparent governance process to manage interactions with high-risk customers should include periodic reviews to assess where the RE sees itself on the compliance maturity scale to address identified weaknesses. For example, a starting point should be the findings of your section 59 independent audit report.
- Customers who appear to have no commercial connection with or business in New Zealand be treated as an indicator of higher risk. Staff should be required to carry out additional due diligence on these customers.

Examples of good practice	Examples of unsatisfactory practice
• Sound written policies specific to high-risk customers and corresponding procedures with documented escalation processes to senior management. • Documented reasoning which sets out the rationale for accepting or rejecting a high-risk customer.	• No written processes embedded, or processes were not well understood by staff. • Processes were documented. But there was no documentation of the rationale for decisions made.

On-going CDD and account monitoring

Under section 31 of the Act, REs are obliged to conduct on-going CDD and account monitoring on new and existing customers.

We understand that most REs had pre-existing clients before the Act came into force in 2013. Therefore, the identity documentation on these customers is unlikely to be in line with current policy requirements. This lack of CDD documentation may reduce the effectiveness of the on-going CDD activities.

Our expectations:

- REs should at least develop a plan to identify high-risk customers, and bring their documentation up to current standards.
- Where customers lack sufficient documentation, REs should understand and document the nature and purpose of the business relationship.
- REs have an insightful transaction monitoring system that can protect the entire business against risks of ML/TF.
- REs gain an in-depth customer knowledge that will alert them to unusual customer activity, and serve as a red flag for investigating whether an activity is normal, or should be classified and filed as an STR.

Our findings:

Some REs are increasingly using sophisticated software to help them monitor transactions, and have demonstrated a good understanding of their customer's normal business activity. Other REs, such as smaller financial adviser businesses, may not need a sophisticated transaction monitoring system. We expect that each RE is able to appropriately monitor transactions and patterns of transactions.

As we reported in 2015, in some cases we are still finding the following:

- Monitoring systems were not fit for purpose. Systems used were either manual, or monitoring was infrequent.
- REs did not have a written process for investigating alerts and, at times, no audit trail of investigations.
- A lack of reports on suspicious transactions.
- Some REs showed a lack of knowledge about their existing customers or had no plan or process to review information on existing customers.

Examples of good practice	Examples of unsatisfactory practice
• An RE with 2,000 customers on-boarded before 30 June 2013, has a plan, signed off by senior management, to review all customers. • Using a risk-based approach, where necessary, the RE will be bringing client documentation in line with current obligations.	• No plan or process to update existing customer records on-boarded prior to 30 June 2013. • Not being aware of on-going CDD obligations in certain circumstances. • REs have no risk rating for existing customers; this is a concern, especially when customers need to be assessed as high-risk, or when enhanced due diligence was required (under their current CDD policy). • REs cannot show that the rules for their automated systems have been appropriately tailored to their business.

Electronic CDD

Part 3 of the Identity Verification Code of Practice (IDVCOP) allows for electronic identity verification.

More REs are considering 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 for REs to use electronic identity verification, as their overall controls should include details about how they plan to reduce the risk of fraud.

REs considering using electronic identity verification must carry out appropriate due diligence on their product provider. The service agreement with the chosen provider must cover these two important points.

The product:

- complies with the IDVCOP
- secures and protects customer information.

Note: We do not endorse or recommend product providers.

Financial Intelligence Unit & STRs

GoAML

All REs need to be registered with **GoAML** to enable to them to report STRs, receive the quarterly FIU Typology Report, and also important updates from the FIU. When the FIU send updates, REs will receive an email message. REs will need to log in to their account to view the message in the **GoAML** inbox.

REs need to read these messages – they are important. They will help keep REs updated and will ensure REs are fully aware of their requirements. All questions or issues on **GoAML** should be directed to the **FIU.**

Suspicious transaction reports

Section 40 of the Act requires suspicious transactions to be reported. Our RE population has filed 47 STRs within this reporting period. Whilst this is a 34% increase since the last report, it only represents a fraction of the 8,415 STRs filed from REs not supervised by us.

In 2017, we will be offering targeted training, with the FIU, to train REs on whether they need to file an STR. This will help staff better understand what the FIU expects of them.

The FIU also offers training for compliance staff, as well as staff who have customer interaction, especially during the on-boarding stage. This will improve knowledge of what is, or may be, suspicious, and help staff to determine when to file an STR.

It is important that all REs are fully aware of how the online **GoAML** portal works and are comfortable using it. For training, contact the **FIU.** Alternatively, **see their website for more information.**

We will send out invitations for the FMA/FIU training sessions in due course.

Our expectations:

- REs need to be registered for the FIU's **GoAML** facility.
- Compliance staff needs to be aware of the **FIU's Typology report**
- An increase in the number of STRs from our REs.

Our findings:

- We continue to see low STRs filings, and are concerned that REs are not fully aware of what constitutes a suspicious or unusual activity/transaction.

Relying on intermediaries

In July 2015 we published an **information sheet on class exemptions for managing intermediaries.**

Feedback suggests that there is a lack of awareness of the existence of the exemption. If you have not already done so, we strongly recommend that you read the information sheet.

Engaging with your supervisor

We are keen to build relationships with those we regulate on a formal and informal basis. While we are unable to provide advice on specific issues, we can provide general comments and guidance. **For all AML/CFT-related queries contact us at: aml@fma.govt.co.nz**

Additions and removals of REs

As part of the annual review of the AML programme, we recommend REs review the official AML/CFT RE list on our website. To make changes to the list, **email** us with a brief explanation of your proposed changes. We continuously monitor the market to identify changes to our RE population, and our website is updated as new information becomes available.

Changes to the AML/CFT compliance officer during the year

To ensure we have up-to-date records on AML/CFT matters, we expect all REs to **email** us if their AML/CFT compliance officer changes.

AML/CFT phase 2

REs will be aware that, earlier this year, the Government announced intention to introduce phase 2 of the AML/CFT regime.

Phase two aims to extend the scope of REs to include lawyers, conveyances, accountants, real estate agencies, and dealers in high value goods.

The Ministry of Justice, on behalf of the Minister, has circulated a consultation paper on this. The consultation paper outlined who should be supervisors for these new REs. The paper is currently in the process of being reviewed by Cabinet. At this point in time, we do not know the outcome of any Cabinet decision and what impact this may have on the FMA as a supervisor.

Source of customer funds or wealth

As reported last year, we continue to see entities encounter difficulties in this area. As part of the phase 2 reforms, it is anticipated that this will be addressed through either regulation or guidance, or both.

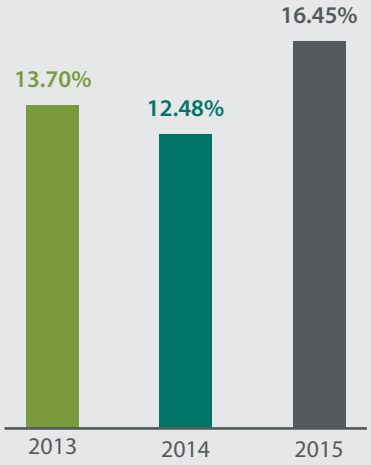
Appendix: How we engaged with the sector

REs are required to file annual reports by 31 August each period, for the year ending 30 June. Data collected from these reports helps to inform our risk-based approach to monitoring the market, to better understand where our REs are located, and what business activities they carried out.

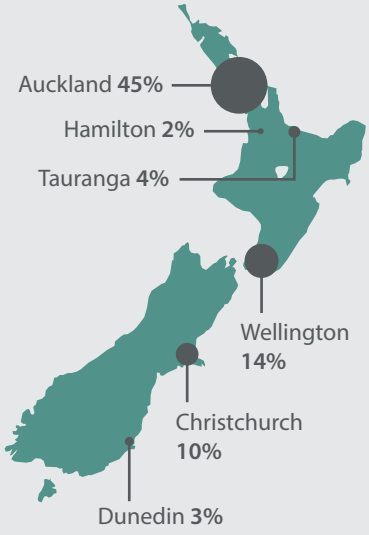
There has been a reduction in the number of late filings of annual reports from previous reporting periods. Late filers are in breach of their regulatory obligations and are recorded for our future monitoring.

Here's a breakdown of REs

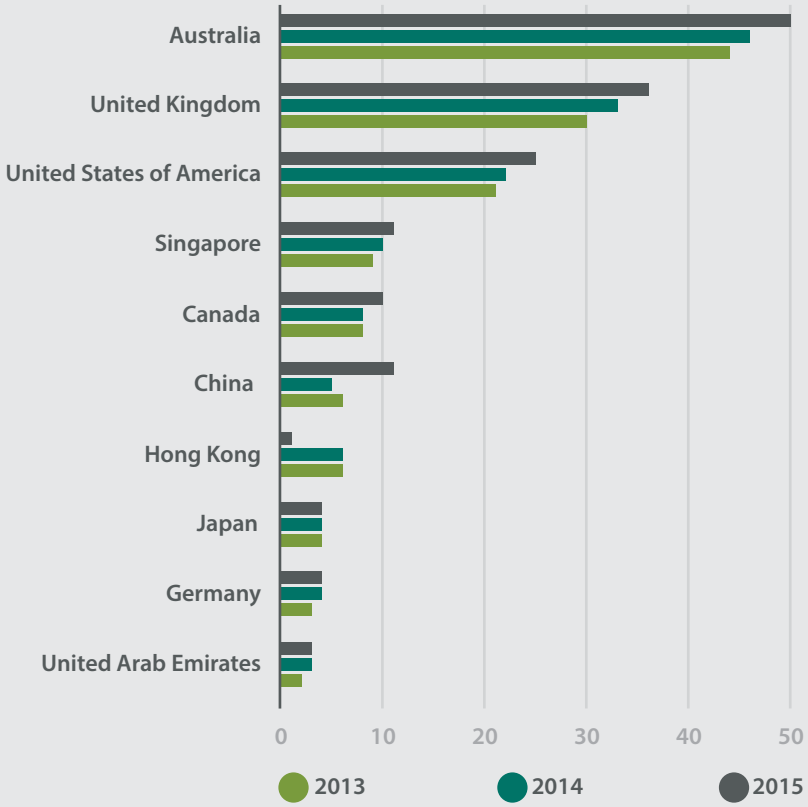
Percentage of REs that are members of a designated business group



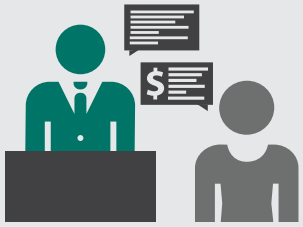
Location of REs



Location of non-resident customers



Face-to-face on-boarding of new customers



49% 2014

43% 2015

Monitoring activity

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

These include:

- 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
- complaints.

During the review period, we did 12 on-site monitoring visits and 12 desk-based reviews. Each visit and review was followed up with feedback reports and other action as required.

We also examined 29 independent AML/CFT audit reports, as well as information required to be supplied to us in the 2014, 2015 and 2016 annual AML/CFT reports.

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

Monitoring

Sub-sector	On-site	Desk-based	Section 59 audit reports	Total
Derivatives issuers	2	1	1	4
Fund managers	4	2	11	17
Financial advisers	3	2	6	11
Issuers of securities		7	11	18
Licensed supervisors and trustee companies	1			1
Equity crowdfunding	1			1
Peer-to-peer lending platform providers	1			1
Total	12	12	29	53

It should also be noted that the desk-based reviews were a result of an initial examination of the 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 that the RE had taken the recommended/suggested actions.

We will continue to ask for section 59 audit reports before our on-site monitoring visits. Initial findings in 2016 show a concerning number of REs who did not complete section 59 audits, and we expect to take regulatory action against these REs.

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)
FIU	Financial Intelligence Unit
GoAML	A reporting tool that allows the rapid and secure exchange of information relating to suspicious transaction report between reporting entities and the Financial Intelligence Unit
IDVCOP	Identity Verification Code of Practice
ML/FT	Money laundering and financing of terrorism
RE	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

FMA

FINANCIAL MARKETS AUTHORITY

TE MANA TATAI HOKOHOKO - NEW ZEALAND