Te Tari Taiwhenua
Internal Affairs

New Zealand Government

Guideline:

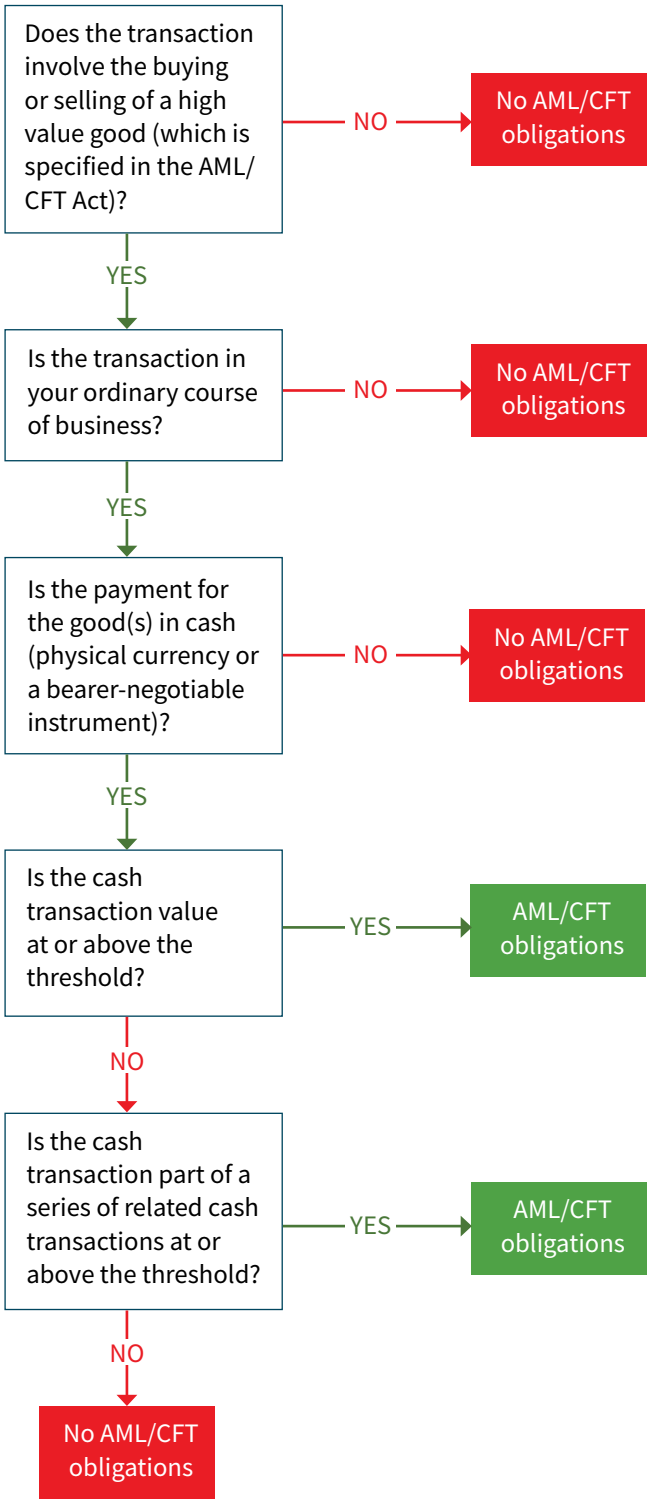
High Value Dealers Complying with the Anti-Money Laundering and Countering Financing of Terrorism Act 2009

May 2019

Contents

Flow-chart: Am I captured?

The following flow-chart will help you determine whether you are captured as a high value dealer (HVD) under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT Act):



Interpreting "cash"

Cash is defined in Section 5 of the AML/CFT Act. It means physical currency (i.e. New Zealand dollars and foreign currency) or bearer-negotiable instruments. A bearer-negotiable instrument means:

(a) a bill of exchange; or
(b) a cheque; or
(c) a promissory note; or
(d) a bearer bond; or
(e) a traveller's cheque; or
(f) a money order, postal order, or similar order; or
(g) any other instrument prescribed by regulations.

Note that all cheques (including bank drafts) are considered bearer-negotiable instruments for the purposes of the AML/CFT Act.

If the transaction does not involve cash, you are not captured by the AML/CFT Act.

Interpreting "high value good" and "ordinary course of business"

The terms "high value good" and "ordinary course of business" are defined in Section 2 'Applying the AML/CFT Act to your business'.

Executive summary

Money laundering (ML) is the method by which people disguise and conceal the proceeds of crime and protect and enjoy their assets. Some people in New Zealand may also be financing terrorism using similar techniques to money launderers to avoid detection by authorities and to protect the identity of those providing and receiving the funds.

The HVD sector is vulnerable to ML and terrorism financing (TF). Criminals target HVDs to launder the proceeds of their crimes to cover their tracks and avoid detection. Some criminals may buy expensive goods with cash, then sell these goods and get 'clean' money for personal use or to fund more criminal activity. Others might, for example, keep expensive goods for personal use, trade them with other criminals, or take them overseas and sell them there to avoid raising 'red flags' in New Zealand.

The AML/CFT Act now captures HVDs from 1 August 2019. Note that HVDs have fewer obligations than other reporting entities. The AML/CFT Act is activities-based and buying and selling high value goods is one of the captured activities.

If you are involved in a cash transaction (or a series of related cash transactions) equal to or above a prescribed threshold (and meet the other criteria set out in Section 2 'Applying the AML/CFT ACT to your business') you will be captured by the AML/CFT Act. It is important to note that if you do not transact using cash you will not be captured and will not have any AML/CFT obligations. The prescribed threshold for cash transactions has not yet been defined in regulations as it is still awaiting approval from Cabinet. The values consulted on with the public were NZD5,000, NZD10,000 and NZD15,000. Once the threshold value is finalised the Department of Internal Affairs (DIA) will update this guidance.

Introducing AML/CFT measures will deter criminals from using your services and help you detect them if they do. It will make it harder for criminals to move cash anonymously using high value goods. Importantly, it will also strengthen the overall AML/CFT system.

We recognise that adjusting to the new AML/CFT system will take time and effort. This guideline, and other existing guidelines, can help you develop awareness of the risks posed by ML/TF, and provide information on how to meet your compliance obligations.

Disclaimer

This guideline is provided for information purposes only and cannot be relied on as evidence of complying with the requirements of the AML/CFT Act. It does not constitute legal advice and cannot be relied on as such. If after reading this guideline you do not fully understand your obligations, you should seek suitable professional or legal advice or contact your supervisor, DIA at Amlcft@dia.govt.nz.

1. Overview

If you are an HVD and meet the criteria outlined in the AML/CFT Act you will have compliance obligations from 1 August 2019. These criteria are outlined in Section 2 'Applying the AML/CFT Act to your business.' The 'Am I captured?' flow-chart at the start of this document will help you determine whether you are captured by the AML/CFT Act.

The table below summarises what HVDs must do for transactions captured by the AML/CFT Act to meet their AML/CFT obligations. Section 4 'Do you know your compliance obligations?' provides you with more detail on these requirements.

What must be done by HVDs captured by the AML/CFT Act	When does it need to be done?	Comment
• Conduct standard customer due diligence (CDD) for all transactions using cash (includes physical currency and bearer-negotiable instruments) when you are captured as an HVD by the AML/CFT Act.	• If CDD is required, the customer's identity must be verified before you enter into a cash transaction with them.	• Can be done by a reporting entity, designated business group (DBG) or a third party. However, the responsibility lies with you. • Note if you are unable to conduct CDD you must not engage in that transaction.
• Submit prescribed transaction reports (PTRs) for a domestic physical cash transaction (includes physical currency, but not bearer-negotiable instruments) which meets or exceeds an applicable threshold value. • Note: Once the prescribed threshold is finalised we will provide further guidance on how PTR requirements apply to HVDs.	• Within 10 working days from the date the transaction took place.	• Can be done by a reporting entity, DBG or a third party. However, the responsibility lies with you. • Submit to the New Zealand Police Financial Intelligence Unit (FIU).

• Keep records of:
  • Identity and verification documentation
  • Suspicious activity reports (SARs) (if you choose to submit them to the FIU)
  • Any audits.
	• Ongoing.
	• Records must be kept for at least five years. In the case of SARs, there may be times when DIA or the Commissioner of Police require you to keep a copy of the report for a period longer than five years.
		• Can be done by a reporting entity, DBG or a third party. However, the responsibility lies with you.

• Audit your AML/CFT compliance obligations.	• At the request of your AML/CFT supervisor, DIA.	• Auditor must be independent and suitably qualified.

2. Applying the AML/CFT Act to your business

What is captured by the AML/CFT Act?

If you are an HVD you will be captured by the AML/CFT Act when all three of the following conditions are met:

You buy or sell specific **high value goods** (listed below) in the **ordinary course of your business**

+

Cash (see glossary for a full definition) is the means of payment for the transaction

+

The cash transaction (or related cash transactions) is **equal to or above the prescribed threshold**

An HVD will not be excused from compliance on the basis that to comply would breach any contract or agreement.

Note the Ministry of Justice (who administers the legislation) has completed consultation with the sector asking for feedback on the cash threshold levels of NZD5,000, NZD10,000 and NZD15,000. The prescribed cash threshold will not be confirmed until Cabinet has approved the recommendation. This guidance will be updated once this cash threshold has been confirmed.

Understanding the AML/CFT Act

Interpreting "ordinary course of business"

Whether an activity is in your ordinary course of business will always be a matter of judgement depending on the nature of your business. Some relevant factors to take into consideration would be whether the activity:

- Is normal or otherwise unremarkable for your business
- Is frequent
- Is regular (meaning predictable, consistent)
- Involves significant amounts of money
- Is a source of income
- Involves significant resources
- Involves a service offered to customers.

In most cases when you trade in high value goods using cash at or above the threshold you will be carrying out an activity in your ordinary course of business and therefore will be captured by the AML/CFT Act.

For further information on this, please refer to the guidance 'Interpreting Ordinary Course of Business' on the Department's website at: https://bit.ly/2po86Fw.

Some important information about cash

The definition of cash for the purposes of AML/CFT

Cash means physical currency (i.e. New Zealand dollars and foreign currency) or bearer-negotiable instruments. A bearer negotiable instrument means:

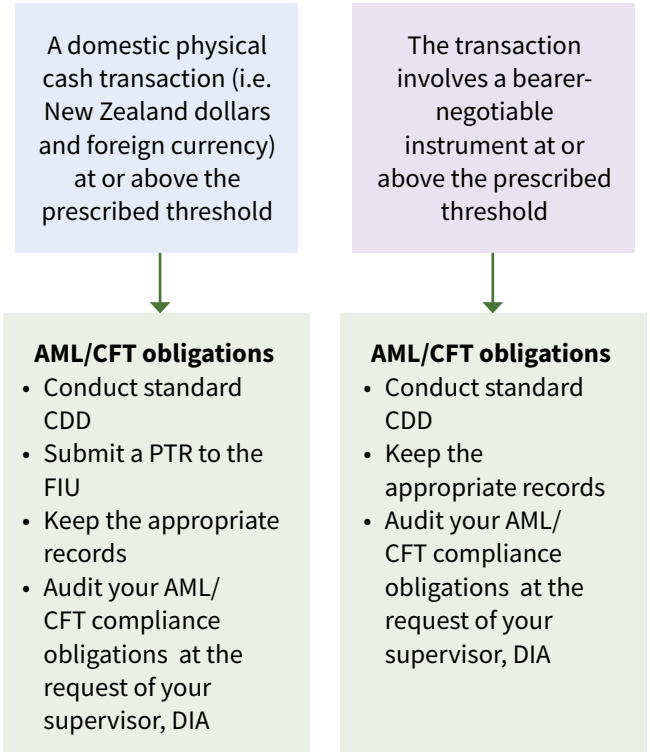
(a) a bill of exchange; or
(b) a cheque; or
(c) a promissory note; or
(d) a bearer bond; or
(e) a traveller's cheque; or
(f) a money order, postal order, or similar order; or
(g) any other instrument prescribed by regulations.

Note that all cheques (including bank drafts) are considered bearer-negotiable instruments for the purposes of the AML/CFT Act.

If the transaction does not involve cash, you are not captured by the AML/CFT Act.

The different AML/CFT obligations for transactions involving physical currency versus those transactions involving bearer-negotiable instruments

The main difference is around PTR requirements – for a domestic physical cash transaction at or above the prescribed threshold you are required to submit a PTR, whereas you are not required to submit a PTR for transactions involving bearer-negotiable instruments.



Bank cheques versus bank deposits

As cheques are considered bearer-negotiable instruments, you can't avoid your AML/CFT obligations by telling your customers to go to the bank and get a bank cheque. However, if customers go to a bank and deposit cash directly into your bank account you will not be captured as an HVD under the AML/CFT Act.

Interpreting "high value goods"

The high value goods which are included in the AML/CFT Act include:

- Motor vehicles
- Ships
- Jewellery
- Watches
- Gold, silver, or other precious metals
- Diamonds, sapphires, or other precious stones
- Paintings
- Prints
- Protected foreign objects
- Protected New Zealand objects
- Sculptures
- Photographs
- Carvings in any medium
- Other artistic or cultural artefacts.

Note that **registered auctioneers** (within the meaning of section 4(1) of the Auctioneers Act 2013) who sell any of the high value goods listed above, at or above the prescribed threshold are captured as HVDs.

Further information on some of the high value good categories is provided below:

High value good	Comment
Motor vehicles	• A motor vehicle is defined by the meaning of Section 6(1) of the Vehicle Sales Act 2003 (https://bit.ly/2Ub9ygy). • It means any of the following: i. A road vehicle that is drawn or propelled by mechanical power and is of a kind ordinarily acquired by consumers for personal, domestic, or household use; ii. A vehicle of any other class or description declared by the Governor-General, by Order in Council, to be a motor vehicle for the purposes of the Vehicle Sales Act 2003. • It also states what is not included as a 'motor vehicle', including, but not limited to, a motor cycle with a cylinder capacity of less than 60 cubic centimetres, a tractor or farm machinery, a trailer and a moped.
Ships	• Within the meaning of Section 2(1) of the Maritime Transport Act 1994 (https://bit.ly/2TNsHQB). • A ship means every description of boat or craft used in navigation, whether or not it has any means of propulsion, and includes - i. A barge, lights, or other like vessel, ii. A hovercraft or other thing deriving full or partial support in the atmosphere from the reaction of air against the surface of the water over which it operates, iii. A marine or other submersible.

High value good	Comment
Protected foreign objects	• Within the meaning of Section 2(1) of the Protected Objects Act 1975 (https://bit.ly/2ODWwST). • It means an object in or from a foreign State that is of importance for archaeology, prehistory, history, literature, art, or science and that belongs to a category set out in Section 2(1) of the Protected Objects Act 1975. • It includes, but is not limited to, rare collections, property relating to history, stamps, furniture more than 100 years old and old musical instruments.
Protect New Zealand objects	• Within the meaning of Section 2(1) of the Protected Objects Act 1975 (https://bit.ly/2ODWwST). • It means an object that is of importance to New Zealand, or to part of New Zealand, for aesthetic, archaeological, architectural, artistic, cultural, historical, literary, scientific, social, spiritual, technological, or traditional reasons; and falls within one or more of the categories of protected objects set out in Schedule 4 (https://bit.ly/2ValTy8) of the Protected Objects Act 1975.

Examples of when you are captured as an HVD

The box below provides examples of HVDs captured under the AML/CFT Act.

These examples are based on a NZD10,000 cash threshold, which is used for illustrative purposes. The examples will be updated once the cash threshold value has been finalised.

The examples are not specific to the named sector and apply to all HVDs.

Example 1: You are an art dealer. A customer pays NZD10,000 in cash for a painting in your shop. You are captured as an HVD by the AML/CFT Act. The buyer has used cash to buy the high value good and the transaction has reached the NZD10,000 threshold which triggers AML/CFT obligations. You are required to meet your AML/CFT obligations.

Example 2: You are a car dealer. A customer wants to trade in their old car to buy a new one and has said that they will pay the remaining amount in cash. The total price of the car is NZD25,000. Their old car covers NZD15,000, so they pay NZD10,000 in cash to bridge the gap. You are captured as an HVD by the AML/CFT Act. The cash transaction has reached the NZD10,000 threshold. You are required to meet your AML/CFT obligations.

Example 3: You sell expensive jewellery. A customer wants to pay NZD40,000 using their credit card, and the remaining NZD10,000 with cash. You are captured as an HVD by the AML/CFT Act. The cash transaction has reached the NZD10,000 threshold. You are required to meet your AML/CFT obligations.

Example 4: You buy second-hand jewellery. A member of the public would like to sell you their diamond necklace for cash. After assessing the necklace, you value it to be worth NZD15,000 and you pay in cash. You are captured as an HVD by the AML/CFT Act. The cash transaction has exceeded the NZD10,000 threshold. You are required to meet your AML/CFT obligations.

Example 5: You buy and sell second-hand luxury watches. A member of the public would like to swap their existing luxury watch for another one in your store. After assessing the watch, you value it to be worth NZD30,000. The luxury watch they want to trade it for is worth NZD20,000. You give them the watch and NZD10,000 in cash to bridge the gap. You are captured as an HVD by the AML/CFT Act. The cash transaction has reached the NZD10,000 threshold. You are required to meet your AML/CFT obligations.

Example 6: You are a boat seller. A customer wants to buy one of your boats worth NZD10,000 using a bank cheque (a bearer-negotiable instrument). As bearer-negotiable instruments are considered cash for the purposes of the AML/CFT Act, the NZD10,000 cash threshold has been reached. You are required to meet your AML/CFT obligations.

Note: You are not required to submit a prescribed transaction report (PTR) on transactions using bearer-negotiable instruments including banks cheques (see Section 4 ‘Do you know your compliance obligations?’ for more information on this).

Interpreting "related cash transactions"

Whether cash transactions are related or not will be a matter of judgement depending on the circumstances. Below are some factors to consider for determining whether cash transactions are related:

- Is the same customer trading with you regularly using cash, and the individual transactions are under the cash threshold but collectively they equal/exceed the threshold?
- Is the customer's behaviour predictable? (i.e. trading in the same/similar high value good every week with cash, over a number of weeks).
- Has a purchase been made on layby and the customer pays for the instalments using cash totalling (or above) the prescribed threshold?
- Do cash transactions from different customers appear related in some way?

The box below provides examples of 'related cash transactions' for HVDs.

These examples are based on a NZD10,000 cash threshold, which is used for illustrative purposes. The examples will be updated once the cash threshold value has been finalised.

The examples are not specific to the named sector and apply to all HVDs.

Note: HVDs do not have PTR requirements for the following examples as the individual cash transactions are below NZD10,000. See Section 4 'Do you know your compliance obligations?' for further information.

Example 1: A customer buys high value goods from you in quick succession (i.e. a few days apart) using cash. Each transaction is NZD2,500 (under the cash threshold amount) but collectively the transactions equal/exceed the threshold. You are captured as an HVD by the AML/CFT Act and therefore have AML/CFT compliance obligations.

Example 2: A customer buys a high value good from your store on layby. They enter into an agreement with you to pay NZD2,000 per month over five months. They pay each instalment in cash. Collectively the cash transactions equal the NZD10,000 threshold value. You are captured as an HVD by the AML/CFT Act and therefore have AML/CFT compliance obligations.

Example 3: Two friends come into your store and choose a jewellery set worth NZD10,000. One of them says they'll pay for it in cash. After finding out the CDD requirements, the other friend offers to pay NZD5,000 in cash. If they both pay NZD5,000 in cash, then you would need to conduct CDD on both of them (and meet the other compliance obligations in accordance with the AML/CFT Act).

Example 4: You buy second-hand jewellery. A customer would like to sell you their diamond necklace for cash. After assessing the necklace, you value it to be worth NZD5,000. The following day the same customer comes back to your store and would like to sell you a gold necklace worth NZD8,000. The cash transactions have exceeded the NZD10,000 threshold. You are captured as an HVD by the AML/CFT Act and therefore have AML/CFT compliance obligations.

We realise despite your best efforts that it may be difficult for you to spot cash transactions that are related, especially if they are spread over time. The Department will be satisfied that you have met your AML/CFT obligations in this regard if you can demonstrate that you are taking reasonable steps to identify related cash transactions (and are carrying out CDD when the cash threshold is reached or exceeded).

What isn't captured by the AML/CFT Act?

If you are an HVD you are not captured by the AML/CFT Act under the following circumstances:

- Buying or selling high value goods using another means of payment (i.e. not trading in cash).
- Trading in cash below the prescribed threshold (although related cash transactions equal to or above the prescribed threshold are captured by the AML/CFT Act).
- Buying or selling goods not listed in the definition of 'high value goods'.

You are also not captured by the AML/CFT Act if you are providing other services in relation to high value goods (as long as you aren't buying or selling these goods). These services may include:

- Mining precious metals or precious stones; or
- Manufacturing jewellery; or
- Crafting or polishing precious stones.

In addition, you are not an HVD if you buy or sell precious metals or precious stones for industrial purposes.

Note that private sales are not captured by the AML/CFT Act.

Territorial scope of the AML/CFT Act

You will be captured by the AML/CFT Act if you are an HVD carrying out cash transactions within New Zealand. You will also be captured if one party is based overseas, but you are conducting the cash transaction through a business operating in New Zealand.

Even though the AML/CFT Act only has jurisdiction in New Zealand, you should consider reporting on suspicious activities and transactions that occur offshore. For more information about reporting suspicious activity, see Section 4 'Do you know your compliance obligations?'.

Relying on third parties

There are provisions in the AML/CFT Act which allow you to share some of your compliance obligations with others. One way to do this is to form a designated business group (DBG). This is explained further below. Section 5 'Do you know your customer?' provides information on when you can rely on others for CDD.

Establishing a designated business group (DBG)

The term DBG is defined in full in the AML/CFT Act. In summary, it means a group of two or more persons who have elected (in writing) to form a group that has been approved by the AML/CFT supervisor to share some obligations under the AML/CFT Act. If you are considering forming a DBG, you should consider the risks and implications for all members.

Who can form a DBG?

You may be able to form a DBG with other entities. Each member of the group must:

- Have elected in writing to be a member of the group;
- Be related to every member of the group as defined in Section 2(3) of the Companies Act 1993;

- Be a related HVD or a subsidiary of an HVD;
- Be a reporting entity resident in New Zealand, or resident in a country that has sufficient AML/CFT systems and is supervised or regulated for AML/CFT purposes; and
- Not be a member of another DBG.

What can DBGs do?

If you are a member of a DBG, you may rely on another HVD who is also a member to conduct CDD on your behalf, provided the identity information is given to you before you carry out a captured transaction. You can also rely on another HVD to make a prescribed transaction report and a suspicious activity report on your behalf. It is important to note that you still retain responsibility for ensuring you are complying with the AML/CFT Act and regulations.

How do you form a DBG?

DIA will consider all applications to form a DBG. You need to ensure that you meet the criteria defined in Section 5(1) of the Act and submit an application form.

There are two guidelines available to help reporting entities to create DBGs, one on the scope of a DBG (https://bit.ly/2OGKmYu) and one on the formation (https://bit.ly/2xNSfUG). We recommend you familiarise yourself with these guidelines before submitting any application. The application form is included in the formation guideline.

3. Do you know what to expect from your AML/CFT supervisor?

This section explains the regulatory approach you can expect from DIA.

The role of DIA and our regulatory approach

DIA is the AML/CFT supervisor for HVDs. Our role includes helping you understand your AML/CFT requirements, ensuring you are meeting your compliance obligations, and investigating and enforcing compliance if necessary. This is to ensure the AML/CFT system operates in a robust manner and that criminals seeking to launder money and finance terrorism are detected and deterred.

We take a risk-based and responsive approach to regulation which means we focus our efforts carefully and deliberately. We use our insight, knowledge and understanding to identify risks, and determine interventions to most effectively deal with those issues. Our compliance work is based on the following principles:

- Outcomes focused – we want to ensure our activities have the maximum impact on delivering our outcomes.
- Fairness – we act with integrity and ensure our responses are fair, reasonable, and unbiased.
- Consistency – although each case is unique we take a consistent and responsive approach to decision-making.
- Public expectations – we acknowledge the public's expectations for firm action toward those who are wilfully non-compliant or negligent.
- Transparency and openness – we are clear about our approach and ensure that those affected have opportunities to provide input.

Our preference is to work with you in a responsive and educative manner, although we are fully prepared to escalate our response with enforcement action. For serious or deliberate non-compliance, we may decide to issue a formal warning or to accept an enforceable undertaking from a reporting entity. Alternatively, we may decide to seek an interim, performance or restraining injunction, or a pecuniary penalty, from the High Court. In the most serious of cases, DIA will prosecute reporting entities for criminal offences under the AML/CFT Act.

Investigations of ML/TF

In New Zealand it is a criminal offence to knowingly and intentionally engage in, or facilitate any other person to engage in, money laundering or the financing of terrorism. The New Zealand Police are responsible for investigating and prosecuting ML/TF offences, as well as forfeiture proceedings relating to the proceeds of crime. A robust AML/CFT system, in which reporting entities are conducting CDD, keeping customer and transaction records, and reporting suspicious activities, is an important tool in the collective fight against financial and organised crime.

4. Do you know your compliance obligations?

This section provides HVDs with information on meeting their minimum AML/CFT obligations.

HVDs have fewer AML/CFT obligations than other reporting entities captured by the AML/CFT Act. Appendix A 'Compliance obligations for other reporting entities' provides you with an overview of the additional requirements that other reporting entities must do to comply with the AML/CFT Act. DIA encourages you to familiarise yourself with those requirements to decide whether they may help protect your business from criminal activity.

> If a customer's behaviour and activity is suspicious, you may decide to submit a suspicious activity report (SAR) to the FIU. While it is optional for you to do this, DIA strongly recommends you report any suspicious activity. These reports provide crucial information to assist the New Zealand Police and other AML/CFT agencies to investigate crime using financial intelligence.

As an HVD, you also need to be aware of your obligations to submit suspicious property reports (SPRs) under the Terrorism Suppression Act 2002. If you are in control of property that you suspect (on reasonable grounds) is owned or controlled, directly or indirectly, by a designated terrorist entity (or property derived or generated from that type of property), you must report that suspicion to the FIU using goAML.

Conduct standard customer due diligence

You will need to conduct standard CDD when all three of the following conditions are met:

You buy or sell specific **high value goods** (listed below) in the **ordinary course of your business**

+

Cash (see glossary for a full definition) is the means of payment for the transaction

+

The cash transaction (or related cash transactions) is **equal to or above the prescribed threshold**

You will need to conduct standard CDD on:

- Your customer;
- Any beneficial owner of a customer; and
- Any person acting on behalf of a customer.

Some customers may be hesitant to provide personal information about themselves (such as their date of birth). However, if you are not able to complete CDD on your customer, you must not engage in the transaction with them. To do so would be a breach of the AML/CFT Act.

Moreover, there may be times where a customer exhibits abusive and/or threatening behaviour. It is important

that you follow your business' health and safety procedures when dealing with abusive customers. Remember you must conduct CDD if you are completing a transaction.

See Section 5 'Do you know your customer?' for more details on how to conduct CDD. We suggest you have information on hand to provide to customers which explains the importance of CDD information for AML/CFT purposes.

Summary of standard CDD requirements

- You must conduct CDD when cash (i.e. bearer-negotiable instruments and physical currency) is the medium of exchange and the other criteria is met.
- If you are an HVD and a transaction is captured under the AML/CFT Act, you need to conduct standard CDD on your customer, beneficial owner of your customer, and any person acting on behalf of your customer.
- A customer's identity must be verified before you carry out a transaction where CDD is required.
- If you cannot complete CDD on your customer, you must not engage in the transaction with them.

Reporting to the New Zealand Police Financial Intelligence Unit (FIU)

Prescribed transaction reports (PTRs) and suspicious activity reports (SARs) must be submitted via the goAML web-based reporting tool and in the reporting format provided by the FIU.

Note that SARs do not replace PTRs. If the transaction meets or exceeds the prescribed cash threshold, then you will need to submit a PTR regardless of whether a SAR was submitted. PTRs and SARs complement other types of reports and information held by the FIU and are used in different ways.

Registering with goAML

goAML allows rapid and secure exchange of information between the FIU, reporting entities, and law enforcement and intelligence authorities. The confidentiality of the data collected is ensured.

To register with goAML you need to firstly register the entity, and then subsequent users who are linked to that entity can be added.

To register the entity, you need to fill out the registration form which is available on the FIU's website at: https://bit.ly/2FKDQOx. The FIU has produced some guidance on how to fill it out: https://bit.ly/2uDqP2B. After completion of the online registration form, you will receive an email confirming that your request has been submitted. The FIU will then review the request, which will be either accepted or rejected. Notification of this will be provided by email (rejected registration requests are unable to be amended, and you must restart the registration form).

Once your entity registration request has been approved, additional users can be added for the entity. The FIU has produced guidance on this process: https://bit.ly/2U0dSiL. New users that have been accepted are placed on a "To Be Trained" list for that area. Where there are sufficient numbers, a training session is arranged and those on the list are invited.

Note: Some older browsers are not compatible with the goAML web application. If you are experiencing difficulties with the application, please ensure that you are using one of the following browsers:

- Microsoft Edge (Windows 10)
- Chrome versions 30+
- Internet Explorer 9+
- Firefox 23+.

Further information on goAML can be found on FIU's website at: https://bit.ly/2TZ2kwa.

Navigating the goAML system

Once you have registered with goAML you will have access to the resource library which includes documentation as well as online training modules to assist in your understanding of submitting PTRs and SARs. Note the resource library is only available once a user has logged into goAML.

We suggest you start with the online training modules as they are a good introduction to goAML. Detailed information is also available in the resource library to guide you through the reporting process.

The resource library is accessible by clicking on the question mark on the top menu bar. A screen shot of where this is located is shown below:

If you have questions about goAML, we suggest you email the FIU in the first instance at: goaml@police.govt.nz.

Prescribed transaction reporting

Why PTRs are important

PTRs add transparency to the financial system by making ML/TF more difficult to hide, as well as improving the detection and disruption of organised crime, fraud and tax evasion.

The types of PTRs relevant for HVDs

There are two types of prescribed transactions that can be conducted through a reporting entity, International Funds Transfers (IFTs) and Large Cash Transactions (LCTs). The only PTR that HVDs will need to submit is an LCT-PTR as it involves transactions where cash is the medium of exchange.

The requirements for an LCT-PTR

LCT-PTRs are required to be submitted to the FIU using goAML as soon as practicable, but no later than 10 working days after the transaction.

An LCT-PTR is only required in relation to a domestic physical cash transaction. A domestic physical cash transaction means a transaction in New Zealand involving the use of physical currency (i.e. New Zealand dollars and foreign currency).

You are not required to submit an LCT-PTR for any single transaction below the threshold value (including cash transactions that appear related). However, you do have CDD obligations for related cash transactions that equal or exceed the prescribed threshold.

Note: Once the prescribed threshold for HVDs is set, you will need to determine when you must submit an LCT-PTR. If the prescribed cash threshold for HVDs is NZD10,000 or less, you will only need to submit a PTR for domestic physical cash transactions equal to or above NZD10,000. If the prescribed cash threshold is above NZD10,000, you will need to submit a PTR each time the domestic physical cash transaction meets or exceeds this threshold. We will be updating this part of the guidance once the prescribed cash threshold is defined in the regulations.

What an LCT-PTR must contain

goAML has a number of fields for you to fill in, some of which are compulsory. You will be unable to submit your LCT-PTR within goAML without the following information:

i. A description of the nature of the transaction;
ii. The amount of the transaction and the currency in which it was denominated;
iii. The date on which the transaction was conducted;
iv. The parties to the transaction, including relevant agents and other facilitators.

If there are errors in your report the FIU will not accept it and they will contact you via the goAML message board to resolve these. For the purposes of reporting timeframes, the submission date is taken as the date of the original submission, and you will not be penalised for delays caused by resolving issues with the report.

Summary of prescribed transaction reporting requirements

- If you are an HVD, you must submit a large cash transaction PTR (LCT-PTR) to the New Zealand Police Financial Intelligence Unit (FIU) when you are involved in a domestic physical cash transaction that meets or exceeds the prescribed cash threshold.
- You must submit an LCT-PTR when each individual cash transaction is equal to or above the prescribed cash threshold.
- You do not have LCT-PTR requirements for transactions involving bearer-negotiable instruments.
- Submit LCT-PTRs to the FIU using goAML as soon as practicable, but no later than 10 working days after the transaction.

Suspicious activity reports (SARs)

Why are SARs important

While it is optional for HVDs to report on suspicious activity, DIA strongly recommends you submit SARs to the FIU. SARs are the main source of information available to the FIU to detect suspected offences.

What SARs apply to

SARs apply to transactions, proposed transactions, services or proposed services, and inquiries. Note there are no monetary thresholds for SARs. You should not only consider the transaction itself, but the broader activity such as a customer's behaviour.

You should also submit SARs (as soon as you can) in circumstances related to security matters including suspected terrorism and terrorism financing.

Reporting SARs using goAML

It is recommended that you submit an SAR to the FIU as soon as practicable but no later than three working days. In most situations the FIU expects that you file an SAR within three days from the time you gathered sufficient information to form suspicion, rather than three days from an initial event. You must submit an SAR to the FIU through goAML. In limited circumstances you can submit an SAR orally, manually or via email.

For further information on submitting SARs, refer to the FIU web page at: https://bit.ly/2HKeHpd.

The difference between Suspicious Activity reports (SARs) and Suspicious Transaction reports (STRs)

SAR is the legislative term that covers both reporting types in goAML, namely 'Suspicious Activity Report' and 'Suspicious Transaction Report'. To correctly submit an SAR to the FIU you need to select the right report type (as indicated by the red circle below).

If you know the dollar value of the transaction, even if the transaction wasn't completed, you should submit a Suspicious Transaction Report. If you didn't complete the transaction and do not know the amount of the proposed transaction, you should submit a Suspicious Activity Report with $0 value.

Protections and immunities for reporting entities submitting SARs

You must not disclose SAR information, or the existence of any SARs, to customers or members of staff that do not need to know about the SAR. This is to protect the identity of the person submitting the SAR and ensure the safety of staff and reporting entities. It also avoids alerting the customer, who may be undertaking criminal activity and should not be advised of the SAR. There are protections and immunities for reporting entities submitting SARs.

It is important to note that if you filed an SAR about one of your customers and as a result the Police investigated and charged the person, your identity would be protected. SAR confidentiality is treated very seriously by the Police.

Examples of suspicious activity

The box below provides examples of suspicious activity that HVDs may encounter. As some of these examples show, there is nothing stopping you from completing a transaction that appears suspicious if you have met your AML/CFT requirements.

These examples are based on a NZD10,000 cash threshold, which is used for illustrative purposes. The examples will be updated once the cash threshold value has been finalised.

The examples are not specific to the named sector and apply to all HVDs.

Note: The following examples illustrate times when you may decide to submit an SAR. However, this isn't a comprehensive list and it is possible that you may come across other scenarios that you consider to be suspicious based on your business and customers.

Example 1: The customer appears nervous and they are keen to complete the transaction as quickly as possible. They also do not want to answer any of your questions relating to the transaction. They pay for the high value good with NZD8,000 of cash. Despite this being under the prescribed threshold, you decide to submit an SAR to the FIU once the transaction is complete as you have reason to suspect the transaction is suspicious.

Report type: Suspicious Transaction Report (with NZD8,000 as the dollar value).

Example 2: The customer wants to purchase a painting worth NZD15,000 with cash. They hand over cash notes, some of which are presented in an unusual condition (i.e. odorous and coated with a white substance). The customer appears on edge and does not want to answer any of your questions. However, they provide you with the necessary identification documentation for CDD purposes. You decide to submit an SAR to the FIU once the transaction is complete as you have reason to suspect the transaction is suspicious.

Report type: Suspicious Transaction Report (with NZD15,000 as the dollar value).

Example 3: The customer asks what items your jewellery shop has and what can be ordered. They then ask about your refund policy. They place an order for an item not in store and pay for it upfront in cash. A week later the customer lets you know that they are no longer interested in the item and want a refund. They instruct you to pay the refund into a third party's bank account.

Report type: Suspicious Transaction Report (with the cost of the item as the dollar value).

Example 4: The customer wants to complete the transaction as quickly as possible. They appear nervous when asked to show identification documentation and end up refusing to provide it. You therefore refuse the cash transaction as you have been unable to carry out CDD. You also decide to submit an SAR to the FIU because you have reason to suspect the activity is suspicious.

Report type: Suspicious Transaction Report (with the cost of the item as the dollar value).

Example 5: A repeat customer that you have known for years suddenly changes their buying behaviour. Rather than buying cars worth NZD10,000, they would like to purchase a car worth NZD50,000 using cash. After carrying out CDD, you decide to ask them questions to find out where this additional wealth has come from. They don't provide you with a satisfactory explanation, so you decide to submit an SAR to the FIU because you have reason to suspect the activity is suspicious.

Report type: Suspicious Transaction Report (with NZD50,000 as the dollar value).

Example 6: A customer who appears nervous and on edge asks about your refund policy. You explain that your business does not give out refunds to customers that change their minds about the item bought. The customer has a large stack of cash with them, although you are not sure how much they are carrying or how much they intend to spend. The customer says they are no longer interested in making a purchase and leaves your store. Even though you haven't completed the transaction you decide to submit an SAR to the FIU.

Report type: Suspicious Activity Report (with $0, since you don't know the dollar value).

Summary of suspicious activity reporting

- SARs provide crucial information to assist the New Zealand Police and its AML/CFT partners to investigate crime using financial intelligence.
- Once reasonable grounds for suspicion exist, it is recommended that you submit an SAR to the FIU as soon as practicable (but no later than three working days).
- Submit SARs to the FIU using the goAML web-based reporting tool.
- There are two report types, namely Suspicious Activity Reports and Suspicious Transaction Reports. You should submit a Suspicious Transaction Report when you know the dollar value of the transaction, and a Suspicious Activity Report when you don't know the dollar value.
- You must not disclose SAR information, or the existence of any SARs, to customers or members of staff that do not need to know about the SAR.
- There are protections and immunities for reporting entities submitting SARs.

Record keeping

You must keep adequate records of identity and verification documents, audits, and SARs (if you choose to report suspicious activity to the FIU). Records must either be kept in written form in English or be readily accessible and convertible into written form in English.

You must keep identity and verification records for at least five years after the completion of that cash transaction.

If you submit an SAR to the FIU, you must keep a copy of the report for a period of at least five years after the report is made, or any longer period that DIA or the Commissioner of Police specifies.

You must keep records relating to audits for a period of at least five years.

After five years, the records must be destroyed unless there is a lawful reason why they should be retained (such as the need to comply with another enactment or to enable you to carry on your business) or the DIA or the Commissioner of Police ask you to keep records for longer.

Summary of record keeping requirements

You must keep the following records:

- Identity and verification evidence for five years from the completion of the cash transaction.
- Reports of suspicious activity for five years after the report is made or any longer period that DIA or the Commissioner of Police specifies.
- Any audits for a period of at least five years.

Audit your AML/CFT obligations

At the request of DIA, you must audit your AML/CFT compliance obligations. The auditor must be independent and suitably qualified.

5. Do you know your customer?

Customer due diligence (CDD) is the process of obtaining and verifying a customer's identity to make sure they are who they say they are. You are required to undertake CDD for any transaction that is captured by the AML/CFT Act.

Who to conduct CDD on

You must conduct CDD on:

- Your customer;
- Any beneficial owner of your customer; and
- Any person acting on behalf of your customer.

Who you must conduct CDD on	Comment
• Your customer	• Is the person who you enter into the cash transaction (or series of related cash transactions) with • Customers who are individuals (as opposed to trusts or companies for example) may be treated as the beneficial owner if you believe on reasonable grounds that the person is not acting on behalf of anyone else.
• Any beneficial owner of a customer	• Someone who owns more than 25 percent of a company that is your customer • Someone who has effective control of a company that is your customer • The person/s on whose behalf a transaction is conducted.

• Any person acting on behalf of a customer	• There are instances where a person is acting on behalf of a customer but is not necessarily a beneficial owner of that customer. For example:
	  • A person exercising a power of attorney for your customer
	  • A legal guardian acting on behalf of a minor who is your customer
	  • An employee who has the authority to act on behalf of a company that is your customer.

Identity requirements

To meet your requirements for standard CDD, the following identity information must be gathered about a customer, the beneficial owner(s), and a person acting on behalf of a customer:

- Full name
- Date of birth
- If the person is not the customer, the person's relationship to the customer
- Company identifier or registration number (if applicable).

The customer's identity must be verified before entering into a transaction where CDD is required.

Verification requirements

You must take reasonable steps to ensure that the information you gather is correct. According to the level of risk involved, you will need to take reasonable steps to verify the identity of any beneficial owners, and to verify the identity and authority of any person who is seeking to act on behalf of your customer. Verification must be done before the transaction is conducted.

How to use the Amended Identity Verification Code of Practice 2013

Identity verification needs to be done by collecting and sighting documents, data, or information provided from a reliable and independent source. You are required to keep records of this information. The Amended Identity Verification Code of Practice 2013 (IVCOP) provides suggested best practice for anyone conducting name and date of birth identity verification on customers (who are natural persons) who have been assessed to be low to medium risk. IVCOP is published on the Department's website at: http://bit.ly/2k13AxJ. Note that IVCOP should be read in tandem with the Explanatory Note, which is also available on the Department's website at: http://bit.ly/2k13AxJ.

Part 1 of IVCOP outlines some of the documents which are acceptable for AML/CFT purposes. You need one form of primary photographic identification such as a New Zealand passport; or one form of primary non-photographic identification such as a New Zealand full birth certificate in combination with a secondary or supporting form of photographic identification; or a New Zealand driver licence and another approved form of identification that is specified on page 5 of IVCOP (i.e. a credit card). The most common combination of identification that HVDs are likely to come across is a New Zealand driver licence and a credit card.

Part 2 of IVCOP relates to document certification using a trusted referee for situations where the original identity documents are not available.

Complying with IVCOP is not mandatory. However, if fully complied with, IVCOP operates as a 'safe harbour'. This means that if you fully comply with the code you are deemed to be compliant with the relevant parts of the AML/CFT Act. It is important to note that if a reporting entity opts out of a code of practice it does not receive the benefit of the safe harbour. In these circumstances, the reporting entity must comply with the relevant statutory obligation by some equally effective means. For this to be a valid justification against any alleged act or omission by the reporting entity, the reporting entity must have provided written notification to its AML/CFT supervisor that it has opted out of compliance with IVCOP and intends to satisfy its obligations by some other equally effective means.

When to conduct CDD

You must conduct CDD (i.e. obtain the required identity information and verify that information) on your customer *before* you conduct the transaction.

What to do if you cannot complete CDD

If you are not able to complete standard CDD on your customer, you must not engage in the transaction with them. To do so would be a breach of the AML/CFT Act. This applies to all circumstances where a customer fails or refuses to provide information, data or documents that you have requested. This also applies if the information, data or documents that the customer provides are inadequate. However, you are free to provide non-captured services to the customer (for example transactions using a method of payment other than cash).

If you are refusing a transaction, you should consider whether you need to file an SAR with the FIU.

It is important to note that paragraph 4 of the IVCOP states you must have appropriate exception handling procedures in place for when a customer cannot meet CDD requirements.

When you can rely on others for CDD

In some specific circumstances, reporting entities can rely on others to conduct CDD if the other party is either:

- A member of the same DBG
- Another reporting entity in New Zealand or a person in another country that has sufficient AML/CFT

systems and measures in place and who is regulated for AML/CFT purposes
- An agent.

Note the other party being relied on must consent to conducting the CDD and providing all relevant CDD information to the reporting entity.

Relying on a member of your designated business group

You can rely on another member of your DBG to conduct CDD on your customer if the identity information is provided before you carry out a transaction with the customer. Any verification information must be able to be given to you by the other member as soon as practicable but within five working days of the request.

It is important to note that you remain responsible for ensuring the CDD is conducted in accordance with the AML/CFT Act.

Relying on another reporting entity or a suitably regulated person overseas

You can rely on another person for conducting CDD on your customer so long as the person:

- Is either a reporting entity in New Zealand, or is a person resident in a country that has sufficient AML/CFT measures in place and who is regulated for AML/CFT purposes; and
- Has a business relationship with the customer concerned; and
- Has conducted CDD to at least the standard required by the AML/CFT Act and:
  - Has provided you with the relevant identity information before you have conducted the transaction; and
  - Can provide relevant verification information on your request as soon as practicable but within five working days; and
- Consents to conducting the CDD and providing all relevant CDD information to the reporting entity.

Relying on an agent

You may authorise a person to be your agent and rely on that agent to conduct CDD and obtain any information required for CDD records. In simple terms it means getting someone to carry out CDD on your behalf. “Agent” is not defined in the AML/CFT Act; instead, the ordinary principles of agency law will apply. Remember that you remain responsible for ensuring the CDD is conducted in accordance with the AML/CFT Act.

6. Understanding ML/TF risk

This section should increase your AML/CFT awareness and help you protect your business from being exploited by criminals. If after reading this section you would like to read more about risks specific to HVDs, please refer to the Phase 2 Sector Risk Assessment on DIA's website at: https://bit.ly/2TmCXE3. You may find pages 29-32 particularly useful as they relate to the HVD sector.

Vulnerabilities associated with HVDs

According to DIA's Phase 2 Sector Risk Assessment 2017, the HVD sector presents a medium-high inherent risk of ML/TF.

Purchasing high value goods from an HVD gives the impression of legitimacy, provides documentation of a source of funds, protects an offender from the added risk of trading with an unknown member of the public, and transactions can be completed relatively quickly. In addition, no special knowledge, skills, tools or resources are required for launderers to use high value goods, making this method of laundering simple and highly attractive to all criminal types.

High value cash transactions can avoid interaction with the financial sector, and money launderers can target businesses that are unlikely to reject them. High value goods are often chosen for their resale value, as easily sold items accelerate the laundering process. Moreover, high value goods are a practical option for ML/TF because transactions are straightforward to undertake, and some items can be easily transported or hidden for safe keeping.

Structuring

Structuring is when a criminal separates a large transaction into smaller ones to avoid scrutiny and detection, particularly to avoid transaction thresholds. It may be difficult to detect this activity especially if spread over time, location and via different types of HVDs. It is important that you are aware of structuring and can spot suspicious activity of this nature if it does occur.

The box below provides an example of structuring that HVDs may encounter:

This example is based on a NZD10,000 cash threshold, which is used for illustrative purposes. This example will be updated once the cash threshold value has been finalised.

The example is not specific to the named sector and applies to all HVDs.

You are a dealer of expensive jewellery. You notice a customer is regularly buying jewellery from your store with cash. Each transaction is just under the NZD10,000 threshold (but altogether the transactions exceed NZD10,000). You have a requirement to conduct standard CDD on this customer as the cash transactions appear to be related and the sum of them exceeds NZD10,000.

If you cannot complete CDD for any reason you should stop selling to this customer. You would be in breach of the AML/CFT Act if you continued to sell to a customer where the sum of related cash transactions totalled NZD10,000 or more, without conducting CDD first.

Note: A customer returning to buy or sell another item does not necessarily mean they are involved in suspicious activity. However, other factors such as the customer's behaviour might raise some red flags.

Vulnerabilities associated with the use of cash

The use of high-value commodities for ML/TF purposes is prevalent where there is an illicit cash economy. Many forms of crime, particularly drug dealing and the sale of stolen property, generate large amounts of cash. The New Zealand methamphetamine and cannabis markets, for example, are largely cash-based. This makes people who buy and sell high value goods vulnerable to money launderers.

Cash remains a popular vehicle for transactions associated with these and other criminal offences because it:

- Is anonymous and flexible
- Exists outside of formal financial institutions
- Does not require any recordkeeping
- There is no paper trail.

Red flags that you may encounter

The table below summarises some of the red flags you may encounter as you carry out your business. It also includes suggested ways to manage the ML/TF risk. For scenarios like the ones below, you may also decide to submit an SAR to the FIU if you think the activity or transaction is suspicious:

Description of ML/TF risk	Notes	What can I do to manage the risk
• The customer is on edge and the cash notes are presented in an unusual condition (i.e. damp, dirty, odorous or coated with substance).	• This may indicate that the money has been used to purchase drugs. • This may indicate the money has been stored in an unorthodox manner (i.e. buried).	• Ask questions to find out where the money has come from and the purpose of the transaction. • Staff safety is most important. Refer to your business' health and safety procedures for dealing with threatening and/or on edge customers.
• The transaction/activity appears to make no business sense.	• If a transaction does not appear to make any business sense it may be because a criminal is trying to launder funds.	• Ask questions to find out whether it is a legitimate transaction (i.e. what is the purpose of this transaction? where have the funds come from?).
• Customer knowingly wishes to sell at an artificially low price and/or is disinterested in obtaining a better price.	• Customers willing to sell items for less than they are worth may indicate the high value good was obtained from criminal activity.	• Ask questions to find out why they are willing to sell the item at a low price.
• Customer is reluctant to provide adequate identification information when making a purchase.	• You must conduct CDD on your customer before you conduct the transaction or activity. • If you are not able to complete CDD on your customer, you must not engage in the transaction with them. To do so would be a breach of the AML/CFT Act.	• Have information available to inform customers on why CDD is necessary for AML/CFT purposes. • Explain to customers that all personal information collected under the AML/CFT Act will be handled in accordance with the Privacy Act 1993. This ensures their personal information is protected and handled appropriately.

Description of ML/TF risk	Notes	What can I do to manage the risk
• There is reason to believe the customer is an intermediary conducting the transaction on behalf of an unrelated third party (for example, the purchase of a vehicle that is intended for the use of the third party and not the purchaser themselves).	• This may result in the beneficial owner or effective controller not being transparent, which increases ML/TF risk.	• If you have reason to suspect the customer is an intermediary conducting the transaction on behalf of an unrelated third party, ask who the item is intended for and whether they are paying for it with their own money or someone else's. • Ensure CDD is conducted on the third party as well as the customer you are dealing with.
• The customer appears nervous or exhibits uncooperative behaviour.	• This may indicate the customer is involved (or has been involved) in illicit activity.	• Ask questions to find out more about the customer.
• A customer orders an item, pays for it in cash, cancels the order and then receives a refund.	• Money launderers may order an item and then cancel it as a way of making 'dirty' money appear 'clean'. Often criminals will want the refund paid into a bank account – it is a way of introducing illicit funds into the legitimate economy.	• Ask questions to find out why the order was cancelled.

Description of ML/TF risk	Notes	What can I do to manage the risk

• The customer is from a high-risk jurisdiction	• Dealing with customers from high-risk jurisdictions may increase your ML/TF risk.	• The following resources may help you assess country risk:
		  • KnowYourCountry Ratings Table (https://bit.ly/2CrXsC1)
		  • Ministry of Foreign Affairs & Trade – UN Sanctions List (https://bit.ly/2CHyTEf)
		  • Transparency International Corruption Perceptions Index 2017 (https://bit.ly/2BJaDBF)
		  • You can find the list of FATF high-risk or monitored jurisdictions on the FATF website (https://bit.ly/2FUuIHX)
		  • The Basel AML Index 2017 Report (https://bit.ly/21zJCmQ)
		  • You may also find page 11 of the Prompts and Notes guidance (https://bit.ly/2OyUCmy) provided by DIA useful when assessing country risk. The Country Assessment Guideline that is referred to in the Prompts and Notes document can also be found on our website (https://bit.ly/2xM6vwa)
		• If you have established that a customer is from a high-risk jurisdiction, you may want to ask them questions to find out where the money has come from.

7. Do you know where to get support?

You can access compliance support from a range of sources:

- DIA as your AML/CFT supervisor
- Professional bodies
- Independent legal or professional advice
- Open source information for the precious metals and stones sector.

Support from your AML/CFT supervisor

We recognise that adjusting to the new AML/CFT system will take time and effort, so we aim to provide you with support. We provide general information and guidance, and more specific support when you are having difficulty understanding your requirements but have a genuine intention to comply. The DIA website provides a wide range of information about how you can comply with the AML/CFT Act. We will advise you when new guidelines are made available.

Support from your industry body

You are encouraged to keep up-to-date and be aware of the information and education on offer from your industry body.

When to seek independent advice

There will be occasions when you need to seek independent advice to ensure you remain compliant with the AML/CFT Act. DIA cannot provide you with legal advice. When you have specific compliance questions about unique circumstances that DIA or your professional body cannot reasonably answer, you may need to seek independent legal advice or advice from an otherwise suitable professional.

Open source information for the precious metals and stones sector

You may find the following resources useful for understanding more about ML/TF risk facing the HVD sector:

- FATF Guidance on Risk-Based Approach for Dealers in Precious Metals and Stones (available at: https://bit.ly/2EblWE9)
- Implementing AML/CFT Measures in the Precious Minerals Sector: Preventing Crime While Increasing Revenue (available at: https://bit.ly/2UynRID)
- FATF Money Laundering and Terrorist Financing Through Trade in Diamonds (available at: https://bit.ly/2Qo1F5r)
- FATF Money Laundering and Terrorist Financing Risks and Vulnerabilities Associated with Gold (available at: https://bit.ly/1FVxTKl).

Glossary

AML/CFT Act (or Act)	Anti-Money Laundering and Countering Financing of Terrorism Act 2009.
Cash	Cash is defined in Section 5 of the AML/CFT Act. It means physical currency (i.e. New Zealand dollars and foreign currency) or bearer-negotiable instruments. Bearer-negotiable instrument means – (a) a bill of exchange; or (b) a cheque; or (c) a promissory note; or (d) a bearer bond; or (e) a traveller's cheque; or (f) a money order, postal order, or similar order; or (g) any other instrument prescribed by regulations. Note that all cheques (including bank drafts) are considered bearer-negotiable instruments for the purposes of the AML/CFT Act.
Customer due diligence (CDD)	The process of obtaining and verifying a customer's identity to make sure they are who they say they are.
Customer	The person who you enter into a cash transaction with.
Department of Internal Affairs (DIA)	The government department tasked with supervising some AML/CFT reporting entities, including HVDs.
Designated business group (DBG)	A group of two or more entities who have elected, and been approved by their AML/CFT supervisor, to combine some of their AML/CFT obligations. Each member of the DBG should be a related reporting entity in New Zealand (or equivalent jurisdiction).
Domestic physical cash transaction	A domestic physical cash transaction means a transaction in New Zealand involving the use of physical currency. It does not include transactions involving bearer-negotiable instruments (i.e. a bill of exchange, cheque, promissory note, bearer bond, traveller's cheque, money order, postal order or similar order).
Financing terrorism offence	As defined in Section 8(1) of the Terrorism Suppression Act 2002.
goAML	The New Zealand Police Financial Intelligence Unit's (FIU's) online reporting portal.
High value good	A high value good is defined in the AML/CFT Act. See Section 2 'Applying the AML/CFT Act to your business' for more information.
Large cash transaction (LCT)	In the context of HVDs, an LCT is a domestic physical cash transaction which meets or exceeds an applicable threshold value.
Money laundering offence	As defined in Section 243 of the Crimes Act 1961.
New Zealand Financial Intelligence Unit (FIU)	The FIU collects, analyses and disseminates financial intelligence relating to suspicious activities and transactions, money laundering and the financing of terrorism.

Ordinary course of business	Some of the relevant factors to take into consideration when determining whether an activity is in the ordinary course of business include: • Is normal or otherwise unremarkable for your business • Is frequent • Is regular (meaning predictable, consistent) • Involves significant amounts of money • Is a source of income • Involves significant resources • Involves a service offered to customers. See Section 2 'Applying the AML/CFT Act to your business' for more information.
Prescribed transaction report (PTR)	It is a report made to the Financial Intelligence Unit on a prescribed transaction. In the context of HVDs, a prescribed transaction is a domestic physical cash transaction which meets or exceeds an applicable threshold value.
Reporting entities	Businesses that must comply with the AML/CFT Act. For example, casinos; designated non-financial businesses or professions; financial institutions; high value dealers; and the NZ Racing Board.
Supervisors (AML/CFT supervisors)	AML/CFT supervisors have responsibility for monitoring compliance with the AML/CFT Act. DIA is the AML/CFT supervisor for a number of sectors including HVDs. The Reserve Bank of New Zealand and the Financial Markets Authority supervise other sectors.
Suspicious activity report (SAR)	A report made to the FIU regarding a suspicious activity. This includes transactions as well as other activities. It is optional for HVDs to submit SARs.
Suspicious property report (SPR)	A report made under the Terrorism Suppression Act 2002 regarding property that you suspect is owned or controlled by a "designated terrorist entity".

Appendix A: Compliance obligations for other reporting entities

Below is a summary of the additional AML/CFT compliance obligations that apply to other sectors, but not to HVDs. You should consider whether any of these additional requirements can help protect your business from being exploited by criminals.

What needs to be done?	What this means for reporting entities (other than HVDs)	How this could apply to HVDs
• Appoint a Compliance Officer.	• A Compliance Officer is appointed to administer and maintain a reporting entity's AML/CFT programme. • The Compliance Officer must be an employee of the reporting entity and report to a senior manager. Alternatively, the Compliance Officer may be a senior manager themselves.	• You could appoint someone senior in your business to be responsible for ensuring your business is meeting its AML/CFT obligations.
• Conduct a risk assessment.	• A reporting entity must undertake an assessment of risks posed to their business by money laundering and financing of terrorism.	• Section 6 'Understanding ML/TF risk' will help you have a general understanding of ML/TF risk. • You may want to consider and record ML/TF risks as they apply to your business. You may also want to document the policies and procedures that your business follows when you do conduct a transaction captured by the AML/CFT Act.
• Develop an AML/CFT programme.	• A reporting entity must develop an AML/CFT programme based on their assessment of ML/TF risks. • It should include policies, procedures and controls for ensuring all compliance obligations are adequately and effectively met.	

What needs to be done?	What this means for reporting entities (other than HVDs)	How this could apply to HVDs
• Report SARs to the FIU.	• When reporting entities identify suspicious activity they must report it to the FIU within three working days of forming that suspicion.	• While it is optional for you to report SARs to the FIU, DIA strongly recommends you report any suspicious activity as these reports provide crucial information to assist the New Zealand Police and other AML/CFT agencies to investigate serious crime using financial intelligence. • We recommend you report any suspicious activity to the FIU within three working days of forming that suspicion.
• Conduct CDD (including enhanced customer due diligence (EDD)).	• Reporting entities are required to apply the level of CDD depending on the level of risk involved. • In some circumstances with higher ML/TF risk, an increased level of CDD is required. This is known as EDD. • For example, reporting entities (other than high value dealers) are required to conduct EDD on a politically exposed person (PEP). A PEP is an individual who is or has been entrusted with a prominent overseas public function in the preceding 12 months, or a relative or close associate of that individual. Due to their position and influence, many PEPs are in positions that can potentially be abused for the purposes of ML/TF.	• You may want to conduct EDD on customers that are higher risk (or the transaction/activity is of higher risk). • EDD requires the collection and verification of the same identity information that is required for standard CDD. However, when undertaking EDD you may need to use increased or more sophisticated measures to do this. • EDD also requires the collection and verification of information relating to the source of wealth (SoW) or source of funds (SoF) of your customer. This to establish where the funds have come from and to determine whether their spending matches their wealth.

What needs to be done?	What this means for reporting entities (other than HVDs)	How this could apply to HVDs
• Ongoing customer due diligence and account monitoring.	• Reporting entities are required to undertake ongoing CDD and account monitoring for customers they are in a business relationship with. • This is to ensure that they have continued confidence that the business relationship and transactions within the relationship are consistent with the customer's business and risk profile. It also assists in spotting suspicious activity.	• Most HVDs will be having one-off interactions with customers. • However, if you are dealing with repeat customers it is worth you considering whether CDD needs to be ongoing. • It may also be worth you monitoring the customer's transactions to help identify suspicious activity over time.

• Keep records.	• Reporting entities are required to obtain the same records as HVDs, as well as the following:
	  • records of transactions;
	  • records that are relevant to the establishment of the business relationship;
	  • records of the risk assessment;
	  • records of the AML/CFT programme; and
	  • any other related records that may be of interest to the supervisor.
		• DIA strongly suggests you keep records of PTRs submitted to the FIU, records on whether an SAR was necessary or not, and an up-to-date record of your risks and any documented policies and processes (see Section 6 'Understanding ML/TF risk).

• Reviewing the risk assessment and AML/CFT programme.	• Reporting entities must conduct a regular review of their risk assessment and AML/CFT programme. • This is to ensure that any business changes or new risks in the operating environment are captured and AML/CFT documents remain fit-for-purpose.	• If you document the risks your business faces, as well as any policies and procedures you follow, DIA recommends that you keep these up-to-date and set a timeframe to review them.

What needs to be done?	What this means for reporting entities (other than HVDs)	How this could apply to HVDs
• Audit risk assessment and compliance programme every two years.	• At least every two years reporting entities must review their risk assessment and compliance programme and have it audited by an independent person who is suitably qualified to conduct the audit.	• You are required to have your compliance obligations audited by an external auditor at the request of DIA.

Endnotes

1. The recent changes were made by the Anti-Money Laundering and Countering Financing of Terrorism Amendment Act 2017 (the AML/CFT Amendment Act): https://bit.ly/2rsooys

2. HVDs that are unable to conduct CDD must comply with Section 37 of the AML/CFT Act: https://bit.ly/2RQalOL

3. You can find out more information about the FIU on their website: https://bit.ly/2QqPF3k

4. Section 9, AML/CFT Act: http://bit.ly/2iR0JH3

5. Section 5(1), AML/CFT Act: https://bit.ly/2Emg0IF

6. Section 2(3) of the Companies Act: https://bit.ly/2GyqlTk

7. The DIA has published guidance on the term 'related' for DBGs: https://bit.ly/2EmXjp1

8. You may also find page 11 of the Prompts and Notes guidance (https://bit.ly/2OyUCmy) provided by DIA useful when assessing country risk. The Country Assessment Guideline that is referred to in the Prompts and Notes document can also be found on our website (https://bit.ly/2xM6vwa).

9. Section 5(1), AML/CFT Act: https://bit.ly/2xHGfmy

10. Section 243, Crimes Act 1961: http://bit.ly/2zYeqXU

11. Section 8(1) and (2A), Terrorism Suppression Act 2002: http://bit.ly/2lZbZlE

12. DIA has produced guidance on 'Beneficial Ownership': https://bit.ly/2BwaZgI

13. DIA has produced a factsheet on 'Acting on behalf of a customer': https://bit.ly/2rvRXPB

14. Section 32(1), AML/CFT Act: http://bit.ly/2hjDuF3

15. Section 33(1), AML/CFT Act (http://bit.ly/2nQNm8F), and see the AML/CFT supervisors' Countries Assessment Guideline (http://bit.ly/2Fc2upe) or the Basel Index (https://bit.ly/2djRNDR), which ranks countries by AML/CFT risk

16. Section 34, AML/CFT Act: http://bit.ly/2HDbWTl

17. Inherent risk is the assessed ML/TF risk before any controls or mitigation measures have been put in place

18. Enhanced Customer Due Diligence Guideline: https://bit.ly/2GrKaHV.

Te Tari Taiwhenua
Internal Affairs

New Zealand Government