



Financial Intelligence Unit

Government of the Cook Islands

Financial Transactions Reporting Act 2017 Practice Guideline for Motor Vehicle Dealers, Pearl Dealers, Jewellers and other persons who deal in high value items.

1. Introduction

The purpose of this document is to provide some guidance specifically for those businesses who deal in high value products.

This document is designed to assist you with your Anti Money Laundering and Terrorist Financing (AML/CFT) obligations and should be read in conjunction with the Financial Transactions Reporting Act 2017 (FTRA), the Financial Transactions Reporting Regulations 2017 (Regulations) and the Practice Guidelines for the Financial Transactions Reporting Act 2017 (Guidelines).

It should be noted these guidelines are not law and do not constitute legal advice. They should not be relied upon as evidence of you complying with your obligations under the FTRA and the Regulations. You should seek your own independent legal advice on the interpretation and requirements of the FTRA and the Regulations.

If you have any questions or require more information concerning these guidelines, the FTRA, the Regulations and the Guidelines please contact the Financial Intelligence Unit.

2. Who has obligations under the FTRA?

Any person who carries on business dealing in high value items of any type are captured however these are likely to include businesses such as:

- art dealers;
- auctioneers;
- motor vehicle dealers;
- jewellers or pearl dealers; and
- precious metal or stone dealers.

3. What are your obligations under the FTRA?

You must develop internal policies, procedures, controls and systems to ensure the following obligations are met:

- internal compliance programme and risk assessments under Part 2, including;
 - appointing a Money Laundering Reporting Officer (MRLO) to oversee your compliance programme;
 - training employees to be aware of the policies, procedures and audit systems adopted by your organisation to deter money laundering and the financing of terrorism;
 - screening directors and key employees before appointing them; and
 - establishing an internal review function to test the effectiveness of your compliance programme and its compliance with the FTRA.
- customer due diligence including identifying Politically Exposed Persons (PEPs) and record keeping under Part 3;
- reporting of cash transactions and suspicious activities under Part 4.

Please refer to the Guidelines for further information and assistance in relation to each of the obligations mentioned above.

4. What are some of the risks specific to the high value goods sector?

High value items represent a higher risk of financial misconduct when they:

- can be used as a transfer of wealth;
- have a high intrinsic value;
- are relatively easy to transport;
- can be bought and sold easily or anonymously; and/or
- are regularly used in most areas of the world.

For example gold is particularly attractive to money launderers because it has a high intrinsic value, is readily accepted across the world and can be melted down into many different forms.

The use of cash or bearer negotiable instruments (“BNIs”) as a means of payment or method to transfer funds can pose a higher risk of financial misconduct than other means, such as wire transfer or credit cards. Unlike many other financial products, with cash, monetary instruments and BNIs there will, likely be no clear audit trail and it may be unclear where the funds have originated from.

Therefore, where cash, monetary instruments or BNI transactions are being proposed by customers, and such requests are not in accordance with your usual experience in dealing with your customers, you must approach such situations with caution and make relevant further enquiries. In relation to cash transactions, you should consider factors such as the amount, currency, denominations and the age of the notes in determining whether the activity is ‘normal’ for the customer along with a comparison with the customer’s expected activity.

You should be vigilant for explanations given by customers which do not stand up to scrutiny. If you are not satisfied that the transaction is legitimate activity, therefore considering it suspicious, a suspicious activity report to the FIU must be made.

5. High Risk Indicators

As with all types of risk assessment, a holistic approach should be taken and the indicators below should be taken into consideration, together with all other relevant factors:

- the transaction(s) does not appear in line with what would be expected of the customer. For example, a legal person acting on their own behalf, not a customer making a bulk purchase;
- the customer over-pays and then requests their over-payment to be refunded by wire transfer or cheque instead of cash. For example a customer wishes to purchase two items, pays for both in cash and then chooses to buy only one of the items;
- the transaction appears to be conducted on behalf of another person;
- it is unusual for a customer to pay cash for the goods in question;
- small denominations of cash used for a large payment;
- the customer has previously paid for goods using debit/credit card or cheque but suddenly offers a large cash payment;
- unusual delivery requests such as asking for an item to be shipped to a third party overseas; and
- unusual enquiries regarding the businesses refund policy. For example, asking if a refund can be made by cheque, transfer or to a third party.

The above list is not exhaustive. New methods for laundering money and financing terrorism are constantly being developed. Typologies reports produced by the FIU are available on the FSC’s website and you should contact the FIU for the latest information where you are uncertain or have questions on any risk matter.

6. When should you conduct Customer Due Diligence?

Customer due diligence must be undertaken by you at any point a person wishes to purchase any high value item to the value of \$10,000 NZD or more.

7. Record Keeping

All copies of customer due diligence information and transactional information must be kept for a minimum period of 6

years from the date of the transaction or the end of an ongoing business relationship.

8. What must be reported to the FIU?

Suspicious Activity

Any activity or requests by a customer or prospective customer that appears to you to be unusual or suspicious in your experience with dealing customers, must be reported to the FIU under section 47. The list in Part 5 above provides guidance as to the type and nature of transactions, events and circumstances that might give you reasonable cause to suspect an activity is suspicious.

Cash Transactions

A purchase of any high value item in cash equal to or greater than \$10,000.00 NZD (or its equivalent) must be reported to the FIU.

9. FIU's Approach to Compliance Monitoring & Enforcement

The FIU has a responsibility to ensure that all reporting institutions are complying with all legislative requirements under the FTRA. To do this, the FIU is being empowered under the Financial Intelligence Act 2015 (FIU Act) to examine your compliance with

the FTRA. The FIU may request information from you, conduct on-site examinations and provide reports to you for this purpose.

The FIU is empowered under section 31 of the FIU Act to enforce compliance on reporting institutions that have failed to comply in whole or in part with any of the obligations under the FTRA, or have failed to undertake directives issued by the FIU to take remedial actions.

10. Penalties for Non-Compliance

Failure to comply without reasonable excuse may cause the FIU to bring legal proceedings including prosecution of which a penalty of up to \$250,000 or a term of imprisonment of up to 5 years may be applied to an individual, or a penalty of up to \$1,000,000 for a body corporate.

11. FIU Contact

For further information about your obligations under the Act, or the FIU and its activities, or, contact the FIU Office on (682) 29182 or email: intel@cifu.gov.ck.