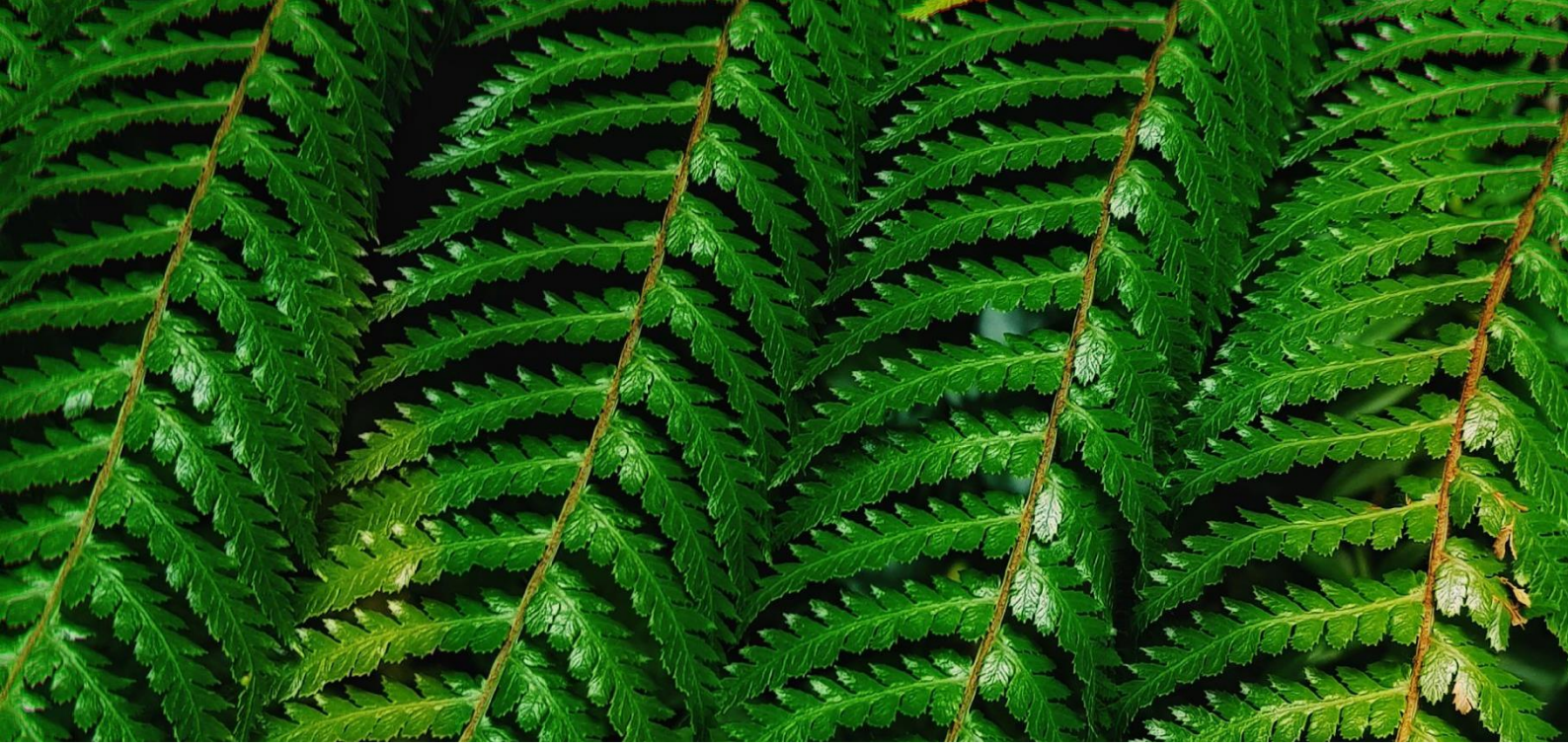


AUGUST 2021

AML/CFT monitoring insights report

Insights from the FMA's monitoring of New Zealand's anti-money laundering and countering financing of terrorism measures by FMA reporting entities from 1 July 2018 – 30 June 2021

FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TĀTAI HOKOHOKO

A message from our Director of Supervision

The period covered by this report has been a very busy one for the FMA's Supervision team, with a number of significant national and international events that affected our reporting entities and how we perform our monitoring activities.

Those events included the terrorist attack on Christchurch mosques in March 2019, which highlighted the importance of reporting entities not only focusing on money-laundering risks within their business, but also considering the risk of terrorist financing within their business. This was followed by the mutual evaluation of the effectiveness of New Zealand's anti-money laundering and countering the financing of terrorism measures by the Financial Action Task Force.

We then had the local outbreak of the COVID-19 pandemic in early 2020, which resulted in lockdowns and reporting entities being unable to onboard customers face-to-face. AML/CFT supervisors responded to this situation by publishing guidelines to help reporting entities comply with AML/CFT verifications during the different COVID-19 Alert Levels. We expect reporting entities that relied on this guidance to have now met all regulatory obligations by completing the delayed verification process for all affected customers.

The pandemic resulted in rapid growth in the use of new technologies by reporting entities, as part of their customer due diligence to do electronic identity verification. These new technologies could change the money laundering and terrorist financing risks faced by businesses. We also noted instances where the rapid growth in customers trading online resulted in processes not being amended to effectively manage the risk of money laundering and terrorist financing within the business. Reporting entities should review their risk assessments accordingly, to determine whether they need to adjust their risk ratings.

As the FMA has previously noted, the AML/CFT regime has matured to a large extent and we therefore have less tolerance for non-compliance with the Anti-Money Laundering and Countering Financing of Terrorism Act. This has resulted in us filing our first AML/CFT civil pecuniary penalty proceedings in the High Court in June 2020. We will continue to take appropriate regulatory action due to non-compliance by reporting entities and have a number of cases currently being considered by our Supervision Response team.

We will continue to work with AML/CFT Supervisors and other agencies in order to improve the level of compliance with the Act by reporting entities in our sector, and encourage reporting entities to engage with the FMA when guidance is required.

James Greig

Director of Supervision

Contents

Executive summary

AML/CFT supervisor's role

The Financial Markets Authority (FMA) is one of three supervisors under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the Act). We work closely with New Zealand's other AML/CFT supervisors, being the Reserve Bank of New Zealand (RBNZ) and the Department of Internal Affairs (DIA), as well as various other agencies, when it comes to supervising AML/CFT reporting entities (REs). The FMA supervises approximately 750 REs as at 30 June 2021.

Our role as an AML/CFT supervisor (as defined in Section 131 of the Act) includes:

- monitoring and assessing the level of ML/TF risk across all FMA reporting entities
- monitoring of REs for compliance with the Act and its regulations
- providing guidance to REs to assist them in complying with the Act and its regulations
- investigating REs for non-compliance with the Act and its regulations
- co-operating via the AML/CFT National Coordination Committee with domestic and international counterparts to ensure the consistent, effective, and efficient implementation of the Act.

We participate in various domestic and international committees with other New Zealand agencies to ensure a consistent and best practice approach is used to supervise REs. Apart from the RBNZ and DIA, these other agencies include the Department of Justice (MoJ), NZ Police's Financial Intelligence Unit (FIU), NZ Customs, Inland Revenue (IRD), the Ministry of Foreign Affairs and Trade (MFAT), and the Ministry of Business, Innovation and Employment (MBIE).

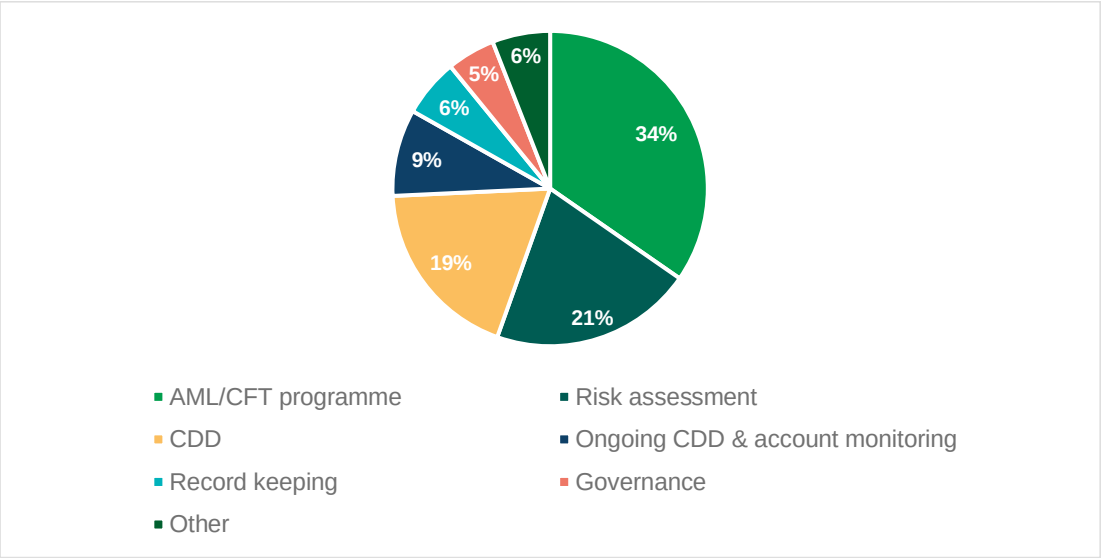
Summary of findings

We conduct regular monitoring activities with REs using a risk-based approach. As part of our monitoring activities we review each RE's compliance with its obligations, including the adequacy and effectiveness of its policies, procedures, and controls to deter and detect ML/FT activities. Our monitoring activities include a mix of desk-based reviews and onsite visits.

During our interactions with REs, we identified non-compliance with basic requirements of the Act. This is disappointing given that the Act has been in place since June 2013. We expect REs to be fully aware of their obligations and to have implemented adequate and effective policies, procedures and controls to ensure compliance.

Our findings include non-compliance in the following key areas:

Chart: AML/CFT non-compliance – key areas



Mutual evaluation

During 2019/20, an assessment team from the Financial Action Task Force (FATF) examined the effectiveness of New Zealand's AML/CFT measures. Their examination included:

- a review of written submissions made by New Zealand
- interviews with a number of government agencies and reporting entities during an onsite visit between February 2020 and March 2020
- a desk-based review of New Zealand's technical compliance with FATF recommendations.

New Zealand's report was discussed at the FATF Plenary in February 2021, where the findings and recommendations were finalised. The final Mutual Evaluation Report (MER) was published on 29 April 2021. Overall, the report is a positive result for New Zealand. The findings are broadly in line with what we anticipated, with New Zealand doing well on the effectiveness of our AML/CFT regime. We have improved our technical compliance since 2009, but there is room for further movement.

Enforcement actions

Enforcement actions are taken in situations where we identify serious breaches and/or non-compliance with the Act. For this purpose, we use a range of regulatory tools in our response, including private and public warnings, and civil or criminal proceedings.

Formal warnings

During the review period, there were 27 formal warnings issued under section 80 of the Act, for breaches of the Act. They included three public warnings:

- In October 2019, to a non-licensed derivatives issuer and forex provider, Circle Markets Limited

- In April 2020, to a sharebroker, Tiger Brokers (NZ) Limited
- In August 2021,[1] to a provider of client money or client property services, Sharesies Limited

Most of the private warnings resulted from REs failing to complete their independent audits within a two-year period.

Other reasons for formal warnings included failure to:

- establish, implement and maintain an AML/CFT programme, or conduct a risk assessment
- appoint an AML/CFT compliance officer
- obtain information from customers about the nature and purpose of the proposed business relationship
- obtain sufficient information to determine whether customers should be subject to enhanced customer due diligence (CDD)
- complete identity verification for a large number of customers as part of standard CDD
- submit an annual AML/CFT report to the FMA by the 31 August deadline
- take reasonable steps to verify customers' identity and/or proof of address
- identify politically exposed persons (PEPs)
- obtain and verify additional identity information needed for enhanced CDD
- conduct ongoing CDD
- remediate breaches identified in AML/CFT audits
- report suspicious transactions to the FIU.

Civil proceedings

In June 2020, the FMA filed civil pecuniary penalty proceedings in the High Court at Auckland against CLSA Premium NZ (CLSAP NZ – formerly KVB Kunlun NZ) for alleged breaches of the Act. This is the FMA's first proceeding against an RE since the Act came into force, and reflects our willingness to take stronger regulatory actions in cases of serious non-compliance.

CLSAP NZ and the FMA subsequently filed an agreed statement of facts in which CLSAP NZ admitted the following breaches of the AML/CFT Act:

- Failure to conduct customer due diligence as required by Part 2
- Failure to terminate an existing business relationship in accordance with section 37
- Failure to report suspicious transactions/activity as required by section 40
- Failure to keep records in accordance with sections 49 and 50.

[1] This monitoring activity was undertaken during the period under review, hence its final outcome was included in the report even though it was finalised after 30 June 2021.

On 5 July 2021, a court hearing for a pecuniary penalty against CLSAP NZ commenced. A final judgement is pending. The maximum pecuniary penalty for each of the alleged breaches is $1 million for a company.

Future focus

We will continue to apply a risk-based approach to monitoring REs. It is eight years since the Act and its regulations came into force, so REs have had enough time to develop and implement adequate and effective policies, procedures and controls to mitigate the risk of ML/TF in their businesses. We intend to perform desk-based and onsite reviews for longer durations, with more in-depth assessment of customer onboarding, account and transaction monitoring, and reporting of suspicious activity to the FIU.

We will also further enhance our analysis of information submitted by REs in their annual AML/CFT reports.

The COVID-19 pandemic had a significant impact on many of our REs and their ability to onboard new customers and perform account monitoring. To assist, we issued specific guidance to REs in this regard (See: Guidance complying with AML/CFT verification requirements during COVID-19 alert levels). In our future monitoring of REs we will assess how much REs relied on this guidance, and if they did so, whether it was applied correctly.

We are currently reviewing the reporting entity population within the financial adviser industry, due to the enactment of the Financial Services Legislation Amendment Act 2019 (FSLA) and the introduction of licensed Financial Advice Providers (FAPs). Close to two-thirds of the REs supervised by the FMA before March 2021 (when FSLA became effective) were financial advisers. Because of that, we are likely to see some developments in this sector. We will closely monitor these changes to determine if there is any material change in the level of ML/TF risk within the sector.

We encourage REs to review the findings and observations in this report and, where required, update their AML/CFT policies, procedures and controls accordingly, to ensure compliance with their obligations.

Our findings and observations

As part of our role as AML/CFT supervisors, we monitor REs for compliance with the Act and its regulations. In doing so, we perform onsite visits and desk-based reviews, and review independent audit reports. Our findings during the monitoring activities we have undertaken are analysed below.

Summary of findings

From 1 July 2018 to 30 June 2021, we conducted 60 monitoring reviews, including 36 onsite visits and 24 desk-based reviews. From those reviews we identified 363 findings requiring remedial action – summarised below. The most common areas requiring remediation were to do with AML/CFT programmes, risk assessments, and CDD. Note: 2020/21 monitoring activities were impacted by COVID-19. At Alert Levels 3 and 4 we paused onsite monitoring while remaining vigilant to any issues raised by REs.

Table: Findings requiring remedial action – key areas

	Total	High	Medium	Low
Year				
2018/19	198	45	87	66
2019/20	132	21	83	28
2020/21	33	8	23	2
Type of findings				
AML/CFT programme	126	19	67	40
Risk assessment	75	11	42	22
Standard CDD	53	17	28	8
Enhanced CDD	17	9	8	0
Ongoing CDD	24	5	10	9
Account and transaction monitoring	9	2	5	2
Governance	18	5	8	5
Record keeping	20	0	14	6
Audit	10	4	5	1
Training	7	1	4	2
SAR	2	1	0	1
Annual Reports	2	0	2	0
Total	**363**	**74**	**193**	**96**

AML/CFT programmes

Section 57 of the Act sets out the minimum requirements for an AML/CFT programme. This includes specific areas where REs must include adequate and effective policies, procedures and controls.

What we found

The majority of our findings in this area related to AML/CFT programmes not meeting minimum requirements by either not including or not adequately describing their policies, procedures and controls in one or more of the specific areas set out in section 57 of the Act. Our findings included breaches in the following areas:

- Customer onboarding processes in relation to complying with CDD requirements
- Processes to determine whether the customer or any beneficial owner is a PEP
- Processes to determine if Enhanced CDD is required
- Ongoing CDD and account monitoring processes
- Reporting of suspicious activities and prescribed transactions
- Outsourced AML/CFT activities
- Examining and maintaining written findings for unusual transactions
- Vetting of senior managers, AML/CFT compliance officers, or any staff engaged in AML/CFT related duties
- Training of senior managers, AML/CFT compliance officers, or any staff on AML/CFT matters

Weaknesses in an entity's AML/CFT programme could result in other areas of non-compliance with the Act. For example, not having sufficient policies, procedures and controls in place to conduct CDD could result in deficiencies when REs carry out CDD in practice, including inadequate identity verification and not obtaining information in relation to the nature and purpose of a business relationship.

We were also concerned with the overall effectiveness of some AML/CFT programmes that did not appear appropriate for the size of the entity, the complexity of business activities undertaken, or the risks identified in the relevant REs' risk assessments.

3 formal warnings (private) **for failures relating to AML/CFT programmes** were issued to REs during the review period.

Our expectations

We expect REs to:

- ensure their AML/CFT programme meets all the requirements of section 57 of the Act and is aligned with their AML/CFT risk assessment
- periodically review their AML/CFT programme (at least annually) to ensure it remains current and fit for purpose

- ensure sufficient records are maintained to confirm that their AML/CFT programme has been reviewed and updated
- refer to the AML/CFT programme guideline produced by AML/CFT supervisors.

Examples of good practice	Examples of unsatisfactory practice
✓ The policies, procedures and controls are adequately designed, and well documented in the AML/CFT programme, clearly explaining who is responsible for activity undertaken and what is expected to perform the activity. ✓ Outsourced AML/CFT activities and the controls of these activities are clearly described in the AML/CFT programme. ✓ AML/CFT programme has clear version control history evidencing each review of the document.	AML/CFT programmes that: x include references that are out of date (for example, some still included reference to 'suspicious transaction report') and no record of review dates maintained x are contained in multiple documents which were not cross-referenced x are not specific to New Zealand and more aligned to overseas legislation x are clearly drafted based on a template that is tailored to a much larger organisation with complex business operations.

Electronic identity verification (EIV)

We note that more and more REs are using EIV as part of their CDD processes. We expect REs opting to use EIV to clearly describe in their AML/CFT programme how EIV will meet the relevant criteria under the Act and Part 3 of the Identity Verification Code of Practice (IDVCOP) and the updated 'Explanatory Note: Electronic Identity Verification Guideline' (For Part 3 of the IDVCOP) published July 2021 (the EIV Guideline).

Clauses 17 and 18 of Part 3 of the IDVCOP require REs using EIV to include the following information in their AML/CFT programme:

- A description of the forms of EIV methods that are considered reliable and independent, and in what circumstances they will be used for the purposes of ID verification
- An explanation of how they considered:
  - accuracy
  - security
  - privacy
  - method of information collection
  - whether the electronic sources have incorporated a mechanism to determine the customer can be linked to the claimed identity
  - whether the information is maintained by a government body (e.g. DIA) or pursuant to legislation (e.g. a credit bureau)

  - if the information has been additionally verified from another reliable and independent source
- An explanation of any additional methods that will be used by the RE to supplement EIV or otherwise to mitigate any deficiencies in the verification process

AML/CFT risk assessment

Section 58 of the Act sets out the obligation to conduct a risk assessment and describes the areas that must be considered for this purpose.

What we found

Risk assessments were found that did not cover all the areas required and/or were not being updated after changes within many/some REs' business.

Areas not considered or not updated by REs to reflect their latest circumstances for the purposes of assessing the risk of ML/TF within their businesses included:

- risk of terrorist financing
- institutions dealt with
- countries dealt with
- products and services offered
- the nature, size, and complexity of the business
- type of customers dealt with.

Some risk assessments did not include references to the material used in the development and articulation of the risks, or an explanation of the methodology of the assessment of risk. It was therefore not clear if the RE had assessed the identified risks in an appropriate and proportionate manner.

Our expectations

We expect REs to:

- review the latest Sector Risk Assessment (SRA) and guidelines issued by the AML/CFT supervisors, for example the FMA's SRA 2017
- ensure risk assessments meet the requirements of Section 58 of the Act
- conduct assessments to identify all the ML/TF risks associated with the business
- review the risk assessment to ensure it remains current and fit for purpose (no less frequently than each year)
- keep records that can evidence that the risk assessment has been reviewed and updated
- consider the Risk Assessment Guideline produced by AML/CFT supervisors.

Examples of good practice	Examples of unsatisfactory practice
✓ The rationale to support risk ratings is clearly described in the risk assessment. ✓ Having a risk rating for each risk assessed and an overall risk rating for the business.	x Not all risks are identified in the risk assessments and assessed, including TF risks, countries and/or institutions dealt with, products and services currently offered. x Contradictions between the content in the AML/CFT programme and the risk assessment. x Identified risks that are not relevant to the business of the RE.

Customer Due Diligence (CDD)

During monitoring we review client files to assess if CDD policies, procedures and controls implemented by REs are adequately designed and operating effectively during the period under review.

Case study: Circle Markets Limited

In October 2019, FMA issued a formal warning to Circle Markets Limited (CML) for failures that included not conducting appropriate and sufficient CDD.

In our view, CML had failed to:

- adequately verify identity information for some customers, as per standard CDD
- obtain additional identity requirements and verify the identity requirements for enhanced CDD for a customer, such as the source of wealth (SoW) and/or source of funds (SoF) of the customer
- take reasonable steps to determine whether a customer or any beneficial owner is a PEP
- conduct adequate ongoing CDD for some customers.

Case study: Tiger Brokers (NZ) Limited

In April 2020, the FMA issued a formal warning to Tiger Brokers (NZ) Limited (TBL) for failures that included not conducting appropriate and sufficient CDD.

In our view, TBL had failed to:

- adequately conduct enhanced CDD and ongoing customer CDD where required
- adequately verify relevant customer identification documents
- obtain adequate SoF or SoW information relating to high-risk customers and take reasonable steps to verify that information
- take reasonable steps to determine whether a customer or any beneficial owner is a PEP.

CDD during customer onboarding

Strong CDD processes for new customers during onboarding are necessary for REs to obtain sufficient knowledge of their customers and the ML/TF risks they might pose to their business. CDD requires the gathering and verification of information about the identity of a customer, any beneficial owner of a customer, or any person acting on behalf of a customer.

What we found

During our review of CDD processes we found:

- inadequate information on the nature and purpose of the proposed business relationship being collected and recorded
- ownership structures not verified to determine beneficial owners of customers (including trusts)
- insufficient or no checks being undertaken to confirm if the customer is a PEP
- verification of identity not conducted in line with the requirements of IDVCOP
- inadequate EIV being done as part of CDD processes, with customers not being linked to the claimed identity or name, and date of birth information not being verified against government databases.

We noted in some instances that exceptions to the CDD policies, procedures and controls were allowed but were not recorded. REs should ensure their CDD procedures only allow for appropriate exception handling. An exceptions procedure should not become the normal procedure. If exceptions are applied, these should be according to internal policies and adequate records must be kept.

Enhanced CDD

The Act sets out specific situations in which enhanced CDD is required. In addition, based on an RE's assessment of the risk involved, enhanced CDD may be required.

One of the key requirements when conducting enhanced CDD is the collection and verification of information relating to the SoW and/or SoF of the customer.

What we found

We found instances of:

- REs that were unable to demonstrate the relevance of the information and documents that were collected to verify customers' SoW and SoF
- staff who did not know how to properly verify SoW and SoF as they failed to take reasonable steps to verify the information collected. In one instance we noted verification of SoW and SoF was only completed by recording vague reasons with no evidential documents being obtained
- enhanced CDD not being done where required.

We encourage REs to read the 'Enhanced customer due diligence guideline' (version March 2019) to get a better understanding of what is expected.

Politically Exposed Persons (PEP) checks

PEP checks must be performed by REs when onboarding new customers, and thereafter on an ongoing basis depending on the level of ML/TF risk. High-risk customers should be checked more frequently.

What we found

We found instances where:

- no PEP checks were undertaken at the time of onboarding and on an ongoing basis where a material change to the business relationship occurred
- PEP policies, procedures and controls were not being adhered to, even when the customer was identified as a PEP
- PEP screening processes were being outsourced, with REs unable to explain the process or confirm whether PEP screening was completed at all
- REs could not provide records of PEP screening results.

REs should review their policies, procedures and controls to ensure that they meet the requirements to perform PEP checks. Where a PEP is identified, the RE must obtain senior management approval to continue with the relationship, and perform enhanced CDD on the customer.

> ***2 formal warnings due to failures relating to conducting PEP checks*** *were issued during the review period*

Our expectations

- REs must ensure they have adequate and effective policies, procedures and controls in place to conduct CDD on all customers, any beneficial owner of a customer, or any person acting on behalf of a customer.
- RE must determine what level of CDD is required based on the level of risk involved with a particular customer.
- Enhanced CDD must be performed by REs on certain high-risk customers, e.g. trusts, PEPs.
- PEP checks must be conducted when the REs establish a new business relationship or when conducting an occasional transaction or activity.
- Evidence of PEP checks performed must be kept on customer files.

Examples of good practice	Examples of unsatisfactory practice
✓ Having a risk rating for each customer which is used to determine frequency of ongoing CDD. ✓ Where material change to the business relationship occurs, customers are flagged for ongoing CDD review.	x Identity verification documents accepted by RE for CDD not meeting requirements as per the IVCOP. For example: x accepting a certified copy of a certified copy of a passport x accepting certified copies that were certified more than 3 months earlier x verification of documents not being conducted x for the purpose of enhanced CDD, not determining a threshold for large investment that would trigger the requirements to conduct enhanced CDD x not considering red flags mentioned in the FMA's SRA 2017 for the purpose of designing the CDD-related processes.

Ongoing CDD and account monitoring

Section 31 of the Act requires REs to conduct ongoing CDD and undertake account monitoring with customers on an ongoing basis. The purpose of this is so REs ensure that they maintain a sufficient level of knowledge about the business relationship and the transactions relating to that customer. This also helps REs identify any grounds for reporting a suspicious activity.

What we found

We found instances of REs:

- continuing to struggle in performing ongoing CDD and account monitoring
- not conducting any ongoing CDD or only performing minimum account monitoring
- using policies, procedures and controls that were not adequately designed, e.g. processes that did not explain how ongoing CDD will be undertaken, whether the approach was risk-based or a random selection of customers, and what checks will be undertaken as part of the ongoing CDD process
- implementing inadequately designed policies, procedures, and controls for transaction monitoring of customer accounts, e.g. in one instance alerts for suspicious transactions were generically applied to all customers irrespective of the level of risk each posed, even for those identified as high risk, when we would have expected more directly targeted alerts.

Examples of good practice	Examples of unsatisfactory practice
✓ An AML/CFT Programme with sufficient processes to ensure that suspicious activities and / or transactions are reported, as soon as practicable but no later than 3 working days after the RE formed its suspicion.	x Lack of red flags to identify suspicious activity. x No review by the AML/CFT compliance officer of suspicious activities identified by frontline staff. x A suspicious activity submitted by an RE was rejected by goAML at the first attempt due to incorrect file format. The RE never corrected the file and resubmitted it.

***2 formal warnings** due to **failures relating to meeting the requirements of suspicious activity reporting** were issued during the review period*

Governance

Senior management and boards should maintain oversight of their entities' compliance with AML/CFT obligations. Good practice would include regular reporting to senior management and the board on AML/CFT related activities within the RE. Senior management and boards should also ensure they get sufficient assurance that the RE is complying with its obligations under the Act.

AML/CFT audits

Section 59 (2) of the Act requires REs to have their risk assessments and AML/CFT compliance programmes audited every two years (now every three years, with effect from 9 July 2021) or at any other time at the request of their AML/CFT supervisor.

However, we have noted several instances where REs failed to have their audits done at all, or had them done late. We also noted REs failing to remediate AML/CFT audit findings. Failure to do so could indicate a lack of willingness to comply with the Act and/or that REs did not prioritise remediation of AML/CFT findings. Senior management had also failed to monitor the progress of these findings being remediated.

***22 formal warnings due to failure to have an audit done within the required timeframe** were issued to REs during the review period.*

Our expectations

- Senior management and boards should maintain adequate oversight of AML/CFT matters.
- Senior management and boards should ensure the business allocates sufficient resources to perform AML/CFT responsibilities.

Examples of good practice	Examples of unsatisfactory practice
✓ REs planning ahead and having AML/CFT audits done within the required timeframe.	x REs missing the AML/CFT audit deadline due to late engagement with an AML/CFT auditor.
✓ Senior management and boards receiving regular reporting on their RE's compliance with its AML/CFT obligations.	x Audit findings being repeated over a number of AML/CFT audits without being adequately remediated.

Other AML/CFT requirements

Record keeping

An emerging issue with REs is poor record keeping practices. The requirements for record keeping are set out in sections 49 to 55 of the Act. We observed examples of insufficient records maintained for:

- identity verification relating to CDD
- interactions with customers
- suspicious and unusual activities identified
- CDD exceptions
- high-risk customers, PEPs and customers subjected to enhanced CDD
- training undertaken by senior management and staff
- staff vetting.

We also noted an instance where the CDD information collected and recorded was not easily accessible to staff.

Staff training

Lack of staff training in relation to AML/CFT continues to be an issue for some REs. Issues include gaps in the training materials regarding AML/CFT obligations, training schedules in the AML/CFT programme not being followed, and inadequate training being done by the AML/CFT compliance officer and other frontline staff.

Some REs were providing training to staff but did not include offshore teams engaged in AML/CFT-related duties as part of this training.

Staff training is integral to ensuring compliance with the Act. REs should therefore ensure that senior managers (including board directors), AML/CFT compliance officers, and any other employees engaged in

AML/CFT-related duties, are given appropriate training on AML/CFT matters, as required by section 57 of the Act.

Financial Intelligence Unit (FIU)

The FIU's core responsibilities are to receive, collate, analyse and disseminate information contained in suspicious activity reports (SARs), prescribed transaction reports (PTRs) and Border Cash Reports.

goAML software

goAML is the software system used by the FIU to counter ML and TF. All REs should register on goAML and use it to submit SARs and PTRs.

The goAML system is also used by the FIU to provide REs with relevant information. The FIU provides free goAML training to all users. REs can contact the FIU to arrange training.

We still find REs that are not registered on goAML and therefore won't receive relevant information from the FIU or be able to file SARs or PTRs. All goAML related questions and issues must be directed to the FIU.

Suspicious activity reports (SARs)

Reporting of suspicious activity to the FIU is a requirement under section 40 of the Act. This must be done by submitting SARs through the goAML portal.

REs should ensure their goAML profile is current, and that they have adequate and effective policies, procedures and controls in place to ensure that SARs are submitted in a timely manner.

The table below shows the number of SARs received by the FIU since the Act came into force.

Table: Suspicious activity reports submitted 2013 – 21

Period	Total SARs submitted to FIU	SARs submitted by FMA 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
2018/19	12,153	170
2019/20	13,604	257
2020/21	24,046	493

In the first three to four years of the Act coming into effect, our REs only submitted a fraction of the total number of SARs filed. Since then, targeted training for REs by the FMA has focused on account and transaction monitoring, and filing SARs. We have now completed two cycles of training in various locations around New Zealand, attended by approximately 400 AML compliance officers and staff with AML/CFT responsibilities. That training appears to have had the desired effect, with large increases in volumes of SARs being filed by REs. We will continue to provide this training and encourage REs to attend.

Engaging with the FMA

A good working relationship with the FMA is important, so we encourage REs to reach out to us if guidance is required. Please email all AML/CFT-related queries to aml@fma.govt.nz

Reminder to REs

Addition and removal of REs

When changes occur within your business that would require updates to the FMA RE list, you need to email the FMA with a short description of the change that occurred, to enable us to update our RE list. We aim to keep the RE list published on our website up to date.

AML/CFT compliance officer changes

Before appointing AML/CFT compliance officers, REs must ensure that they are adequately experienced to administer and maintain their AML/CFT programme. When you change your AML/CFT compliance officer we expect that you will email us the contact details of your newly appointed AML/CFT compliance officer.

Appendix: How we engaged with the sector

Annual AML/CFT report

REs are required to file an annual AML/CFT report each year, for the year ending 30 June. That data informs our risk-based approach to monitoring, allowing us to better understand where our REs are located and what business activities they carry out.

The number of late filings of annual AML/CFT reports is continuing to decline. Late filing is a breach of REs' regulatory obligations and has in the past resulted in warnings being issued.

At the time of writing this report, REs were still filing their annual AML/CFT reports for the period ending 30 June 2021, which are due 30 September 2021.

Therefore, our analyses of annual AML/CFT information and trends (illustrated below) are based on reports submitted by REs as at 30 June 2020:

Chart: REs that are members of a designated business group

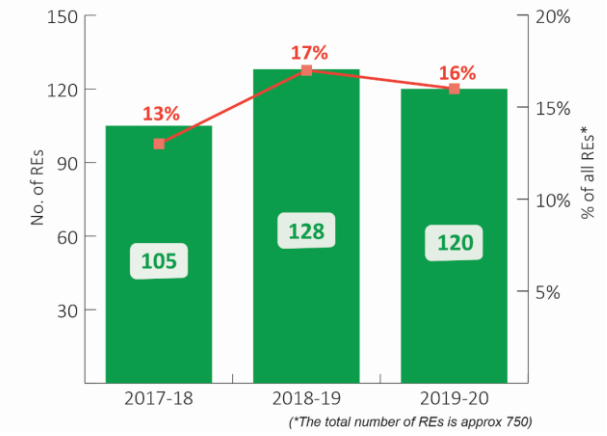


Chart: REs with face-to-face onboarding of all new customers

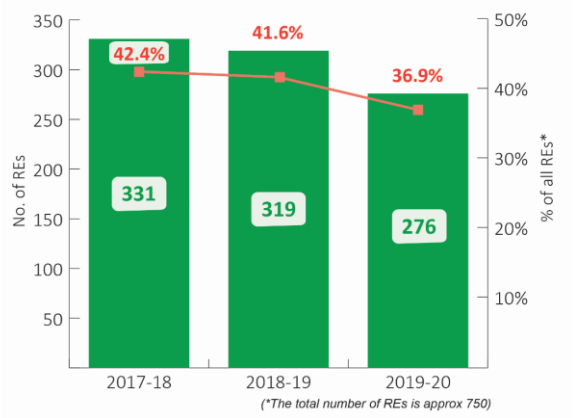


Chart: Location of non-resident customers

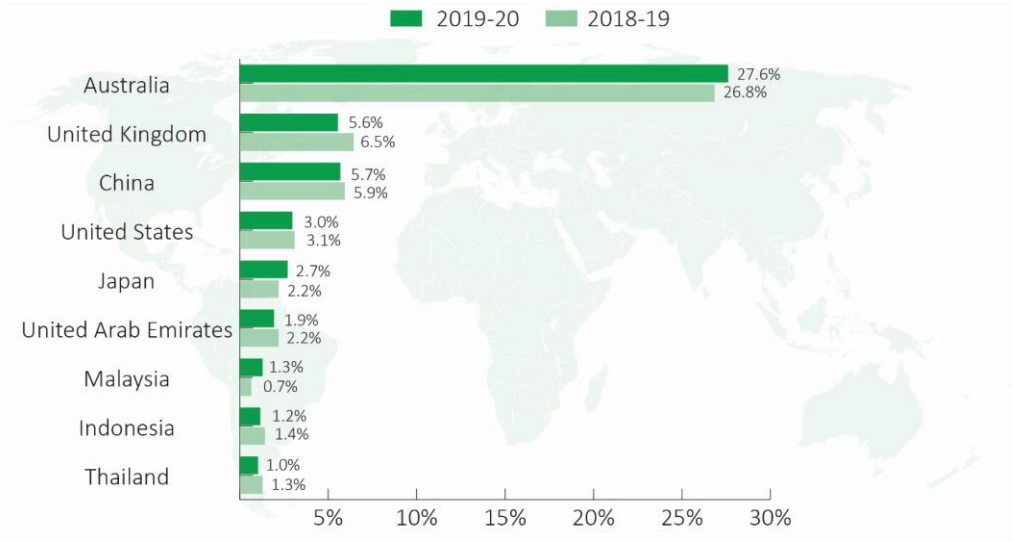


Chart: Location of REs in New Zealand 2019-20

Interaction with domestic and international agencies

We participate in various domestic and international committees alongside other New Zealand agencies, including the Ministry of Justice (MoJ), NZ Police's Financial Intelligence Unit (FIU), NZ Customs, Inland Revenue (IRD), the Ministry of Foreign Affairs and Trade (MFAT) and the Ministry of Business, Innovation and Employment (MBIE).

Domestic committees

AML/CFT Oversight Committee (OC)	National Coordination Committee (NCC)	Sector Supervisors Forum (SSF)
MoJ, FMA, RBNZ, DIA, FIU, Customs	MoJ, FMA, RBNZ, DIA, FIU, Customs	FMA, RBNZ, DIA. FIU and MoJ as observers
Supports the NCC by providing strategic oversight of the operation and effectiveness of the AML/CFT regime	Coordinates between AML/CFT supervisors, NZ Police and other agencies to ensure the consistent, effective and efficient operation of the regime	Supports the NCC by coordinating operational matters between the AML/CFT supervisors

International committees and forums

Financial Action Task Force (FATF)	Asia-Pacific Group on ML (APG)	International Supervisor Forum (ISF)	Pacific AML/CFT Supervisor Forum (PASF)
New Zealand is a member country of FATF.	New Zealand and 41 other countries are APG members.	New Zealand, Australia, Canada, UK, USA.	New Zealand, Australia, and various Pacific islands.
FATF develops and promotes policies to protect the global financial system against money laundering (ML) and terrorist financing (TF).	The purpose of APG is to ensure the adoption, implementation and enforcement of FATF standards.	SF members engage, support, and share information and operational practices. They also consult on common supervisory priorities and issues.	PASF members work together to strengthen the capability of countries within the region to supervise REs.

RE monitoring activity

During the period 1 July 2018 to 30 June 2021, we conducted 36 onsite monitoring visits and 24 desk-based reviews. For each of these monitoring visits and desk-based reviews we sent feedback letters with remedial action to be undertaken where required. We also examined independent AML/CFT audit reports for 156 REs, as well as information included in the annual AML/CFT reports they submitted.

During the review period, 27 formal warnings[2] (including three public warnings) were issued under section 80 of the Act, for significant breaches of the Act.

Our reviews of independent AML/CFT audit reports in certain instances also resulted in onsite visits and desk-based reviews being undertaken where concerns with audit findings were noted.

The table below summarises our direct engagement with REs in each sub-sector.

Table: FMA direct engagement with REs by sub-sector

Sector	SRA 2017 Risk Rating	Onsite			Desk based			s59 audit reviews			Enforcement action taken		
		2018/19	2019/20	2020/21	2018/19	2019/20	2020/21	2018/19	2019/20	2020/21	2018/19	2019/20	2020/21
DI	H	5		1	2					1		1	
Brokers and custodians	M-H	12	3	1	1	5		6	12	2	5	2	1
Fund managers	M-L	4	2			1		7	10	8			
Financial advisers	M-L	3		1	1	6	3	47	23	9	6	5	6
Equity crowdfunding platforms	M-L				1								
Peer-to-peer lending providers	M-L				1					2			
DIMS providers	M-L	3	1		2			7	3	1			
Licensed supervisors	L									1			
Issuers of securities	L					1		4	5	8			1
Total		**27**	**6**	**3**	**8**	**13**	**3**	**71**	**53**	**32**	**11**	**8**	**8**

[2] Included are private warnings issued in September 2021. These were included as they relate to monitoring activities undertaken during the period under review, hence the final outcome was included in the report even though it was completed after 30 June 2021.

Glossary

Act	The Anti-Money Laundering and Countering Financing of Terrorism Act 2009 and its regulations
AML/CFT	Anti-money laundering and countering financing of terrorism
CDD	Customer due diligence, as defined in section 11 of the Act
Enhanced CDD	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 on 30 June 2013, or who has subsequently entered into a business relationship with the RE
EIV Guideline	Electronic Identity Verification Guideline – For Part 3 of IDVCOP published July 2021
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
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.

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