Te Tari Taiwhenua
Internal Affairs

Te Kāwanatanga o Aotearoa
New Zealand Government

Anti-Money Laundering and Countering Financing of Terrorism

Regulatory Findings Report

2018–2019

Keeping New Zealand in business for good

Contents

01
Director's message

Director's message

Kia ora koutou

We're pleased to share this report summarising our regulatory findings from July 2018 to June 2019, a period of significant growth in our supervisory responsibilities and the number of businesses required to implement procedures and processes to protect New Zealanders from the social and economic harm arising from money laundering and terrorism financing.

Every year an estimated $1.35 billion from fraud and illegal drugs is laundered through legitimate New Zealand businesses. Part of our role as a regulator is to support businesses to disrupt and deter financial crime, increase confidence in the New Zealand financial sector, and meet our international obligations in relation to combatting money laundering and terrorism financing.

It's been great to see the commitment and willingness of the businesses we supervise to comply with the Anti-Money Laundering and Countering Financing of Terrorism Act 2009. We know how disruptive and harmful it can be to a business that is unwittingly taken advantage of by money launderers or those involved in financing terrorism.

To help meet this challenge, we have grown our teams in Auckland, Wellington and Christchurch over the last 18 months to further support the increased number of businesses we supervise. We have held more than 50 training events and presented at over 30 conferences or forums throughout the country to help our new sectors (accountants, lawyers, conveyancers, bookkeepers, real estate agents, and high-value dealers) understand and meet their compliance obligations and the important role they play in protecting New Zealanders from the harm caused by criminals laundering money and/or financing terrorism.

We do understand and appreciate that adjusting business processes and coming up to speed with the obligations under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 requires change. In our experience, compliance becomes common practice as business processes mature and embed.

We target our regulatory resources to areas of high money laundering or financing terrorism risk. That focus over the twelve months of this report has resulted in civil proceedings, issuing five formal warnings and accepting one enforceable undertaking for breaches of the Act. (Read about these on page 23.)

Our focus for the coming year is to strengthen our risk-based supervisory approach and continue our engagement work to support businesses under our supervision. We will continue to build awareness and understanding through our education and engagement activities, such as training roadshows, webinars and the industry advisory group, to collectively strengthen the AML/CFT system. We will also progress the work with our system partners for the Financial Action Task Force (FATF) 2020 Mutual Evaluation of New Zealand.

Ngā mihi ki a koutou katoa.

Mike Stone
Director, Anti-Money Laundering Group
Department of Internal Affairs

02

Background to this report

Background to this report

This report shares our regulatory findings for the 12 months ended 30 June 2019. It is intended to help the businesses we supervise understand our expectations, and how they can improve their systems and processes to comply with their AML/CFT obligations.

These businesses are known officially as reporting entities – see the Glossary for more on those types of businesses.

We take a risk-based approach to our compliance work. This means we use intelligence and risk analysis, along with professional knowledge and expertise, to target and prioritise our activities to the higher risk areas of money laundering and financing terrorism. This does not mean we ignore areas of lower risk, and we continue to work with businesses in these groups to ensure the appropriate level of compliance is maintained.

The Department of Internal Affairs has supervised some businesses under the Act since 2013, with additional sectors introduced between July 2018 and August 2019.

Businesses we supervise

June 2013

Financial institutions and casinos

- Money remitters, non-bank non-deposit taking lenders, money changers, payroll providers, factoring, financial leasing, safe deposit box providers, non-bank credit card providers, cash transporters, tax pooling, means of payment providers, virtual asset service providers (VASPs)
- Casinos

June 2013

Designated non-financial business or profession

- Trust and Company Service Providers (TCSPs)

July 2018

- Lawyers
- Conveyancers
- Additional Trust and Company Service Providers (TCSPs)

October 2018

- Accountants

January 2019

- Real Estate Agents

August 2019

- Racing Industry Transition Agency
- High Value Dealers

For unfamiliar terms and abbreviations, please see the Glossary on pages 25 and 26.

03

Executive summary

Executive summary

Our role

The Anti-Money Laundering Group's role at the Department of Internal Affairs is to supervise and support businesses to comply with the Anti-Money Laundering and Countering Financing of Terrorism Act 2009. It is also to help them prevent their businesses being misused by criminals for money laundering or terrorism financing.

We work with the Reserve Bank of New Zealand, the Financial Markets Authority, the Ministry of Justice, and the NZ Police Financial Intelligence Unit (FIU), as well as other government agencies, to build an effective AML/CFT system.

Our findings – in brief

Effective risk assessment

Over the year of this report, we have seen some very good examples of risk assessments and AML/CFT programmes. These risk assessments clearly demonstrate an understanding of the nature, size and complexity of the business, the types of customers, activities and transactions, and the money laundering and financing terrorism risks they face.

The policies, procedures and controls in an AML/CFT programme must be based on a risk assessment. The risk assessment is a core element of an effective AML/CFT programme and is fundamental to a business' ability to meet its obligations under the Act. So, if a business understands its money laundering and terrorism financing risks and vulnerabilities, it can direct its compliance resources to where it's most useful and urgent.

We will continue to focus our supervision on whether or not a business understands its money laundering and financing terrorism risks. Risk assessments must be kept current, reviewed and updated at appropriate times to reflect changes in the business, with version-controlled documentation showing the alterations.

Applying AML/CFT documents in practice

Over the 12 months to 30 June 2019, a common factor we observed is a disconnect between a business' risk assessment and AML/CFT programme, and how these documents are used in practice. We inspected businesses with well-written documents that seemed 'technically compliant' on paper, but when we visited we saw their procedures, policies and controls were not effectively implemented.

Use of generic template

Many businesses have adopted generic templates for their risk assessment and AML/CFT programme documents. In some circumstances, the content has been wholly generic and not specific to their business, types of customers, transactions or activities conducted.

While a template can be a useful starting point for a risk assessment or developing an AML/CFT programme, the Act requires the identification of the specific money laundering and financing terrorism risks that a particular business faces. The risk assessment must also enable the business to determine the level of risk in relation to its AML/CFT obligations. This means the risk assessment must be specific to the individual business' circumstances, customers and activities. The risks must then be managed and mitigated through its AML/CFT programme.

When we undertake our compliance engagements, it is usually clear which businesses are using a generic template and which are not. We consider generic template content to be an indicator the business may not be adequately meeting its AML/CFT obligations.

Areas of non-compliance

The most common areas of non-compliance were the following:

- Risk assessments too generic and not specific to the money laundering and financing terrorism risks the business faced.
- Written documents incomplete and not covering all the relevant obligations. These include a lack of procedures for politically exposed person (PEP) checking, beneficial ownership checks, enhanced customer due diligence, suspicious activity and prescribed transaction reporting.
- The written AML/CFT programme documentation is technically compliant but not implemented effectively in practice.
- Compliance officers' inadequate understanding of their businesses' money laundering and financing terrorism risks, and poor implementation of policies, procedures and controls in practice.
- Customer due diligence (CDD) and Enhanced CDD not undertaken in accordance with the Act's requirements.
- The compliance officer does not have the required level of influence in the business to escalate issues and ensure governance level support for the AML/CFT programme.
- Insufficient training and vetting of senior management, compliance officers and any staff member with AML/CFT duties.
- AML/CFT risk assessment and programme documents not kept up to date, with no version control used.

04

Is New Zealand in business for good?

Is New Zealand in business for good?

Over the 12 months to 30 June 2019, we completed 149 desk-based reviews and 49 on-site inspections. These resulted in 60 remediation plans, as well as other regulatory action, including formal warnings and one enforceable undertaking.

Overall, we found that businesses with a positive approach to compliance had a greater understanding of AML/CFT obligations.

These were also the businesses with risk assessments that reflected their actual money laundering or financing terrorism risks, and had programmes in place to mitigate them. These businesses were the most prepared for an on-site inspection, showing that practical and effective AML/CFT measures were being implemented.

Money launderers can trade on the professionalism and skills of professional service providers to move criminal proceeds to make them look like legitimate funds or assets.

Desk-based reviews

A desk-based review (DBR) is an assessment of the technical compliance of a business' written risk assessment and AML/CFT programme.

First we notify the business in writing that we need to review these documents as part of our supervision of how they are complying with the Act. When we finish our review, we write a report that rates and comments on what we find.

The usual ratings for each area we assess are non-compliant, partially compliant or compliant. For areas of partial or non-compliance, our report may include recommendations or required actions for the business to take to become compliant.

Examples of good practice

Risk assessment

- Businesses respond to our notifications and provide documents in a timely manner.
- Risk assessments clearly demonstrate an understanding of the nature, size and complexity of the business, its types of customers, activities and transactions, and the money laundering and financing terrorism risks faced while doing business.
- Businesses can provide evidence or regular reviews and updating of their risk assessment.

AML/CFT programme

- AML/CFT programmes contain clearly written policies, procedures and controls for the various circumstances where ongoing and enhanced customer due diligence is needed. These policies, procedures and controls are integrated with wider business practices.
- Documented risk-escalation and reporting policies that say who is responsible for suspicious activity and prescribed transaction reporting, and who is responsible if that person is away.
- AML/CFT training content is tailored to the business.
- AML/CFT programmes clearly specify the type of external and internal training required for the compliance officer, senior management and staff involved.
- Staff training records are kept, and how staff complied with training requirements is monitored.
- Businesses respond and implement remediation plans when a desk-based review identifies gaps.

Examples of unsatisfactory practice

Some businesses, particularly within the legal and accounting sectors, have relied heavily on generic templates, and their measures do not reflect their individual businesses' money laundering or financing terrorism risks.

Risk assessment

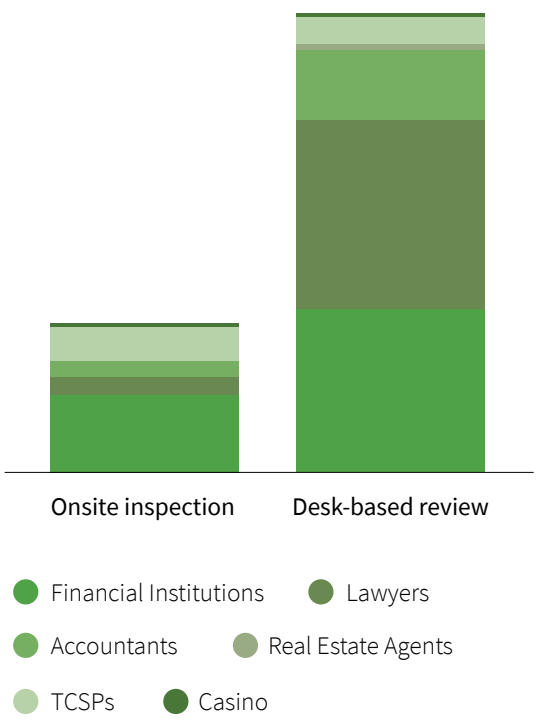
- Risk assessments and AML/CFT programmes developed in other countries and do not comply with New Zealand legislation.
- Risk assessments that describe the business but contain no assessment of its ML/TF risks and vulnerabilities.
- The risk assessment does not demonstrate a good understanding of the business and its customers or transactions.

AML/CFT programme

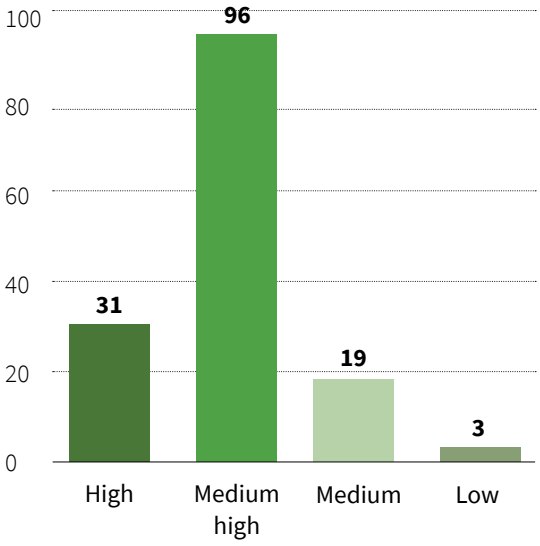
- AML/CFT programmes disconnected or not related to the risk assessment.
- The documents quote the Act but without detail around how its requirements are integrated with business practices.
- Lack of written procedures for politically exposed person (PEP) checking, beneficial ownership checks, enhanced customer due diligence, suspicious activity and prescribed transaction reporting.
- Small businesses with a small customer base, or that provide one service, with overly complex and unworkable risk assessments and AML/CFT programmes.
- No clear process to escalate issues.

Approximately 50% of our on-site inspections and 65% of our desk-based reviews were of designated non-financial businesses and professions (DNFBPs).

On-site inspections and desk-based reviews



Number of desk-based reviews based on DIA's inherent sector risk ratings (1 July 2018 – 30 June 2019)



On-site inspection

An on-site inspection assesses the establishment, implementation and effectiveness of a business' AML/CFT programme and is usually undertaken after a desk-based review.

An on-site inspection is done at the business' location and involves interviewing the compliance officer, inspecting practices and procedures, reviewing physical and electronic records, and interviewing some staff. On-site inspections may take just a few hours or several days depending on the size and complexity of the business.

After an on-site inspection we write a report detailing how well the business is implementing its AML/CFT programme and whether it is effective. For areas of non-compliance we may provide requirements or make recommendations for how the business can become compliant.

Examples of good practice

Risk assessment

- The compliance officer demonstrates a detailed understanding of the risk assessment and the money laundering and financing terrorism risks the business faces.
- Staff and senior managers understand the risks and are committed to their AML/CFT obligations.
- Workshops are carried out with a range of staff to brainstorm the business' money laundering and financing terrorism vulnerabilities and risks as part of creating the risk assessment. Along with valuable insights from staff's professional judgement, this helps build an AML/CFT compliance culture across the business.
- Staff and managers are well prepared for and engaged during an on-site inspection.

AML/CFT programme

- AML/CFT policies and practices have been fully integrated into wider business processes.
- Documents are well organised and easily accessible.

Customer due diligence (CDD)

- Information about the nature and purpose of the business relationship with the client is recorded at the start. This information is updated regularly and used during ongoing CDD and account monitoring.
- An initial customer risk-rating is determined at the start of the relationship and is used to work out how much verification is needed in relation to beneficial owners, and whether enhanced CDD is necessary. It also helps decide the level of ongoing CDD. This risk-rating is reviewed and updated regularly during ongoing CDD and account monitoring.
- Original CDD documents are copied and scanned, with the staff member's name and date of copying clearly recorded.
- Controls are in place to ensure that if CDD (including enhanced CDD) can't be done, the business relationship with the customer is terminated and/or an occasional transaction or activity is not carried out.

Reporting to NZ Police Financial Intelligence Unit (FIU)

- The business is registered for goAML and appropriate staff are trained.
- Prescribed transaction reports (PTRs) and good quality suspicious activity reports (SARs) are submitted within required timeframes.

Record keeping

- Centralised record keeping is in place for all CDD, activity and transaction records, and other business correspondence. This includes keeping a written record of findings relating to examining a customer's activities and transactions, and any decisions made about the level of CDD and account monitoring.

Training and vetting

- Criminal record checks are undertaken for the compliance officer, all senior managers and all staff engaged in AML/CFT-related duties.
- AML/CFT training records are centralised, with reminders set for completion and refresher training.
- AML/CFT is a standing item on team meeting agendas of staff involved with AML/CFT duties.
- Policies, procedures and controls are well understood by staff, and the requirements for enhanced CDD and reporting suspicious activity are effectively implemented.

Independent audit

- Any deficiencies are addressed following an audit, with these changes implemented in a revised AML/CFT programme and risk assessment.

Examples of unsatisfactory practice

Risk assessment

- Risk assessments are not kept up to date and have no version control documented.
- New products or services are introduced, or customers in new countries dealt with, without any assessment of their money laundering and/or financing terrorism risks.
- The compliance officer does not demonstrate a good understanding of the risk assessment.

AML/CFT programme

- An AML/CFT programme that doesn't reflect the changing risks the business may face.
- Documents are incomplete.

Customer due diligence (CDD)

- There is no evidence CDD is carried out.
- Trusts are taken on as clients without any enhanced CDD.
- Copies of the identity documents used for verification are not kept.
- Decisions relating to the level of CDD (i.e. standard or enhanced), and the reasons for these decisions, are not documented.

- For a company, identifying beneficial owners extends only to those who own more than 25% of a company, or those with effective control, without any assessment of whether there may be others that meet the definition of beneficial owner.
- Customers are taken on online using electronic verification but without considering whether the person really is who they claim to be.
- Electronic verification processes are not set out in the AML/CFT programme, and the business does not demonstrate an understanding of the services provided and if they meet the required standard.

Reporting to NZ Police Financial Intelligence Unit (FIU)

- The business is not goAML registered and doesn't know how to submit a suspicious activity report.
- Staff do not understand the confidentiality requirements of reporting to the FIU.
- Staff do not know the reporting requirements or relevant thresholds.

Record keeping

- Correspondence (e.g. emails) about a business relationship are not kept.
- Documentation and information can not be easily provided when requested.

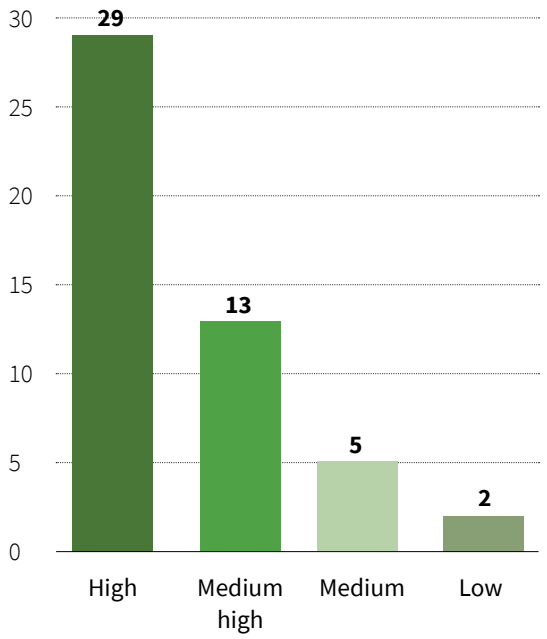
Training

- There is no evidence senior managers have been trained.
- Staff training is irregular or inconsistent.

Independent audit

- Faults found during an independent audit have not been fixed.
- No audit has been undertaken within the required time frame.

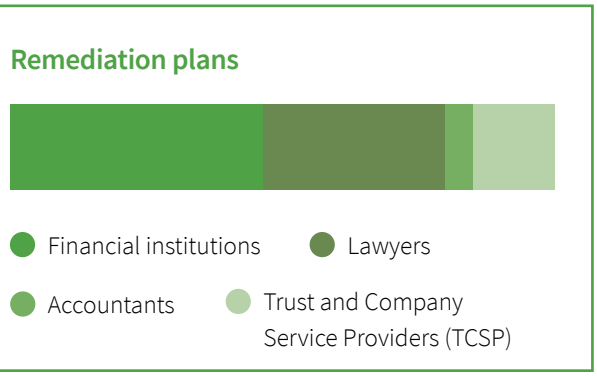
Number of on-site inspections based on DIA's inherent sector risk rating (1 July 2018 – 30 June 2019)



Remediation

A desk-based review or on-site inspection report may include recommendations and requirements to fix compliance faults or gaps. This could be done through a remediation plan, where we and the business agree steps they must take to become compliant with the Act. Timeframes for review and follow-up are also set.

Breakdown of remediation plans by sector (1 July 2018 – 30 June 2019)



05

Education and engagement

Supporting businesses to comply

Education and engagement are key parts of our work to help businesses understand and implement effective compliance practices.

Over the 12 months ending 30 June 2019, we responded to more than 4,000 queries by phone or email from businesses we supervise. We responded to 85% of all queries within 1-2 days, with less than 10% taking six or more days to resolve.

As is to be expected, queries by sector peaked in the month of legislated obligations, and there were some common themes across each sector.

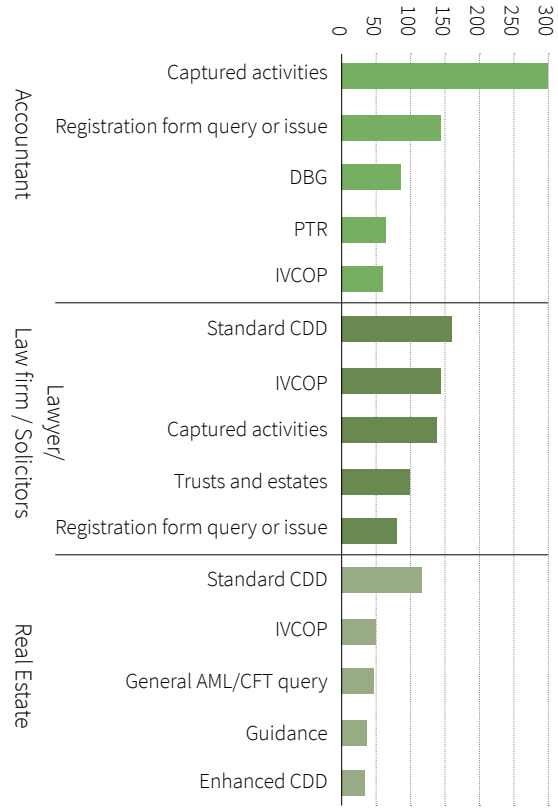
We focus on ensuring businesses have the support and knowledge to comply with the legislation. Our experience with multiple businesses shows that most want to do the right thing, so we are here to support them with guidance material, webinars, roadshows and training sessions.

Most common queries

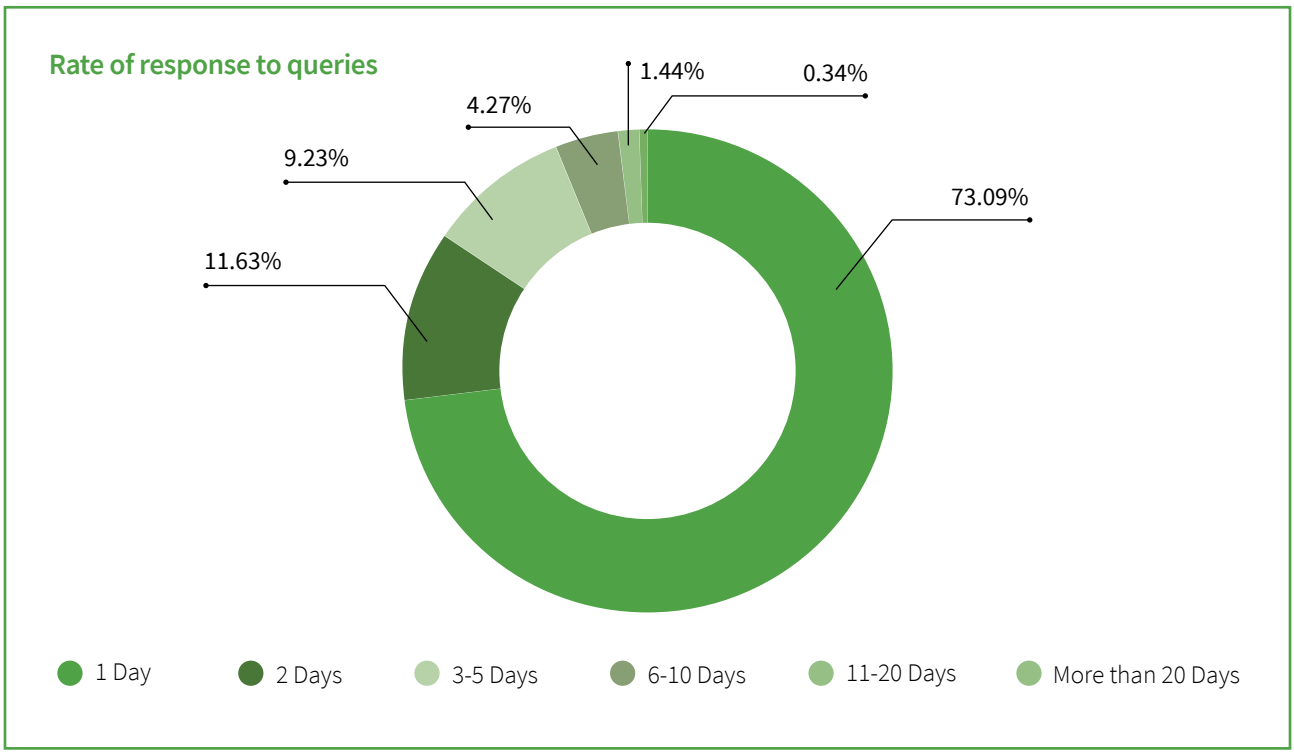
Over the last 12 months of this report the most common query from the accounting sector was about 'captured activities'. These are activities specified under the definition of "designated non-financial business or profession" in the Act.

For the legal and real estate sectors, it was about standard CDD.

Top 5 queries by sector



Please refer to the glossary on pages 25 and 26 for explanations of abbreviations.



Reporting suspicious activities and transactions

Data from the NZ Police Financial Intelligence Unit indicates that reporting entities we supervise submitted more than a third of all suspicious activity reports (SARs) it received in the 12 months ending 30 June 2019.

The Reserve Bank of New Zealand supervises banks, which carry out the highest volume of financial transactions. For the entities we supervise to make up such a high percentage of SARs shows the businesses we supervise are positively engaged in monitoring and reporting suspicious requests or transactions, to help detect criminal activity and preventing harm to our communities.

SARs		All reporting entities	DIA's reporting entities	
	Period	Total	Total	%
Transactions based	01/07/2018 – 30/06/2019	11,658	3,916	34%
Activity based	01/07/2018 – 30/06/2019	495	221	45%

06

Designated business groups (DBG)

Designated business groups (DBG)

DBG groups allow businesses to cooperate to meet their AML/CFT obligations.

There are a number of categories under which businesses may form a DBG, including

- Joint ventures
- Related companies under the Companies Act
- Related law firms
- Related accounting practices
- Related trust and company service providers.

Each category will have different requirements. Please refer to our guidelines for more detailed information.

DBG members can

- share a compliance officer (via ministerial exemption until June 2023)
- share compliance expertise across the group
- coordinate staff training
- rely on another member to conduct CDD for them.

We may assess all members of the group as part of our regulatory activity.

As of August 2019, nearly 200 designated business groups had been established by the Department's reporting entities.

07

Our enforcement toolkit

Our enforcement toolkit

We work with reporting entities to assist businesses to comply with the Act. If a remedial plan has not improved compliance we can use a range of enforcement tools.

Formal warning	This warns that sanctions may be imposed if areas of AML/CFT non-compliance are not addressed. Depending on the seriousness of the non-compliance, we may publish the formal warning to deter others.
Enforceable undertaking	This is a legally binding written agreement detailing what the business must do to comply with its AML/CFT obligations within an agreed timeframe.
Injunctions	We may go to the High Court to force a business to do something it has refused or failed to do, and if that refusal or failure is or would be a civil liability act under the Act. For example, we could seek an injunction restraining a person from acting as an AML/CFT compliance officer, or being a member of key management personnel of any organisation deemed a reporting entity under the Act. We might also ask the court to restrain someone from doing something that contravenes the Act.
Civil proceedings	Taken through the High Court, this enforcement action seeks fines and/or injunctions. Fines can go up to $200,000 per civil liability act for an individual, or $2 million for a body corporate.
Criminal proceedings	This seeks criminal prosecution and penalty through the courts. The maximum penalty is a term of imprisonment of not more than two years and/or a fine of up to $300,000 for an individual, or $5 million for a body corporate.

If a business is used to launder money or help finance terrorism, the reputational cost – and penalties if there has been AML/CFT non-compliance – may be a lot more than the cost of compliance.

Recent formal warnings

IE Money Limited provides money remittance and foreign exchange services to domestic and overseas customers. A formal warning was issued in August 2018 for failing to meet AML/CFT requirements of conducting CDD, monitoring accounts and transactions, recordkeeping, and establishing, implementing or maintaining an AML/CFT programme.

Run Da International Limited provided money remittance services to domestic and overseas customers. A formal warning was issued in May 2019 for failing to conduct CDD, failing to adequately monitor accounts and transactions, failing to keep records and failing to establish, implement or maintain their AML/CFT programme.

Regus New Zealand Management Limited (Regus) provides serviced office spaces, including virtual office services to customers in New Zealand and overseas. A formal warning was issued in June 2019 for failing to meet various AML/CFT requirements, including conducting CDD and enhanced CDD, failing to keep records, and failing to establish, implement and maintain a current risk assessment and AML/CFT programme.

Customhouse Safe Deposits Limited (CSDL), also known as Commonwealth Vault, is the largest safe deposit provider in New Zealand and trades in gold and silver bullion. It was issued a formal warning in June 2019 for failing to conduct CDD, failing to adequately monitor accounts and transactions, failing to keep records, and failing to establish, implement or maintain its AML/CFT programme.

Enforceable undertakings

Ink Patch Money Transfer Limited (Ink Patch): We agreed to an enforceable undertaking in February 2019 from Ink Patch, a money remitter for customers wanting to send funds to Samoa. Ink Patch failed to meet AML/CFT requirements, including failing to conduct CDD, failing to adequately monitor accounts and transactions, and failing to implement or maintain an AML/CFT programme. A formal warning had been issued in January 2015 to Ink Patch for repeated non-compliance.

Civil proceedings

Jin Yuan Finance Limited (Jin Yuan) offered money remittance services and had a history of non-compliance with the Act between June 2013 and June 2017. We initially tried to assist Jin Yuan to meet its obligations, but by 2015 it was still non-compliant. A formal warning was issued and published in 2015.

During the four years we monitored Jin Yuan, we were repeatedly told it was doing its business through one company bank account. For this period, Jin Yuan declared itself to have undertaken 55,097 transactions with a total of $278.5 million of business. However, it later emerged the company was using 17 bank accounts. Jin Yuan's actual business was inferred to be significantly greater than had been declared to the Department.

Jin Yuan was held to have committed civil liability acts of failing to conduct CDD, failing to adequately monitor accounts and transactions, continuing business relationships with persons who did not provide satisfactory evidence of their identities, failing to report suspicious transactions, and failing to keep records. In the High Court in Auckland on 3 October 2019, Jin Yuan was ordered to pay a fine of $4 million plus costs.

The AML/CFT Act is risk based, which means businesses should focus on the areas of operations with a higher money laundering or terrorism financing risk.

08 Glossary

Glossary

AML/CFT

Anti-money laundering and countering financing of terrorism.

Beneficial owner

The individual(s) with effective control of a customer or person on whose behalf a transaction is conducted, or owns a prescribed threshold of the customer or person on whose behalf a transaction is conducted.

CDD

Customer due diligence. Under 'standard CDD', a reporting entity is required to identify and verify the identity of a customer, any beneficial owner of a customer, and any person acting on behalf of a customer. Standard CDD requirements are set out in sections 15 to 17 of the Act. See also 'enhanced CDD' and 'simplified CDD'.

DBG

Designated business group. As defined in section 5 of the Act, a DBG is a group of two or more people where there is a written agreement between those making up the group. An entity that elects to join a DBG may rely on another member of the DBG to carry out some of its obligations under the Act, provided certain conditions are met.

DNFBP

Designated non-financial business or profession. This includes law firms, conveyancing practitioners, incorporated conveyancing firms, accounting practices, real estate agents, and trust and company service providers.

Enhanced CDD

Enhanced customer due diligence. A higher level of CDD requiring at least standard customer due diligence, as well as obtaining and verifying information relating to the source of a customer's funds or wealth. These requirements are set out in section 23 to 25 of the Act. Further enhanced CDD requirements are specific to politically exposed persons, wire transfers, correspondent banking, and new or developing technologies or products that might favour anonymity. These are set out in sections 26 to 30 of the Act.

Financial institutions supervised by the Department

Money remitters, NBNDTLs (see below), payroll providers, payment providers, factoring, financial leasing, safe deposit box providers, non-bank credit card providers, cash transporters, tax pooling, means of payment providers, VASPs (see below) and other financial institutions not supervised by Reserve Bank of New Zealand or the Financial Markets Authority.

FIU

The 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 FIU relating to suspicious activity and prescribed transaction reports.

HVD

High-value dealer. A person who is in trade and, in the ordinary course of business, buys or sells one or more articles (including precious metals and stones, jewellery, watches and cars) specified in section 5 of the Act by way of a cash transaction or a series of related cash transactions (of NZ$10,000 or more).

IVCOP

Amended Identity Verification Code of Practice 2013. The suggested best practice for verifying a customer's name and date of birth. The Amended Identity Verification Code of Practice 2013 covers identity verification, document certification and electronic identity verification.

ML/TF

Money laundering and terrorism financing.

NBNDTL

Non-bank non-deposit taking lender.

PEP

Politically exposed person. An individual who holds, or has held at any time in the preceding 12 months in any overseas country, a prominent public function. Immediate family members and close associates of these people are also considered PEPs. The full definition of PEP is in section 5 of the Act.

PTR

Prescribed transaction report. A reporting entity must submit a prescribed transaction report to the FIU for any domestic cash transaction valued at NZ$10,000 or over, and for any international wire transfer valued at NZ$1,000 or over. A PTR must be submitted within 10 working days of the transaction taking place.

RE

Reporting entity. Financial institutions or DNFBPs that, in the ordinary course of business, carry out one or more activities specified in section 5 of the Act. Reporting entities also include casinos, high-value dealers and the Racing Industry Transition Agency.

Risk(s)

Risk of money laundering or terrorism financing.

SAR

Suspicious activity report. A reporting entity must submit a SAR where the reporting entity has reasonable grounds that a transaction or proposed transaction, a service or proposed service, is suspicious. The full definition of SAR is found under section 39A of the Act.

Simplified CDD

Simplified customer due diligence. A lower standard of CDD for certain types of customers. Sections 19 to 21 of the Act sets out the requirements for carrying out simplified CDD.

The Act

The Anti-Money Laundering and Countering Financing of Terrorism Act 2009 and its regulations.

TCSP

Trust and company service provider.

VASP

Virtual asset service provider.

Te Tari Taiwhenua
Internal Affairs

Te Kāwanatanga o Aotearoa
New Zealand Government

January 2020