ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

Banking

Sector Specific AML/CFT Guidance Notes

August 2021

Whilst this publication has been prepared by the Financial Services Authority, it is not a legal document and should not be relied upon in respect of points of law. Reference for that purpose should be made to the appropriate statutory provisions.

Contact:
AML/CFT Division
Financial Services Authority
PO Box 58
Finch Hill House
Bucks Road
Douglas
Isle of Man
IM99 1DT

Tel: 01624 646000
Email: aml@iomfsa.im
Website: www.iomfsa.im

Version 3
Last updated August 2021

Contents

Version history

Version 2 (April 2020)	Updates made to links in relation to the updated NRA
Version 3 (August 2021)	Updates to reflect changes to the main structure of the AML/CFT Handbook Updates to footnotes to include links in the main body for consistency purposes 5 - changes made to reflect the removal of timescales for ongoing monitoring from the Code

1. Foreword

For the purposes of this sector specific guidance, the terms "banking" and "bank" refer to a business conducting activity that would require a licence under Class 1 of the Regulated Activities Order 2011 (as amended) to undertake deposit taking.

2. Introduction

The purpose of this document is to provide some guidance specifically for the banking sector in relation to anti-money laundering and countering the financing of terrorism ("AML/CFT"). This document should be read in conjunction both with the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019 ("the Code") and the main body of the AML/CFT Handbook ("the Handbook").

Though the guidance in the Handbook, and this sector specific guidance, is neither legislation nor constitutes legal advice, it is persuasive in respect of contraventions of AML/CFT legislation dealt with criminally, by way of civil penalty or in respect of the Authority's considerations of a relevant person's (as such a term is defined in paragraph 3 of the Code) regulatory / registered status and the fit and proper status of its owners and key staff where appropriate.

This document covers unique money laundering and financing of terrorism ("ML/FT") risks that may be faced by banks and provides further guidance in respect of approaches to customer due diligence where it may vary across or between sectors.

The case studies in this document were taken from typologies published by the Australian Transaction Reports and Analysis Centre ("AUSTRAC") and the Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC"). The Authority recommends that relevant persons familiarise themselves with these, and other typology reports concerning the banking sector such as the FATF Guidance for a Risk Based Approach for the Banking Sector which was published in 2014.

2.1 National Risk Assessment

The Island's first National Risk Assessment ("NRA") was published in 2015 and was updated in 2020. The banking sector must ensure their business risk assessment (and customer risk assessments where necessary) take into account any relevant findings of the NRA.

The nature of banking products and services, and some customer segments serviced (including high net worth individuals ("HNWI"), complex structures and PEPs), result in core inherent vulnerabilities. These vulnerabilities include, but are not limited to:

- Difficulty in establishing source of funds / source of wealth in more complex structures and understanding the purpose of such structures;
- The non-face to face nature of relationships and use of introducers / third parties;
- Sanctions risks arising from the international nature of the sector and exposure to higher risk countries (including for payments); and
- Domestic laundering (using cash) from drug related crimes.

The importance of strong controls is therefore paramount to manage and mitigate these vulnerabilities. The NRA sets out the main risks and vulnerabilities in detail.

It is considered that the overall risk for Banking is medium taking into account the threats and vulnerabilities, balanced against the controls in place in the sector. The domestic inherent retail risk (including HNWI) is medium but the international retail (including HNWI) and corporate / trust sector risks are inherently medium high. There are limited instances of the IoM banking sector being potentially used for FT, and ML is considered to be the higher risk.

3. Risk Guidance

The banking industry is a broad sector and the ML/FT risks will vary for each bank based on a wide range of factors such as the type of products they supply, their customers and delivery channels.

The Code mandates that a number of risk assessments are completed –

- a business risk assessment (paragraph 5);
- a customer risk assessment (paragraph 6); and
- a technology risk assessment (paragraph 7)

In order to complete these risk assessments and keep them up-to-date vigilance should govern all aspects of a bank's dealings with its customers, including:

- account opening;
- non-account holding customers;
- safe custody and safe deposit boxes;
- deposit-taking;
- lending; and
- transactions into and out of accounts generally, including by way of electronic transfer (wire transfer) and automated cash deposits into third party accounts.

3.1 General Higher Risk Indicators

As with the basic elements of a risk assessment, discussed in chapter 2 of the Handbook, the following activities may increase the risk of the relationship. Just because an activity / scenario is listed below it does not automatically make the relationship high risk; a customer's rationale / nature / purpose of the business relationship etc. should be considered in all cases.

If a bank is unable to obtain a satisfactory explanation from a customer in the event of the following situations, features, or activities, or any other features which cause it concerns, it should be determined whether this is suspicious or unusual activity. Refer to chapter 5 of the Handbook for further detail of the Island's suspicious activity reporting regime.

As stated in paragraph 13 (Ongoing monitoring) of the Code:

13 Ongoing monitoring

(2) Where a relevant person identifies any unusual activity in the course of a business relationship or occasional transaction the relevant person must –

(a) perform appropriate scrutiny of the activity;

(b) conduct EDD in accordance with paragraph 15; and

(c) consider whether to make an internal disclosure.

(3) Where a relevant person identifies any suspicious activity in the course of a business relationship or occasional transaction the relevant person must –

(a) conduct EDD in accordance with paragraph 15 of the Code, unless the relevant person believes conducting EDD will tip off the customer; and

(b) make an internal disclosure.

This list of higher risk indicators is by no means exhaustive, and banks should be vigilant for any transactions where suspicion may be aroused and take appropriate measures. A list of suggested red flags is included at section 3.2 of this document.

- where a customer is reluctant to provide normal information or provides only minimal information;
- where a customer's documentation cannot be readily verified;
- where a customer seems to deliberately provide information which is difficult or expensive for the bank to verify;
- the customer is reluctant to provide the bank with complete information about the nature and purpose of the relationship including anticipated account activity;
- the customer is located in a higher risk jurisdiction;
- transactions involving numerous jurisdictions;
- unusual cash deposits without apparent cause, particularly where such deposits are subsequently withdrawn or transferred within a short time;
- frequent small or modest cash deposits which taken together are substantial;

- the collection (either within the Isle of Man or in another country or territory) of significant cash sums singly or in accumulations without a plausible and legitimate explanation;
- where deposits are received from other banks and the bank is aware of a regular consolidation of funds from such accounts prior to a request for onward transmission of funds;
- the customer is reluctant to meet personnel from the bank in person and / or uses a "front person;
- the avoidance by the customer or its representatives of direct contact with the bank (such as the use of night safes to make large cash deposits);
- the use of nominee accounts, trustee accounts or client accounts which appear to be unnecessary for, or inconsistent with, the type of business carried on by the underlying principal;
- the use of numerous accounts for no clear commercial reason where fewer would suffice (so serving to disguise the scale of the total deposits);
- the use by the customer of numerous individuals (particularly persons whose names do not appear on the mandate for the account) to make deposits, the bank must ensure it knows the beneficial owner as per the Code requirements;
- frequent switches of funds between accounts in different names or in different countries or territories;
- substantial withdrawal(s) from a previously dormant or inactive account;
- substantial withdrawal(s) from an account which has just received an unexpected large credit from overseas;
- substantial withdrawal(s) from an account that incurs a significant penalty which would normally be avoided;
- use of bearer instruments outside a recognised dealing system in settlement of an account or otherwise;
- where there appears to be no reasonable explanation to retain an account in a different jurisdiction to that of the customer;
- where a customer declines to provide information which normally would make them eligible for valuable credit or other premium banking services (which benefit the customer); or where they inexplicably avoid normal banking facilities, such as higher interest rate facilities for larger credit balances;
- the customer exhibits unusual concern with the bank's compliance with reporting requirements and/or AML/CFT policies and procedures;
- the customer funds deposits, withdraws or purchases financial / monetary instruments below a threshold amount to avoid certain reporting / record keeping requirements;
- wire transfers / payments are sent to, or originate from, high risk jurisdictions without apparent business reason; and
- the customer's transaction pattern suddenly changes in a manner that is inconsistent with the customer's normal activities or inconsistent with the customer's profile.

3.2 Red Flags

In addition to the above higher risk indicators, there are some factors that are likely to be "red flags" in relation to that particular relationship and would therefore usually be suspicious activity. If a relevant person identifies suspicious activity appropriate steps as explained in section 3 of this document, and the Code, must be taken. This list of red flags is by no means exhaustive and is as follows:

- where it is identified a customer provides false or misleading information and/or has tried to conceal their identity;
- where it is identified a customer provides suspicious identification documents;
- the customer refuses to provide the bank with relevant / accurate information about the nature and intended or ongoing purpose of the relationship, including anticipated account activity;
- the customer is secretive / evasive when asked to provide more information;
- when requested, the customer refuses to identify a legitimate source of funds or source of wealth;
- the customer refuses to provide details on beneficial owners of an account or provides information which is false, misleading or substantially incorrect;
- the customer enquires about how quickly they can end a business relationship;
- where the business relationship is ended unexpectedly by the customer and the customer accepts unusually high fees to terminate the relationship without question;
- the customer appears to be acting on behalf of someone else and does not provide satisfactory information regarding whom they are acting for;
- the customer is known to have criminal / civil / regulatory proceedings against them for crime, corruption, misuse of public funds or is known to associate with such persons; and
- the customer is interested in paying higher charges to keep their identity secret.

3.3 Other risk factors specific to the banking sector

The following section of the guidance covers some of the other risk factors specifically related to the banking sector. Further guidance surrounding risk assessments is outlined in chapter 2 of the Handbook.

- Loan and mortgage facilities (including the issuing of credit and charge cards) could be used by launderers at the layering or integration stages of the traditional ML process. Secured borrowing can be an effective method of layering and integration because it

puts a legitimate financial business (the lender) with a genuine claim to the security in the way of those seeking to restrain or confiscate the assets.

- Particular precautions need to be taken in relation to requests to hold boxes, parcels and sealed envelopes in safe custody. Where such facilities are made available to non-account holders, the identification and verification procedures of the Code must be complied with.

4. Customer due diligence

Part 4 of the Code requires relevant persons to undertake customer due diligence and ongoing monitoring in relation to all business relationships. Chapter 3 of the Handbook provide guidance on how to identify and verify the identity of the customer in relation to both a natural and legal person. Also, guidance on the timing of identification and verification of identity is provided. Please also see section 3.8 of the Handbook for further details on source of funds and source of wealth. For details of particular concessions which may be applicable please see Chapter 4 of the Handbook.

In all cases where the requirements of Part 4 of the Code cannot be met (Paragraphs 8(5), 9(9), 10(5), 12(11), 14(6), 15(8) and 19(11)) the procedures and controls must be provide that –

(a) the business relationship must proceed no further;
(b) the relevant person must consider terminating[1] the business relationship; and
(c) the relevant person must consider making an internal disclosure.

In instances where the above occurs any decisions must be documented with the rationale for the decision explained, and signed off, in accordance with the bank's processes.

4.1 The formation of a business relationship

Paragraph 8(2) of the Code provides that, the procedures and controls in relation to new business relationships must be undertaken -

8 New business relationships
(a) before a business relationship is entered into; or
(b) during the formation of that relationship.

[1] In relation to a new business relationship (paragraph 8) the business relationship must be terminated.

In respect of a bank it is considered that issuing an account number to a customer (e.g. following receipt of an application form and loading customer details onto the system), whether as a "pending account" or otherwise, would constitute forming a business relationship. However, it is recognised that the relationship may not yet be fully established. Accepting funds into a pending account also constitutes forming a business relationship (even where no withdrawals or transfers can be made) but again it is recognised that the business relationship may not yet be fully established.

4.2 Un-activated accounts

When an application form is received by a bank with no CDD, or unsatisfactory CDD attached (rather than a minor issue with the CDD as explained in section 4.3 of this document) the bank may require that an account number is assigned to the customer in order to process the application. As there is no CDD held on the customer the relationship cannot be fully established. Therefore, the bank must ensure that no funds are allowed in or out of the account (i.e. a "no deposits flag" or similar must be in place) and the account cannot be "active".

The system must be able to physically prevent the straight through deposit of funds to the account. The customer should be made aware that funds will not be accepted or withdrawn until CDD is complete and satisfactory. When the CDD is complete an appropriately experienced member of staff must remove the "no deposits flag" to enable funds to be received into the account (the account may at this point still be blocked for withdrawals if it has not fully been signed off).

If funds are received (electronically or by cheque) the bank must have a process in place to deal with this and the funds must not be deposited into the account. The bank must either delay the application of funds / cashing of the cheque until the account has been signed off, or return the funds / cheque.

4.3 Pending accounts

Pending accounts may be used for operational purposes where there may be a minor issue to address before the account can be fully signed-off. When an account is treated as a "pending account" customer funds may be received into these accounts but no withdrawals should be permitted until the account take-on process is satisfactorily completed and the "pending" status removed.

Examples of the common issues which a bank may face in completing the account sign-off include:

- problems with certification of identity documents;
- missing, insufficient or out-of-date address verification documents; and/or:

- a lack of full information on submitted application forms.

An account would not be able to be treated as a "pending account" if an application form was received with no additional supporting documentation (see section 4.2 of this document). To use a "pending account", the verification of the customer's identity must have been completed (paragraph 8 of the Code only allows the verification of identity to be absent in very exceptional circumstances (paragraph 8(4)). Also, the customer's source of funds and the nature and intended purpose of the relationship must have been established.

5. Ongoing Monitoring

The Code requirements in relation to ongoing monitoring of business relationships are covered by paragraph 13 of the Code. Section 3.4.6 of the Handbook further explains the ongoing monitoring provisions of the Code.

CDD information in respect of all customers should be reviewed periodically to ensure that it is accurate and up to date. It should also be considered as part of this review whether there are any changes to the customer risk rating. To be most effective, resources should be targeted towards monitoring those relationships presenting a higher risk of ML/FT.

5.1 Frequency of ongoing monitoring – standard risk relationships

The Handbook explains that dates for periodic CDD/ECDD reviews are set on a risk sensitive basis. The depth and breadth of CDD/ECDD to be reviewed and the frequency of such reviews being determined per the risk.

The Authority accepts that in respect of some banks, due to the volume and nature of clients that services are provided to, CDD information on standard risk customers may be reviewed on a trigger event basis.

In order for such a trigger event approach to be acceptable and effective, the triggers themselves need to be suitably robust and comprehensive, with reference to the types of customers and products within the standard risk portfolio. Banks should also consider if a backstop review period should be in place for the review of standard risk customers' CDD information (in the event that triggers do not occur).

For example, appropriate arrangements should be in place to screen the customer database to establish whether any customers may have had a change of status, for example have become PEPs. In addition, consideration should also be given to the adequacy of monitoring systems in place for corporate customers to make sure that companies to which services are provided (and transactions processed) have not been struck off. Further information on screening is included in sections 3.4.6.1, 3.4.6.2 and 3.8.10.1 of the Handbook and section 5.2 of this document.

In addition section 3.3.6 Handbook sets out that changes of CDD information should be verified on a risk basis.

5.2 Customer Screening

Screening of a customer usually falls into two distinct parts:

- Initial screening undertaken as part of CDD checks during the take on of a customer relationship, and
- Screening of the bank's client base as part of ongoing monitoring processes.

Initial CDD screening by banks should be conducted as part of the customer risk assessment required by paragraph 6 of the Code, in order to assist in determining the ML/FT risks associated with the customer. It will often take the form of a search performed on the name of the customer (or connected account party) using public domain and/or internal risk management systems. Banks should ordinarily screen to determine whether the customer or other party has any PEP connections, is subject to any sanctions restrictions, or adverse information/negative press.

In respect of ongoing monitoring, ideally, information on all parties associated to a customer relationship should be uploaded into a searchable database, which would then be automatically screened on a periodic basis (which could be daily) for PEP and sanctions information, and any 'hits' would be investigated to determine whether or not they are appropriate to the customer.

As part of ongoing monitoring, the Authority considers it is also appropriate for banks to screen their client database for negative press / adverse information on a periodic basis, in addition to the checks undertaken during client take-on. The Authority considers that if automatic screening of the bank's database for negative press is not possible or practical, then screening for this should be conducted manually in line with the timeframes set out in section 5.1 above. More frequent monitoring of negative press information for known PEP customers should also be considered.

5.3 Higher risk customers

It is important that the reviews in respect of higher risk customers are conducted on a timely basis, with details of the review being fully documented in order that timeliness, completeness and consistency can be demonstrated. Where such reviews are not conducted within the intended period, it is important any 'backlog' position is reported outside of the team conducting the review, in order that any associated risks can be monitored (i.e. to a risk committee or board).

A review may identify issues that require remediation but which cannot be resolved promptly. Any remediation activity must be time limited and tracked to completion. With reference to this, and depending on the level of concerns arising from outstanding matters, banks should consider whether activity on an account should be restricted pending remediation being completed.

It is recognised that sometimes the remediation of a relationship may be protracted; however, the Authority would not expect remediation issues outstanding from the previous annual review to remain outstanding at the start of the next review unless there were exceptional circumstances, and this course of action was agreed by senior management.

An annual review should be scheduled within a year of the start date of the previous review, not the date the previous review was signed off. Section 5.3.1 below details the minimum information that the Authority would expect to see recorded during an independent review of a higher risk customer.

5.3.1 Customer Reviews – areas to consider

The below is not designed to be a template for completion, however, are the suggested areas a bank should consider and document when conducting such a review.

Account Name			
Account Number(s)			
Connected Accounts			
Date of Review		Previous review	
Relationship Manager			
Reviewer			
Risk rating at start of review			
Reason for risk rating			

Background/nature of customer

Include details of:

- Brief background of customer, occupation, residency etc.
- Number of accounts (and balances)
- Connected parties (where applicable)
- Purpose of account
- Source of funds/wealth
- Any adverse media checks

Additional information for corporate/trust/foundation accounts

- Nature of business
- Key parties to this account – including details of the UBO
- Area of trade/counterparties
- Any connected accounts (e.g. same UBO)
- Structure (including ownership, control and rationale)
- Any adverse media checks

CDD review

Commentary on CDD and EDD held (including that for connected parties where appropriate), including confirmation that the CDD and EDD remains up to date and appropriate. Any concessions used – e.g. eligible introducer

Activity review

Commentary on the actual/anticipated activity through the account (s) (payments/turnover/currencies/counterparties) and comparison to expectations, given knowledge of customer and expected nature of business/source of funds/source of wealth.

Transaction review

Brief commentary on turnover through account within the last 12 months and whether the value and volume of these transactions is in line with expectations given knowledge of customer and expected nature of business/source of funds/source of wealth.

Ensure appropriate action is taken in relation to the occurrence of any unusual or suspicious activity – see section 3.1 of this document for further details.

Other information

Any additional searches undertaken as part of this review e.g. sanctions, PEPs, internal databases, adverse media, online searches etc.

Note: Where screening of certain information (e.g. for sanctions and PEPs) is conducted automatically (e.g. daily or weekly) then additional manual screening is not necessarily required at annual review.

Any other relevant information e.g. changes expected within the next 12 months.

Customer risk assessment

Details of considerations of the customer risk and any appropriate changes. Include any new risks identified and any actions to address these risks, e.g. obtaining additional EDD, consideration as to whether the relationship is still within the bank's risk appetite, SAR submission, increasing the frequency of reviews, undertaking enhanced transaction monitoring, restricting activity etc.

Actions to be taken

Detail the proposed course of actions to be taken, how this will be documented and the timescales in which this action will be completed.

Reviewer confirmations

The reviewer should be confirming that: • A full independent review has been undertaken of the above customer; • The information stated is accurate, up to date and complete; • The risk rating remains appropriate (or stated otherwise – including rationale if rating has been revised); • Any causes for concern have been addressed and any suspicions have been appropriately reported.			
Date review complete		Next review diarised	
Bank's sign off /approval process			

6 Case Studies

The case studies below are real life examples of risks that have crystallised causing losses and/or sanctions (civil and criminal) against banks. The majority of these examples are from case studies provided by FIUs of other jurisdictions, namely FINTRAC (Canada) and AUSTRAC (Australia).

6.1 Fraud related money laundering

FINTRAC received one suspicious transaction report ("STR") from a bank, which generated a case involving ten individuals and twelve businesses, located in the greater Toronto area, suspected of possible fraudulent and money laundering activities. An additional 22 STRs, provided by the same bank and two others, as well as one money transmission business, further contributed to this case.

FINTRAC's analysis revealed that most businesses in this case appeared to be involved in the employment service industry and the associated individuals/officers conducted multiple cash deposits. Employees of the businesses were also paid in cash. These transactions were found to be unusual since the employment service industry is not typically cash driven.

The businesses were linked through common directors/officers, financial transactions, and shared addresses/phone numbers. The individuals involved were also linked through similar addresses and joint signing authorities for various bank accounts.

One individual was the subject of a previous disclosure to law enforcement regarding fraud/extortion activities and was suspected to have links to Eastern European organized crime.

Higher risk indicators associated with this case:

- Individuals made cash deposits (in $100 and $50 denominations) into the personal accounts of multiple associates who then issued cheques payable to other individuals (i.e. use of pass through accounts).
- Numerous businesses paid their employees in cash and reporting entities indicated in the STR that this was not consistent with typical business operations.
- Cheques were deposited into business accounts then immediately withdrawn in cash or through the issuance of cheques payable "to cash" or payable to the individual making the initial deposit.
- Reporting entities also reported excessive cash flow in the business accounts.

The transactions conducted in this case were mostly representative of the placement and layering stages of money laundering. The relevant designated information was disclosed to four different law enforcement agencies.

6.2 Drug related money laundering

FINTRAC received information from law enforcement regarding a number of individuals and businesses, located in the greater Vancouver area, under investigation for suspected involvement in the importation of drugs to Canada from an Asian country.

FINTRAC's analysis revealed financial transactions associated to five of the individuals and three money service businesses that were mentioned in the information provided by law enforcement. FINTRAC suspected that six additional individuals and five businesses specializing in telecommunications, construction, foreign exchange and interior renovation were also involved in the scheme.

Thirty-five STRs reported to FINTRAC by multiple branches of four different banks and three different credit unions were instrumental in allowing FINTRAC to find connections between the various players in this scheme, as well as identifying ones that may not have been previously known to law enforcement.

Higher risk indicators associated with this case:

- Large cash deposits (in CAD and USD) into personal accounts were sometimes followed by the purchase of bank drafts payable to trust companies or money services/currency exchange businesses.
- Domestic wire transfers between personal accounts were followed by the purchase of bank drafts payable to trust companies.
- Bank drafts and cheques issued from other financial institutions were deposited into personal and business accounts and were sometimes followed by an electronic transfer to a Middle Eastern country.
- Electronic transfers were also received from the same Middle Eastern country.
- Multiple transactions were carried out on the same day at the same branch but with different tellers, hours apart.
- Some cash deposits were structured to keep amounts under the reporting threshold and/or conducted at different branches.
- Cash, cheques and bank drafts were deposited by third parties into the business accounts of money service businesses and domestic wires were received into the same accounts; they were immediately followed by withdrawals to purchase bank drafts payable to other money service businesses which then sent electronic transfers to various beneficiaries in foreign countries.
- The same money service businesses receiving deposits or wires also directly sent electronic transfers to beneficiaries in foreign countries.

Individuals and entities involved in this case appear to have conducted a number of suspicious activities mostly representative of the placement and layering stages of money laundering in addition to furthering their drug trafficking activities. FINTRAC disclosed all relevant designated information to law enforcement to assist them in their investigation.

6.3 Terrorist financing

FINTRAC received information from law enforcement and intelligence agencies regarding a non-profit organisation ("NPO"), located in the greater Toronto area, which was suspected of acting as a front for a terrorist organisation. The NPO and associated individuals were suspected of facilitating the acquisition and aggregation of financial resources in Canada, as well as the transmission of resources ultimately for the benefit of the terrorist organization's operations overseas.

The NPO was the subject of several FINTRAC disclosures to law enforcement and intelligence agencies between 2002 and 2007. STRs, from financial institutions were instrumental in assisting FINTRAC in its analysis.

Higher risk indicators associated with this case:

- The NPO ordered many electronic transfers to the benefit of individuals and entities (including a foreign NPO also suspected of being a front for the terrorist organization) located overseas. The transfers were ordered primarily through major financial institutions rather than through domestic money service businesses.
- Various officers of the NPO made large cash deposits to the various accounts of the suspect NPO, held at multiple financial institutions, for which the source of funds was unknown.
- An individual also attempted to deposit a number of cheques, made payable to third parties, to the account of the suspect NPO
- Multiple, recurrent electronic credits were made to the accounts of the suspect NPO for which the original source of funds and remitters' identity were unknown.
- The deposit of cash and monetary instruments (cheques, bank drafts etc.) to the account of the suspect NPO, were often followed by the purchase of bank drafts or offshore movement of funds FINTRAC disclosed all relevant designated information to law enforcement and intelligence agencies to assist them in their investigation.