ANTI-MONEY LAUNDERING AND PREVENTION OF TERRORIST FINANCING REGULATIONS

ARRANGEMENT OF REGULATIONS

PART I

PRELIMINARY PROVISIONS AND INTERPRETATION

PART II

CUSTOMER DUE DILIGENCE

PART III

POLICIES, SYSTEMS AND CONTROLS, RECORD KEEPING AND TRAINING

PART IV

COMPLIANCE AND DISCLOSURES

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

PART V

DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSION

PART VI

MISCELLANEOUS

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

ANTI-MONEY LAUNDERING AND PREVENTION OF TERRORIST FINANCING REGULATIONS – SECTION 177(2)

(Legal Notices 14/2010, 36/2011, 11/2013 and 57/2013)

Commencement

[29 July 2010]

PART I

PRELIMINARY PROVISIONS AND INTERPRETATION

Short title

1. These Regulations may be cited as the Anti-Money Laundering and Prevention of Terrorist Financing Regulations.

Interpretation

2. (1) In these Regulations—

"Anti-Money Laundering Committee" means the Anti-Money Laundering Committee under the Ordinance;

"bank" means a person that carries on banking business within the meaning of the Banking Ordinance, whether or not that business is carried on in, or from within, the Islands;

"beneficial owner" has the meaning specified in regulation 3;

"branch" includes a representative or contact office;

"business relationship" means a business, professional or commercial relationship between a financial business and a customer which is expected by the financial business, at the time when contact is established, to have an element of duration;

"cash" means—

(a) notes and coins;

(b) postal orders; or

(c) travellers' cheques,

in any currency;

"Code" means an Anti-Money Laundering and Prevention of Terrorist Financing Code issued under section 118 of the Ordinance and, in relation to a financial business, means a Code that applies to the financial business;

"Commission" means the Financial Services Commission established under the Financial Services Commission Ordinance 2001 and continued under the Financial Services Commission Ordinance 2007;

"correspondent banking relationship" has the meaning specified in regulation 7(1);

"customer due diligence measures" has the meaning specified in regulation 5;

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

"designated non-financial business and profession" means a financial business that is not a regulated financial business; *(Inserted by L.N. 57/2013)*

"DNFBP Register" means the register of non-regulated financial businesses established and kept under regulation 24;

"DNFBP Supervisor" means the person or body prescribed as the supervisory authority for designated non-financial businesses and professions; *(L.N. 57/2013)*

"enhanced customer due diligence measures" has the meaning specified in regulation 13(1);

"enhanced ongoing monitoring" has the meaning specified in regulation 13(1);

"FATF" means the international body known as the Financial Action Task Force on Money Laundering;

"FATF Recommendations" means—

(a) the Forty Recommendations; and

(b) the Nine Special Recommendations,

issued by the FATF, incorporating the amendments made on 22 October 2004 and such other amendments as may from time-to-time be made;

"financial business" has the meaning specified in Schedule 2;

"foreign regulated person" has the meaning specified in regulation 8;

"foreign regulatory authority", means an authority in a jurisdiction outside the Islands which exercises in that jurisdiction supervisory functions substantially corresponding to those of the Commission or the supervisory authority for designated non-financial businesses and professions, with respect to enforcing compliance with the Ordinance, these Regulations and the Codes;

"high value dealer" means a person who, by way of business, trades in goods, precious metals or precious stones, when he receives, in respect of any transaction, whether the transaction is executed in a single operation or in several linked operations, a payment or payments in cash of—

(a) in the case of precious metals or precious stones, at least $15,000, or the equivalent in another currency;

(b) in the case of any other goods, at least $50,000, or the equivalent in another currency;

"identification information" has, in relation to a financial business, the meaning specified in the relevant Code;

"independent legal professional" means a firm or sole practitioner who, by way of business, provides legal or notarial services to other persons, when preparing for or carrying out transactions for a customer in relation to—

(a) the buying and selling of real estate and business entities;

(b) the managing of client money;

(c) the opening or management of bank, savings or securities accounts;

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(d) the organisation of contributions necessary for the creation, operation or management of companies; or

(e) the creation, operation or management of trusts, companies or similar structures, excluding any activity that requires a licence under the Trustees Licensing Ordinance or the Company Management (Licensing) Ordinance;

"intermediary" means a person who has or seeks to establish a business relationship or to carry out an occasional transaction on behalf of his customer with a financial business, so that the intermediary becomes a customer of the financial business;

"introducer" means a person who has a business relationship with a customer and who introduces that customer to a financial business with the intention that the customer will form a business relationship or conduct an occasional transaction with the financial business so that the introducer's customer also becomes a customer of the financial business;

"money laundering compliance officer" means the person appointed by a financial business as its compliance officer under regulation 21;

"money laundering disclosure" means a disclosure under section 124, 125 or 126 of the Ordinance;

"Money Laundering Reporting Officer" or "MLRO" means the person appointed by a financial business under regulation 22;

"occasional transaction" has the meaning specified in regulation 4;

"ongoing monitoring" has the meaning specified in regulation 5(5);

"Ordinance" means the Proceeds of Crime Ordinance;

"politically exposed person" has the meaning specified in regulation 6;

"recognised exchange" has the meaning specified in paragraph (4);

"regulated business" means a business for which a regulatory licence is required;

"regulated person" means a person who holds a regulatory licence;

"regulatory licence" means a licence specified in Schedule 1;

"relevant business" means a business which, if carried on by a person, would result in that person being a financial business;

"shell bank" has the meaning specified in regulation 7(3);

"sole trader" means an individual carrying on a relevant business who does not in the course of doing so—

(a) employ any other person; or

(b) act in association with any other person;

"supervisory authority" means—

(a) in the case of a regulated financial business, the Commission; and

(b) in the case of a designated non-financial business and profession, the DNFBP Supervisor;

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

"Terrorism (UN) Order" means the Terrorism (United Nations Measures) (Overseas Territories) Order 2001;

"terrorist financing disclosure" means a disclosure under—

(a) article 10 or Part 1 of Schedule 1 of the Anti-terrorist Financing Order;

(b) article 8 of the Terrorism (UN) Order; or

(c) article 10 of the Al-Qa'ida and Taliban (United Nations Measures) (Overseas Territories) Order 2002; and

"third party" means a person for whom a customer is acting.

(2) Words and expressions defined in the Ordinance have the same meaning in these Regulations.

(3) In these Regulations, unless the context otherwise requires, "customer" includes a prospective customer.

(4) Subject to subregulation (5), "recognised exchange" means—

(a) an exchange that is a member of the World Federation of Exchanges; or

(b) such other exchange as may be recognised by the Commission by notice published in the *Gazette.*

(5) An exchange is not a recognised exchange within the meaning of paragraph (4) if it is situated in a country specified by the Commission, by notice published in the *Gazette*, as a country that does not implement, or does not effectively apply, the FATF Recommendations

Meaning of "beneficial owner"

3. (1) Subject to subregulation (3), each of the following is a beneficial owner of a legal person, a partnership or an arrangement—

(a) an individual who is an ultimate beneficial owner of the legal person, partnership or arrangement, whether or not the individual is the only beneficial owner; and

(b) an individual who exercises ultimate control over the management of the legal person, partnership or arrangement, whether alone or jointly with any other person or persons.

(2) For the purposes of subregulation (1), it is immaterial whether an individual's ultimate ownership or control of a legal person, partnership or arrangement is direct or indirect.

(3) An individual is deemed not be the beneficial owner of a body corporate, the securities of which are listed on a recognised exchange.

(4) In this regulation, an "arrangement" includes a trust.

Meaning of "occasional transaction"

4. (1) A transaction is an occasional transaction if the transaction is carried out otherwise than as part of a business relationship, and is carried out as—

(a) a single transaction that amounts to the sum specified in subregulation (2), or more; or

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(b) two or more linked transactions that, in total amount to the sum specified in subregulation (2), or more, where—

(i) it appears at the outset to any person handling any of the transactions that the transactions are linked; or

(ii) at any later stage it comes to the attention of any person handling any of those transactions that the transactions are linked.

(2) The amount specified for the purposes of subregulation (1) is—

(a) in the case of a wire transfer transaction, or linked transactions, $1,000; or *(Amended by L.N. 36/2011)*

(b) in the case of any other transaction, or linked transactions, $15,000.

Meaning of "customer due diligence measures" and "ongoing monitoring"

5. (1) "Customer due diligence measures" are measures for—

(a) identifying a customer;

(b) determining whether the customer is acting for a third party and, if so, identifying the third party;

(c) verifying the identity of the customer and any third party for whom the customer is acting;

(d) identifying the identity of each beneficial owner of the customer and third party, where either the customer or third party, or both, are not individuals;

(e) determining who are the natural persons that ultimately own or control the customer that is not an individual; *(Inserted by L.N. 36/2011)*

(f) taking reasonable measures, on a risk-sensitive basis, to verify the identity of each beneficial owner of the customer and third party so that the financial business is satisfied that it knows who each beneficial owner is including, in the case of a legal person, partnership, trust or similar arrangement, taking reasonable measures to understand the ownership and control structure of the legal person, partnership, trust or similar arrangement; and

(g) obtaining information on the purpose and intended nature of the business relationship or occasional transaction.

(2) Customer due diligence measures include—

(a) where the customer is not an individual, measures for verifying that any person purporting to act on behalf of the customer is authorised to do so, identifying that person and verifying the identity of that person; and

(b) where the customer is not an individual, measures for determining who are the natural persons that ultimately own or control the customer; *(Inserted by L.N. 36/2011)*

(c) where the financial business carries on insurance business, measures for identifying each beneficiary under any long term or investment linked policy issued or to be issued by the financial business and verifying the identity of each beneficiary.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(3) Customer due diligence measures do not fall within this regulation unless they provide for verifying the identity of persons whose identity is required to be verified, on the basis of documents, data or information obtained from a reliable and independent source.

(4) Where customer due diligence measures are required by this regulation to include measures for identifying and verifying the identity of the beneficial owners of a person, those measures are not required to provide for the identification and verification of any individual who holds shares in a company that is listed on a recognised exchange.

(5) "Ongoing monitoring" of a business relationship means—

(a) scrutinising transactions undertaken throughout the course of the relationship, including where necessary the source of funds, to ensure that the transactions are consistent with the financial business's knowledge of the customer and his business and risk profile; and

(b) keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up-to-date and relevant by undertaking reviews of existing records.

Meaning of "politically exposed person"

6. (1) "Politically exposed person" means a person who is—

(a) an individual who is, or has been, entrusted with a prominent public function by—

(i) a country, including the Islands; or

(ii) an international body or organization;

(b) an immediate family member of a person referred to in paragraph *(a)*; or

(c) a known close associate of a person referred to in paragraph *(a)*.

(2) Without limiting subregulation (1)*(a)*, the following are politically exposed persons within the meaning of that paragraph—

(a) heads of state, heads of government and senior politicians;

(b) senior government or judicial officials;

(c) high-ranking officers in the armed forces;

(d) members of courts of auditors or of the boards of central banks;

(e) ambassadors and chargés d'affaires;

(f) senior executives of state-owned corporations; and

(g) important political party officials.

(3) Without limiting subregulation (1)*(b)*, the following are immediate family members of a person specified in subregulation (1)*(a)*—

(a) a spouse;

(b) a partner, that is an individual considered by his or her national law as equivalent to a spouse;

(c) children and their spouses or partners, as defined in paragraph *(b)*;

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(d) parents;

(e) grandparents and grandchildren; and

(f) siblings.

(4) Without limiting subregulation (1)*(c)*, the following are close associates of a person specified in subregulation (1)*(a)*—

(a) any person known to maintain a close business relationship with that person or to be in a position to conduct substantial financial transactions on behalf of the person;

(b) any person who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with that person; and

(c) any person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of that person.

(5) For the purposes of deciding whether a person is a close associate of a person referred to in subregulation (1)*(a)*, a financial business need only have regard to information which is in that person's possession or is publicly known.

Meaning of "shell bank" and "correspondent banking"

7. (1) "Correspondent banking" means the provision of banking services by one bank, (the "correspondent bank") to another bank (the "respondent bank").

(2) Without limiting subregulation (1), banking services includes—

(a) cash management, including establishing interest-bearing accounts in different currencies;

(b) international wire transfers of funds;

(c) cheque clearing;

(d) payable-through accounts; and

(e) foreign exchange services.

(3) A "shell bank" is a bank that—

(a) is incorporated and licensed in a country in which it has no physical presence involving meaningful decision-making and management; and

(b) is not subject to supervision by the Commission or a foreign regulatory authority, by reason of its membership of, or affiliation to, a group that is subject to effective consolidated supervision.

Meaning of "foreign regulated person"

8. (1) "Foreign regulated person" means a person—

(a) that is incorporated in, or if it is not a corporate body, has its principal place of business in, a jurisdiction outside the Islands (its "home jurisdiction");

(b) that carries on business outside the Islands that, if carried on in the Islands, would require a regulatory licence;

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(c) that, in respect of the business referred to in paragraph *(b)*—

(i) is subject to legal requirements in its home jurisdiction for the prevention of money laundering and terrorist financing that are consistent with the requirements of the FATF Recommendations, for the time being issued, for that business; and

(ii) is subject to effective supervision for compliance with those legal requirements by a foreign regulatory authority.

(2) For the purposes of the definition of "foreign regulated person", the Code may specify jurisdictions that may be regarded as having legal requirements for the prevention of money laundering that are consistent with the requirements of the FATF Recommendations.

Scope of Regulations

9. These Regulations apply to all financial businesses.

Application of Regulations outside the Islands

10. (1) Subject to subregulations (2), (3) and (4), a relevant financial business that has a branch located in, or a subsidiary incorporated in, a country outside the Islands shall, to the extent that the laws of that country permit—

(a) comply with these Regulations and the Code in respect of any business carried on through the branch; and

(b) ensure that these Regulations and the Code are complied with by the subsidiary with respect to any business that it carries on.

(2) A relevant financial business shall have particular regard to ensure that paragraph (1) is complied with where the country in which its branch or subsidiary is situated does not apply, or insufficiently applies, the FATF Recommendations.

(3) If the country in which a branch or subsidiary of a financial business is situated has more stringent standards with respect to the prevention of money laundering and terrorist financing than are provided for in these Regulations and the Code, the relevant financial business shall ensure that the more stringent requirements are complied with by its branch or subsidiary.

(4) Where the laws of a country outside the Islands do not permit a branch or subsidiary of a financial business to comply with subregulation (1), the relevant financial business shall—

(a) notify the Commission in writing; and

(b) to the extent that the laws of the foreign country permit, apply alternative measures to ensure compliance with the FATF Recommendations and to deal effectively with the risk of money laundering and terrorist financing.

(5) For the purposes of this regulation, "relevant financial business" means a financial business—

(a) that is a regulated financial business; and

(b) that is—

(i) a company incorporated in the Islands;

(ii) a partnership based in the Islands;

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(iii) an individual resident in the Islands; or

(iv) any other person having its principal or head office in the Islands.

PART II

CUSTOMER DUE DILIGENCE

Application of customer due diligence measures and ongoing monitoring

11. (1) Subject to subregulations (5) and (6), a financial business shall apply customer due diligence measures—

(a) before the financial business establishes a business relationship or carries out an occasional transaction;

(b) where the financial business—

(i) suspects money laundering or terrorist financing; or

(ii) doubts the veracity or adequacy of documents, data or information previously obtained under its customer due diligence measures or when conducting ongoing monitoring; and

(c) at other appropriate times to existing customers as determined on a risk-sensitive basis.

(2) Without limiting subregulations (1)*(b)*(ii) and (1)*(c)*, a financial business shall obtain identification information when there is a change in the—

(a) identification information of a customer;

(b) beneficial ownership of a customer; or

(c) third parties, or the beneficial ownership of third parties.

(3) A financial business shall conduct ongoing monitoring of a business relationship.

(4) In applying customer due diligence measures and conducting ongoing monitoring, a financial business shall—

(a) assess the risk that any business relationship or occasional transaction involves, or will involve, money laundering or terrorist financing, depending upon the type of customer, business relationship, product or transaction;

(b) be able to demonstrate to the supervisory authority—

(i) that the extent of the customer due diligence measures applied in any case is appropriate having regard to the circumstances of the case, including the risks of money laundering and terrorist financing; and

(ii) that it has obtained appropriate information to carry out the risk assessment required under paragraph *(a)*.

(5) A financial business may complete the verification of the identity of a customer, third party or beneficial owner after the establishment of a business relationship if—

(a) it is necessary not to interrupt the normal conduct of business;

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(b) there is little risk of money laundering or terrorist financing occurring as a result; and

(c) verification of identity is completed as soon as reasonably practicable after the contact with the customer is first established.

(6) The verification of the identity of a bank account holder may take place after the bank account has been opened provided that there are adequate safeguards in place to ensure that, before verification has been completed—

(a) the account is not closed; and

(b) transactions are not carried out by or on behalf of the account holder, including any payment from the account to the account holder.

(7) A financial business that contravenes this regulation commits an offence and is liable on summary conviction, to a fine of $50,000.

Requirement to cease transaction or terminate relationship

12. (1) If a financial business is unable to apply customer due diligence measures before the establishment of a business relationship or before the carrying out of an occasional transaction in accordance with these Regulations, the financial business shall not establish the business relationship or carry out the occasional transaction.

(2) If regulation 11(5) or (6) apply and a financial business is unable to complete the verification of the identity of a customer, third party or beneficial owner after the establishment of a business relationship, the financial business shall terminate the business relationship with the customer.

(3) If a financial business is unable to undertake ongoing monitoring with respect to a business relationship, the financial business shall terminate the business relationship.

(4) If subregulation (1), (2) or (3) applies with respect to a financial business, the financial business shall consider whether he is required to make a money laundering disclosure or a terrorist financing disclosure.

(5) Subregulations (1), (2) and (3) do not apply where the financial business is a lawyer and is in the course of ascertaining the legal position for that person's client or performing the task of defending or representing the client in, or concerning, legal proceedings, including advice on the institution or avoidance of proceedings.

(6) If the financial business has made a money laundering or terrorist financing disclosure, subregulations (1), (2) and (3) do not apply to the extent that the financial business is acting—

(a) in the case of a money laundering disclosure, with the consent or deemed consent of the Anti-Money Laundering Committee; or

(b) in the case of a terrorist financing disclosure made under the Anti-terrorist Financing Order, with the consent of a constable, where such consent may lawfully be given.

(7) A financial business who contravenes this regulation commits an offence and is liable on summary conviction to a fine of $50,000.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

Enhanced customer due diligence and ongoing monitoring

13. (1) For the purposes of these Regulations, "enhanced customer due diligence measures" and "enhanced ongoing monitoring" mean customer due diligence measures, or ongoing monitoring, that involve specific and adequate measures to compensate for the higher risk of money laundering or terrorist financing.

(2) A financial business shall, on a risk-sensitive basis, apply enhanced due diligence measures and undertake enhanced ongoing monitoring—

(a) where the customer has not been physically present for identification purposes;

(b) where the financial business has, or proposes to have, a business relationship with, or proposes to carry out an occasional transaction with, a person connected with a country that does not apply, or insufficiently applies, the FATF recommendations;

(c) where the financial business is a bank which holds a National Banking licence granted under the Banking Ordinance that has or proposes to have a banking or similar relationship with an institution whose address for that purpose is outside the Islands;

(d) where the financial business has or proposes to have a business relationship with, or to carry out an occasional transaction with, a politically exposed person;

(e) where any of the following is a politically exposed person—

(i) a beneficial owner of the customer;

(ii) a third party for whom a customer is acting;

(iii) a beneficial owner of a third party described in subparagraph (ii);

(iv) a person acting, or purporting to act, on behalf of the customer.

(f) in any other situation which by its nature can present a higher risk of money laundering or terrorist financing.

(3) A financial business who contravenes this regulation commits an offence and is liable on summary conviction, to a fine of $50,000.

Reliance on introducers and intermediaries

14. (1) Subject to this regulation and any requirements in the Code, a financial business may rely on an introducer or an intermediary to apply customer due diligence measures with respect to a customer, third party or beneficial owner, if—

(a) the introducer or intermediary is a regulated person or a foreign regulated person; and

(b) the introducer or intermediary consents to being relied on.

(2) Before relying on an introducer or intermediary to apply customer due diligence measures with respect to a customer, third party or beneficial owner, a financial business shall immediately obtain adequate assurance in writing from the intermediary or introducer that—

(a) the intermediary or introducer has applied the customer due diligence measures for which the financial business intends to rely on it;

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(b) the intermediary or introducer is required to keep, and does keep, a record of the evidence of identification relating to each of the customers of the intermediary or introducer;

(c) the intermediary or introducer will, without delay, provide the information in that record to the financial business at the financial business's request; and

(d) the intermediary or introducer will, without delay, provide the information in the record for provision to the Commission, where requested by the Commission. *(Amended by L.N. 36/2011)*

(3) Where a financial business relies on an introducer or intermediary to apply customer due diligence measures, the financial business remains liable for any failure to apply those measures.

(4) This regulation does not prevent a financial business from applying customer due diligence measures by means of an outsourcing financial business or agent provided that the financial business remains liable for any failure to apply such measures.

Simplified due diligence requirements

15. (1) A financial business is not required to apply customer due diligence measures before establishing a business relationship or carrying out an occasional transaction where—

(a) the business has reasonable grounds for believing that the customer is—

(i) a regulated person;

(ii) a foreign regulated person;

(iii) a public authority in the Islands; or

(iv) a body corporate, the securities of which are listed on a recognised exchange; or

(b) in the case of life insurance business, the product is a life insurance contract where the annual premium is no more than $500 or where a single premium of no more than $2,000 is paid.

(2) Subregulation (1)*(a)* does not apply with respect to any third party for whom the customer may be acting or with respect to the beneficial owners of such a third party.

(3) Subregulation (1) does not apply if—

(a) the financial business suspects money laundering or terrorist financing; or

(b) the customer is located, or resides, in a country that does not apply, or insufficiently applies, the FATF recommendations.

Shell banks and anonymous and numbered accounts

16. (1) A financial business —

(a) shall not enter into or continue a correspondent banking relationship with a shell bank;

(b) shall take appropriate measures to ensure that it does not enter into, or continue, a correspondent banking relationship with a financial business in a

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

foreign country that is known to permit its accounts to be used by a shell bank.

(Inserted by L.N. 36/2011)

(2) A financial business shall not set up or maintain a numbered account, an anonymous account or an account in a name which it knows, or has reasonable grounds to suspect, is fictitious.

(3) A financial business that contravenes paragraph (1) or (2) commits an offence and is liable on summary conviction to a fine of $100,000. *(Inserted by L.N. 36/2011)*

PART III

POLICIES, SYSTEMS AND CONTROLS, RECORD KEEPING AND TRAINING

Policies, systems and controls to prevent and detect money laundering and terrorist financing

17. (1) Subject to subregulation (5), a financial business shall establish, maintain and implement appropriate risk-sensitive policies, systems and controls to prevent and detect money laundering and terrorist financing, including policies, systems and controls relating to—

(a) customer due diligence measures and ongoing monitoring;

(b) the reporting of disclosures;

(c) record-keeping;

(d) the screening of employees;

(e) internal controls;

(f) risk assessment and management;

(g) the monitoring and management of compliance with, and the internal communication of, its policies, systems and controls to prevent and detect money laundering and terrorist financing, including those specified in paragraphs *(a)* to *(f)*.

(2) The policies, systems and controls referred to in subregulation (1) must include policies, systems and controls which provide for—

(a) the identification and scrutiny of—

(i) complex or unusually large transactions;

(ii) unusual patterns of transactions which have no apparent economic or visible lawful purpose; and

(iii) any other activity which the financial business regards as particularly likely by its nature to be related to the risk of money laundering or terrorist financing;

(b) the taking of additional measures, where appropriate, to prevent the use for money laundering or terrorist financing of products and transactions which are susceptible to anonymity;

(c) determining whether—

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(i) a customer, any third party for whom the customer is acting and any beneficial owner of the customer or third party, is a politically exposed person;

(ii) a business relationship or transaction, or proposed business relationship or transaction, is with a person connected with a country that does not apply, or insufficiently applies, the FATF Recommendations; or

(iii) a business relationship or transaction, or proposed business relationship or transaction, is with a person connected with a country that is subject to measures for purposes connected with the prevention and detection of money laundering or terrorist financing, imposed by one or more countries or sanctioned by the European Union or the United Nations.

(3) A financial business with any subsidiary or branch that carries on a relevant business shall communicate to that subsidiary or branch, whether in or outside the Islands, the financial business's policies and procedures maintained in accordance with this regulation.

(4) A financial business shall maintain adequate procedures for monitoring and testing the effectiveness of—

(a) the policies and procedures maintained under this regulation; and

(b) the training provided under regulation 20.

(5) A sole trader is not required to maintain policies and procedures relating to internal reporting, screening of employees and the internal communication of such policies and procedures.

(6) For the purposes of this regulation—

(a) "scrutiny" includes scrutinising the background and purpose of transactions and activities; and

(b) "transaction" means any of the following—

(i) an occasional transaction;

(ii) a transaction within an occasional transaction; or

(iii) a transaction undertaken within a business relationship.

(7) A financial business that contravenes this regulation commits an offence and is liable on summary conviction, to a fine of $50,000.

Records required to be kept

18. (1) Subject to subregulation (4), a financial business shall keep the records specified in subregulation (2) and such additional records as may be specified in the Code—

(a) in a form that enables them to be made available on a timely basis, when lawfully required, to the Commission or law enforcement authorities in the Islands; and

(b) for at least the period specified in regulation 19.

(2) The records specified for the purposes of subregulation (1) are—

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(a) a copy of the evidence of identity obtained pursuant to the application of customer due diligence measures or ongoing monitoring, or information that enables a copy of such evidence to be obtained;

(b) the supporting documents, data or information that have been obtained in respect of a business relationship or occasional transaction which is the subject of customer due diligence measures or ongoing monitoring;

(c) a record containing details relating to each transaction carried out by the financial business in the course of any business relationship or occasional transaction;

(d) all account files; and

(e) all business correspondence relating to a business relationship or an occasional transaction.

(3) The record to which subregulation (2)*(c)* refers must include sufficient information to enable the reconstruction of individual transactions.

(4) A financial business who is relied on by another person in accordance with these regulations shall keep the records specified in subregulation (2)*(a)* for the period of five years beginning on the date on which he is relied on in relation to any business relationship or occasional transaction.

(5) Where the financial business (the "first person") is an introducer or intermediary and has given the assurance that is required under regulation 14(2) to another financial business (the "second person"), the first person shall make available to the second person, at the second person's request, a copy of the evidence of identification that the first person is required to keep under this regulation, such evidence being the evidence that is referred to in regulation 14(2).

(6) Subregulation (4) and (5) do not apply where a financial business applies customer due diligence measures by means of an outsourcing financial business or agent.

(7) For the purposes of this regulation, a person relies on another person where he does so in accordance with regulation 14.

(8) A financial business who contravenes this regulation commits an offence and is liable on summary conviction, to a fine of $50,000.

Period for which records must be kept

19. (1) Subject to subregulation (2), the period specified for the purposes of regulation 18 is five years beginning on—

(a) in the case of the records specified in regulation 18(2)*(a)*, the date on which—

(i) the occasional transaction is completed; or

(ii) the business relationship ends; or

(b) in the case of the records specified in subregulation 18(2)*(b)*—

(i) where the records relate to a particular transaction, the date on which the transaction is completed;

(ii) for all other records, the date on which the business relationship ends.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(2) The Commission or the Anti-Money Laundering Committee may, by written notice, specify a period longer than five years for the purposes of regulation 18, and such longer period as is specified in the notice shall apply instead of the period of five years specified in subregulation (1).

Training

20. (1) A financial business shall take appropriate measures for the purposes of making employees whose duties relate to the provision of relevant business aware of—

(a) the anti-money laundering and counter-terrorist financing policies, procedures, systems and controls maintained by the financial business in accordance with these Regulations or the Code;

(b) the law of the Islands relating to money laundering and terrorist financing offences; and

(c) these Regulations, the Code and any Guidance issued by the Commission or a supervisory authority.

(2) A financial business shall provide employees specified in subregulation (1) with training in the recognition and handling of—

(a) transactions carried out by or on behalf of any person who is or appears to be engaged in money laundering or terrorist financing; and

(b) other conduct that indicates that a person is or appears to be engaged in money laundering or terrorist financing.

(3) For the purposes of subregulation (2), training shall include the provision of information on current money laundering techniques, methods, trends and typologies.

(4) A financial business that contravenes this regulation commits an offence and is liable on summary conviction, to a fine of $50,000.

PART IV

COMPLIANCE AND DISCLOSURES

Money laundering compliance officer

21. (1) Subject to subregulation (8), a financial business, other than a sole trader, shall appoint an individual approved by the relevant supervisory authority as its money laundering compliance officer in respect of the relevant business being carried on by the financial business.

(2) A sole trader is the money laundering compliance officer in respect of his or her relevant business.

(3) A financial business shall ensure that—

(a) the individual appointed as money laundering compliance officer under this regulation is of an appropriate level of seniority; and

(b) the compliance officer has timely access to all records that are necessary or expedient for the purpose of performing his or her functions as money laundering compliance officer.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(4) The principal function of the money laundering compliance officer is to oversee and monitor the financial business' compliance with the Ordinance, all legislation in force concerning terrorist financing, these Regulations and the Code.

(5) When an individual has ceased to be the money laundering compliance officer of a financial business, the financial business shall as soon as practicable appoint another individual approved by the relevant supervisory authority as its money laundering compliance officer.

(6) A financial business shall give the Commission written notice within seven days after the date—

(a) of the appointment of a money laundering compliance officer; or

(b) that an individual ceases, for whatever reason, to be its money laundering compliance officer.

(7) The money laundering compliance officer of a financial business may also be appointed to be its money laundering reporting officer.

(8) The Codes may modify the requirements of this regulation in relation to particular types or category of financial business.

(9) A financial business that contravenes this regulation commits an offence and is liable on summary conviction, to a fine of $25,000.

Money laundering reporting officer

22. (1) Subject to subregulation (6), a financial business, other than a sole trader, shall appoint an individual as its money laundering reporting officer to—

(a) receive and consider internal money laundering and terrorist financing disclosures;

(b) considering whether a suspicious activity report should be made to the Anti-Money Laundering Committee; and

(c) where he considers a suspicious activity report should be made, submitting the report.

(2) A financial business shall ensure that—

(a) the individual appointed as money laundering reporting officer under this regulation is of an appropriate level of seniority; and

(b) the money laundering reporting officer has timely access to all records that are necessary or expedient for the purpose of performing his or her functions.

(3) When an individual has ceased to be the money laundering reporting officer of a financial business, the financial business shall forthwith appoint another individual approved by the relevant supervisory authority as its money laundering reporting officer.

(4) A financial business shall give the Commission written notice within 7 days after the date—

(a) of the appointment of a money laundering reporting officer; or

(b) that an individual ceases, for whatever reason, to be its money laundering reporting officer.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(5) The money laundering reporting officer of a financial business may also be appointed to be its money laundering compliance officer.

(6) The Codes may modify the requirements of this regulation in relation to particular types or category of financial business.

(7) A financial business that contravenes this regulation commits an offence and is liable on summary conviction, to a fine of $25,000.

PART V

DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

Designated supervisory authority

23. The Commission is designated as the sole supervisory authority for a financial business that is not a regulated person for the purposes of section 161(2) of the Ordinance.

Register of designated non-financial businesses and professions

24. (1) The DNFBP Supervisor must establish and keep a register of designated non-financial businesses and professions. *(Amended by L.N. 57/2013)*

(2) There shall be a separate part of the DNFBP Register for each category of designated non-financial business and profession. *(Inserted by L.N. 36/2011 and 57/2013)*

(3) Each part of the DNFBP Register shall contain the following information in respect of each designated non-financial business and profession that has been registered in accordance with regulation 26—

(a) the name, address in the Islands and contact details of the designated non-financial business and profession;

(b) the relevant business for which the designated non-financial business and profession is registered;

(c) the date of registration and, if applicable, de-registration of the designated non-financial business and profession;

(d) such other information as the DNFBP Supervisor considers appropriate.

(Amended by L.N. 36/2011 and L.N. 57/2013)

(4) The DNFBP Register and the information contained in any document filed with the DNFBP Supervisor may be kept in such manner as the DNFBP Supervisor considers appropriate, including either wholly or partly, by means of a device or facility that—

(a) records or stores information magnetically, electronically or by other means; and

(b) permits the information recorded or stored to be inspected and reproduced in legible and usable form.

(Amended by L.N. 57/2013)

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

Application to register

25. (1) A person may apply to the DNFBP Supervisor to be registered as a designated non-financial business and profession in the DNFBP Register. *(Amended by L.N. 57/2013)*

(2) The application must—

(a) be in writing and in the form specified by the DNFBP Supervisor ;

(b) be signed by the applicant or by a person acting on the applicant's behalf;

(c) be accompanied by such documents or information as may be specified on the application form or by the DNFBP Supervisor;

(d) be accompanied by a non-refundable registration fee of $150.
(Amended by L.N. 11 of 2013 and L.N. 57/2013)

(3) The DNFBP Supervisor may require an applicant to—

(a) provide it with such documents and information, in addition to those specified in subregulation (2), as it reasonably requires to determine the application and any such information shall be in such form as the DNFBP Supervisor may require; and

(b) verify any document and information provided in support of an application in such manner as the DNFBP Supervisor may specify.
(Amended by L.N. 57/2013)

(4) If, before the determination by the DNFBP Supervisor of an application—

(a) there is a material change in any information or documentation provided by or on behalf of the applicant to the DNFBP Supervisor in connection with the application; or

(b) the applicant discovers that any such information or documentation is incomplete, inaccurate or misleading;

the applicant shall give the DNFBP Supervisor as soon as possible written particulars of the change or of the incomplete, inaccurate or misleading information or documentation.
(Amended by L.N. 57/2013)

Registration

26. (1) Following the receipt of an application under regulation 25 and any additional documents or information that it has required under regulation 25(3), the DNFBP Supervisor must either—

(a) register the applicant as a designated non-financial business and profession in the DNFBP Register; or

(b) refuse the application under regulation 27.

(2) If the DNFBP Supervisor registers the applicant, it must provide it with written notice of its registration.

(Amended by L.N. 57/2013

Refusal of application

27. (1) The DNFBP Supervisor may refuse an application for registration if—

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(a) the application does not comply with regulation 25;

(b) the applicant fails to provide any information or documents required by the under regulation 25(3); or

(c) the DNFBP Supervisor is of the opinion that—

(i) the applicant does not intend to carry on the relevant business for which it seeks registration;

(ii) the designated non-financial business and profession, or any of its directors, senior officers or owners do not satisfy the DNFBP Supervisor fit and proper criteria; or

(iii) it is contrary to the public interest for the designated non-financial business and profession to be registered.

(2) If the DNFBP Supervisor refuses an application for registration, it must send the applicant a written notice of refusal, stating the grounds for its refusal.

(Amended by L.N. 57/2013

Disciplinary action

28. For the purposes of sections 168 of the Ordinance —

(a) a designated non-financial business and profession that contravenes a provision of these Regulations set out in Columns 1 and 2 of the table in Schedule 3, commits a disciplinary violation; and

(b) the amount specified in Column 3 of the table in Schedule 2 with respect to a disciplinary violation, is the maximum administrative penalty that the DNFBP Supervisor may impose on a designated non-financial business and profession for that disciplinary violation.

(Amended by L.N. 57/2013)

PART VI

MISCELLANEOUS

Directions where FATF applies counter-measures

29. The relevant supervisory authority may direct a financial business—

(a) not to enter into a business relationship;

(b) not to carry out an occasional transaction;

(c) not to proceed any further with a business relationship or occasional transaction;

(d) to impose any prohibition, restriction or limitation relating to a business relationship or occasional transaction; or

(e) to apply enhanced customer due diligence measures to any business relationship or occasional transaction;

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

with any person who is situated or incorporated in a country to which the FATF has decided to apply counter-measures.

Customer information

30. (1) For the purposes of section 140 of the Ordinance, "customer information", in relation to a person ("the specified person") and a regulated person, is information whether the specified person holds, or has held, an account or accounts at the regulated person, whether solely or jointly with another, and, if so, information as to—

(a) the account number or numbers;

(b) the specified person's full name;

(c) where the specified person is an individual, the individual's—

(i) date of birth; and

(ii) most recent address, any previous address, any postal address and any previous postal address;

(d) where the specified person is a company—

(i) the country where the company is incorporated or is otherwise constituted, established or registered;

(ii) the address of the registered office, any previous registered office, any business address, any previous business address, any postal address and any previous postal address;

(e) where the specified person is a partnership or unincorporated body of persons, the information specified in paragraph *(c)* with respect to each individual authorised to operate the account, whether solely or jointly;

(f) such evidence of identity with respect to the specified person as has been obtained by the regulated person;

(g) the date or dates on which the specified person began to hold the account or accounts and, if the specified person has ceased to hold the account or any of the accounts, the date or dates on which the person did so;

(h) the full name of any person who holds, or has held, an account at the regulated person jointly with the specified person;

(i) the account number or numbers of any other account or accounts held at the regulated person to which the specified person is a signatory and details of the person holding the other account or accounts;

(j) the full name and the information contained in paragraph *(c)*, *(d)* or *(e)*, as relevant, of any person who is a signatory to an account specified in subparagraph (i).

Prescribed amounts

31. The following amounts are prescribed for the purposes of the Ordinance—

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(a) application of section 32(1) of the Ordinance (minimum amount remaining to be paid under a confiscation order for discharge), the amount prescribed is $500;

(b) discharge under section 33 of the Ordinance, the amount prescribed is $100;

(c) minimum threshold for the purposes of section 101(1) of the Ordinance, the amount prescribed is $250;

(d) definition of "recoverable cash" under section 113 of the Ordinance, the amount prescribed is $250.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

SCHEDULE 1

(Regulation 2)

REGULATORY LICENCES

"Regulatory licence" means—

(a) a licence issued under the Banking Ordinance;

(b) a licence issued under the Trustees Licensing Ordinance;

(c) a licence issued under the Company Management (Licensing) Ordinance;

(d) a licence issued under the Mutual Funds Ordinance;

(e) a licence issued under the Investment Dealers (Licensing) Ordinance;

(f) a licence issued under the Insurance Ordinance;

(g) a licence issued under the Money Transmitters Ordinance

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

SCHEDULE 2

(Regulation 2)

FINANCIAL BUSINESS

1. The following are "financial businesses" when acting in the course of a business carried on in, or from within, the Islands—

(a) subject to paragraph 2, a person who carries on any kind of regulated business;

(b) a person who carries on money services business as defined in the Money Transmitters Ordinance;

(c) a person who, by way of business, provides any of the following services to third parties—

(i) acting as a secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons or arranging for another person to act in one of the foregoing capacities or as the director of a company;

(ii) providing a business, accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;

(iii) acting as, or arranging for another person to act as, a nominee shareholder for another person;

(d) a person who conducts as a business one or more of the following activities for, or on behalf of, a customer—

(i) lending, including consumer credit, mortgage credit, factoring, with or without recourse, and financing of commercial transactions, including forfeiting;

(ii) financial leasing;

(iii) issuing and managing means of payment, including credit and debit cards, cheques, travellers' cheques, money orders and bankers' drafts and electronic money;

(iv) financial guarantees or commitments;

(v) participation in securities issues and the provision of financial services related to such issues;

(vi) providing advice on capital structure, industrial strategy and related questions and advice and services relating to mergers and the purchase of undertakings;

(vii) safekeeping and administration of cash;

(viii) investing administering or managing funds or money;

(ix) money brokering;

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(e) a person who, as a business, trades for his own account or for the account of customers in—

(i) money market instruments, including cheques, bills, certificates of deposit and derivatives;

(ii) foreign exchange;

(iii) exchange, interest rate and index instruments;

(iv) financial futures and options;

(v) commodities futures; or

(vi) shares and other transferable securities;

(f) a person who, by way of business—

(i) provides accountancy or audit services; or

(ii) acts as a real estate agent;

(g) an independent legal professional;

(h) a high value dealer;

(i) a person who operates a casino by way of business, whenever a transaction involves accepting a total cash payment of $3,000 or more, or the equivalent in another currency.

2. A company that carries on insurance business is a financial business only where it carries on—

(a) long-term insurance business; or

(b) any form of life insurance business or investment related insurance business that may be classified as general insurance business.

3. A person who carries on business as an insurance intermediary is a financial business only where the person acts with respect to any type of business referred to in paragraph 2*(a)* or *(b)*.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

SCHEDULE 3

(Regulation 28)

DISCIPLINARY ACTION

DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

REGULATION	Brief Description of Violation	ADMINISTRATIVE PENALTY ($)
11(1)	Failure to apply required customer due diligence measures	$5,000
12	Failure to comply with requirements in subregulations (2) and (3) concerning business relationship with the customers	$7,500
13 (1)	Failure to apply enhanced due diligence in respect of any relevant requirements in 13(1)*(a)* to *(f)*	$5,000
16 (1) and (2)	Failure to comply with the requirements in subregulation (1) and (2) not to set up or maintain a numbered account, an anonymous account or in a name that is fictitious	$7,500
17	Failure to comply with requirements in subregulations (3) and (4) concerning the maintenance of policies and procedures	$2,500 and $250 for every day the disciplinary violation continues or occurs
18	Failure to comply with the requirements in subregulations (1), (4) and (5) concerning the keeping of records	$2,500 and $250 for every day the disciplinary violation continues or occurs
20	Failure to comply with the requirements in subregulations (1) and (2) concerning the training of employees	$2,500 and $100 for every day the disciplinary violation continues or occurs
21	Failure to comply with the requirements in subregulations (1), (3), (5) and (6) concerning the appointment of a money laundering compliance officer	$2,500 and $100 for every day the disciplinary violation continues or occurs
22	Failure to comply with the requirements in subregulations (1), (2), (3) and 4 concerning the appointment of a money laundering reporting officer	$2,500 and $100 for every day the disciplinary violation continues or occurs

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

ANTI-MONEY LAUNDERING AND PREVENTION OF TERRORIST FINANCING CODE

ARRANGEMENT OF REGULATIONS

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

PART 9

WIRE TRANSFERS

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

ANTI-MONEY LAUNDERING AND PREVENTION OF TERRORIST FINANCING CODE – SECTION 118(1)

(Legal Notice 13/2011)

Commencement

[6 May 2011]

PART 1

PRELIMINARY PROVISIONS AND INTERPRETATION

Short title

1. This Code may be cited as the Anti-Money Laundering and Prevention of Terrorist Financing Code.

Interpretation

2. (1) In this Code—

"AML" means anti-money laundering;

"AML/CFT Regulations" means the Anti-Money Laundering and Prevention of Terrorist Financing Regulations;

"bank" means a bank that holds a licence issued under the Banking Ordinance or a financial business which conducts as a business one or more of the activities specified in paragraph 1*(d)*(i) to (ix) of Schedule 2 to the AML/CFT Regulations;

"board" means—

(a) in relation to a corporate body, the board of directors, committee of management or other governing authority of the corporate body, by whatever name called or, if the corporate body only has one director, that director;

(b) in relation to a partnership, the partners, or in the case of a limited partnership, the general partners; or

(c) in relation to any other organisation or undertaking, the persons fulfilling functions equivalent to the functions of the directors of a company;

"CFT" means combating terrorist financing;

"Code" means this Code;

"director", in relation to a legal entity, means a person appointed to direct the affairs of the legal entity and includes—

(a) a person who is a member of the governing body of the legal entity; and

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(b) a person who, in relation to the legal entity, occupies the position of director, by whatever name called;

"legal entity" includes a company, a foundation, a partnership, whether limited or general, an association or any unincorporated body of persons, but does not include a trust;

"POCO" means the Proceeds of Crime Ordinance;

"TCI" means the Turks and Caicos Islands;

"terrorist financing legislation" means—

(a) the Anti-terrorist Financing Order;

(b) the Terrorism (UN) Order;

(c) the Al-Qa'ida and Taliban (United Nations Measures) (Overseas Territories) Order 2002;

(d) the Counter Terrorism Order 2010; and

(e) any legislation having application in the TCI with respect to terrorist financing.

(2) Any word or phrase defined in POCO or the AML/CFT Regulations has, unless the context otherwise requires, the same meaning in this Code.

Scope of Code

3. This Code applies, to the extent specified, to—

(a) financial businesses within the meaning of the AML/CFT Regulations; and

(b) directors and boards of financial businesses.

PART 2

POLICIES, SYSTEMS AND CONTROLS

Risk assessment

4. (1) A financial business shall carry out and document a risk assessment for the purpose of—

(a) assessing the money laundering and terrorist financing risks that it faces;

(b) determining how to best manage those risks; and

(c) designing, establishing, maintaining and implementing AML/CFT policies, systems and controls that comply with the requirements of the AML/CFT Regulations and this Code and that are appropriate for those risks.

(2) The risk assessment carried out under subregulation (1) shall take particular account of—

(a) the organisational structure of the financial business, including the extent to which it outsources activities;

(b) its customers;

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(c) the countries with which its customers are connected;

(d) the products and services that the financial business provides or offers to provide; and

(e) how the financial business delivers its products and services.

(3) A financial business shall review and update the risk assessment if there are material changes to any of the matters specified in subregulation (2).

(4) As part of the risk assessment referred to above, a financial business shall prepare and update a risk profile for each customer taking into account the matters specified in subregulation (2).

Responsibilities of board

5. (1) The board of a financial business has ultimate responsibility for—

(a) identifying and managing the money laundering and terrorist financing risks that the financial business faces;

(b) ensuring that adequate resources are devoted to AML/CFT efforts; and

(c) ensuring that the financial business complies with its obligations under POCO, the AML/CFT Regulations and this Code.

(2) Without limiting paragraph (1), the board of a financial business has the following responsibilities—

(a) undertaking the risk assessment required by regulation 4;

(b) on the basis of the risk assessment, establishing documented policies to prevent money laundering and terrorist financing;

(c) ensuring that—

(i) appropriate and effective AML/CFT policies, systems and controls are established, documented and implemented; and

(ii) AML/CFT responsibilities are clearly and appropriately apportioned; and

(d) assessing the effectiveness of, and compliance with, the policies, systems and controls established and promptly taking such actions as is required to remedy deficiencies.

Policies, systems and controls

6. (1) Without limiting regulation 17 of the AML/CFT Regulations, the policies, systems and controls established, maintained and implemented by a financial business under that regulation shall be documented and shall—

(a) include customer acceptance policies and procedures;

(b) provide for transaction limits and management approvals to be established for higher risk customers;

(c) provide for the monitoring of compliance by branches and subsidiaries of the financial business both within and outside the TCI.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(2) A financial business shall establish, maintain and implement systems and controls and take such other measures, as it considers appropriate to guard against the use of technological developments in money laundering or terrorist financing.

(3) A financial business shall maintain an adequately independent audit function to test compliance (including sample testing) with their policies, systems and control established under this regulation.

(4) A financial business shall communicate the policies, systems and control established in accordance with subregulation (1) to all its staff.

Outsourcing

7. (1) Subject to subregulation (2), a financial business may outsource AML/CFT activities, including obligations imposed by the AML/CFT Regulations or this Code.

(2) A financial business shall not outsource—

(a) its AML/CFT compliance functions without the prior written approval of the Commission;

(b) any activity, if the outsourcing of that activity would impair the ability of the Commission to monitor and supervise the financial business with respect to its AML/CFT obligations;

(c) the setting and approval of the its AML/CFT risk management and other strategies;

(d) oversight of the its AML/CFT policies, systems and controls; or

(e) any activity unless it is satisfied that the person to whom the activity is to be outsourced will report any knowledge, suspicion, or reasonable grounds for knowledge or suspicion of money laundering or terrorist financing activity to its MLRO.

(3) A financial business shall—

(a) consider the effect that any outsourcing arrangement may have on the money laundering and terrorist financing risks that it faces; and

(b) comply with such general outsourcing requirements as may, from to time, be issued by the Commission with respect to regulated persons.

(4) Where a financial business outsources an AML or CFT activity, it retains ultimate responsibility for the performance of that activity.

Money laundering reporting officer

8. (1) Subject to paragraph (2), the MLRO appointed by a financial business pursuant to regulation 22 of the AML/CFT Regulations shall—

(a) be an employee of the financial business or of a company in the same group as the financial business and shall be based in the TCI;

(b) have the appropriate skills and experience and otherwise be fit and proper to act as its MLRO;

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(c) possess sufficient independence to perform his role objectively;

(d) have sufficient seniority in the organisational structure of the financial business to undertake its responsibilities effectively and, in particular, to enable the MLRO to have direct access to the board with respect to AML/CFT matters; and

(e) have sufficient resources, including time, to perform the function of MLRO effectively.

(2) A financial business may apply to the Commission for an exemption from paragraph (1)*(a)*.

Money laundering compliance officer

9. (1) Subject to subregulation (2), the MLCO appointed by a financial business pursuant to regulation 21 of the AML/CFT Regulations shall—

(a) be an employee of the financial business or of a company in the same group as the financial business and shall be based in the TCI;

(b) have the appropriate skills and experience and otherwise be fit and proper to act as its MLCO;

(c) possess sufficient independence to perform his role objectively;

(d) have sufficient seniority in the organisational structure of the financial business to undertake its responsibilities effectively and, in particular, to ensure that his requests, where appropriate, are acted upon by the financial business and its staff and his recommendations properly considered by the board;

(e) report regularly, and directly, to the board and have regular contact with the board;

(f) have sufficient resources, including time, to perform the function of MLCO effectively;

(g) have unfettered access to all business lines, support departments and information necessary to perform the functions of MLCO effectively.

(2) A financial business may apply to the Commission for an exemption from subregulation (1)*(a)*.

PART 3

CUSTOMER DUE DILIGENCE

Scope of, and interpretation for, this Part

10. (1) This Part applies to customer due diligence measures that a financial business is required to apply by the AML/CFT Regulations.

(2) For the purposes of this Part, a branch or subsidiary is a "qualifying branch or subsidiary" if it is part of—

(a) a group of companies that has its head office in a country—

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(i) that is subject to legal requirements in its home country for the prevention of money laundering and terrorist financing that are consistent with the requirements of the FATF Recommendations; and

(ii) is subject to effective supervision for compliance with those legal requirements by a foreign regulatory authority;

(b) a group headquartered in a well-regulated country which applies group standards to subsidiaries and branches worldwide, and tests the application of, and compliance with, such standards.

Customer due diligence measures to be applied by financial business

11. (1) Subject to complying with the specific requirements of the AML/CFT Regulations and this Code, a financial business must apply a risk-sensitive approach to determining the extent and nature of the customer due diligence measures to be applied to a customer and to any third party or beneficial owner.

(2) Without limiting subregulation (1), a financial business shall—

(a) obtain customer due diligence information on every customer, third party and beneficial owner comprising—

(i) identification information in accordance with regulation 14, 16, 19 or 21 as the case may be; and

(ii) relationship information in accordance with regulation 12;

(b) consider, on a risk-sensitive basis, whether further identification or relationship information is required;

(c) on the basis of the information obtained under paragraph *(a)* and *(b)*, prepare and record a risk assessment with respect to the customer;

(d) verify the identity of the customer and any third party and take reasonable measures, on a risk-sensitive basis, to verify the identity of each beneficial owner in accordance with regulation 5(1)*(e)* of the AML/CFT Regulations and the relevant regulation of this Code; and

(e) periodically update the customer due diligence information that it holds and adjust the risk assessment that it has made accordingly.

(3) In preparing a risk assessment with respect to a customer, a financial business shall take account of all relevant risks and shall consider, in particular, the relevance of the following risks—

(a) customer risk;

(b) product risk;

(c) delivery risk; and

(d) country risk.

(4) Where a financial business is required by the AML/CFT Regulations or this Code to verify the identity of a person, it shall verify that person's identity using documents, data or information obtained from a reliable and independent source.

(5) This regulation does not limit the requirements of the AML/CFT Regulations.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(6) For the purposes of this regulation, "beneficial owner", with respect to a customer, means a beneficial owner of the customer or of a third party.

Relationship information

12. (1) For the purposes of regulation11, relationship information is information concerning the business relationship, or proposed business relationship, between the financial business and the customer.

(2) The relationship information obtained by a financial business shall include information concerning—

(a) the purpose and intended nature of the business relationship;

(b) the type, volume and value of the expected activity;

(c) the source of funds and, where the customer risk assessment indicates that the customer, business relationship or occasional transaction presents a high risk, the source of wealth of the customer, third party or beneficial owner;

(d) details of any existing relationships with the financial business;

(e) unless the customer is resident in the TCI, the reason for using a financial business based in the TCI; and

(f) such other information concerning the relationship that, on a risk-sensitive basis, the financial business considers appropriate.

(3) Where the customer, third party or beneficial owner is the trustee of a trust or a legal entity (including a company), a financial business shall obtain the following relationship information—

(a) the type of trust or legal entity;

(b) the nature of the activities of the trust or legal entity and the place or places where the activities are carried out;

(c) in the case of a trust—

(i) where the trust is part of a more complex structure, details of that structure, including any underlying companies or other legal entities;

(ii) classes of beneficiaries or charitable objects;

(d) in the case of a legal entity, its ownership and, where the legal entity is a company, details of any group of which the company forms a part, including details of the ownership of the group;

(e) whether the trust, the trustee(s) or the legal entity is subject to supervision in or outside the TCI and, if so, details of the relevant supervisory body.

Politically exposed persons

13. (1) A financial business shall establish, maintain and implement appropriate risk management systems to determine whether a customer, third party or beneficial owner is a politically exposed person and those risk management systems shall take into account that a person may become a politically exposed person after the establishment of a business relationship.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(2) A financial business shall ensure that no business relationship is established with a politically exposed person, or where the third party or beneficial owner is a politically exposed person, unless the prior approval of the board or senior management has been obtained.

(3) Where a financial business has established a business relationship with a customer and the customer, a third party or beneficial owner is subsequently identified as a politically exposed person, the business relationship shall not be continued unless the approval of the board or senior management has been obtained.

(4) Subregulation (3) applies whether the customer, third party or beneficial owner —

(a) was a politically exposed person at the time that the business relationship was established, but the person was subsequently identified as a politically exposed person; or

(b) becomes a politically exposed after the establishment of the business relationship.

(5) A financial business shall take reasonable measures to establish the source of wealth and the source of funds of customers, third parties and beneficial owners identified as politically exposed persons.

Identification information, individuals

14. (1) A financial business shall obtain the following identification information with respect to an individual who it is required by the AML/CFT Regulations or this Code to identify—

(a) the full legal name of, any former names of and any other names used by the individual;

(b) the gender of the individual;

(c) the principal residential address of the individual; and

(d) the date of birth of the individual.

(2) Where a financial business determines that an individual who it is required to identify presents a higher level of risk, the financial business shall obtain additional identification information with respect to the individual.

(3) The additional identification information to be obtained with respect to a higher risk individual shall include at least two of the following—

(a) the individual's place of birth;

(b) the individual's nationality; and

(c) an official government issued identity number or other government identifier.

Verification of identity, individuals

15. (1) A financial business shall—

(a) verify the identity of an individual where required by the AML/CFT Regulations or this Code to do so; and

(b) take reasonable measures to re-verify an aspect of an individual's identity if it changes after the individual's identity has been verified.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(2) Without limiting subregulation (1)*(b)*, the following represent changes of an individual's identity within the meaning of that paragraph—

(a) marriage;

(b) change of nationality; and

(c) change of address.

(3) Where a financial business determines that an individual whose identity it is required to verify presents a low risk, the financial business shall, using evidence from at least one independent source verify—

(a) the individual's full legal name, any former names and any other names used by the individual; and

(b) either—

(i) the principal residential address of the individual; or

(ii) the individual's date of birth.

(4) Where a financial business determines that an individual whose identity it is required to verify presents a higher level of risk, the financial business shall, using evidence from at least two independent sources, verify—

(a) the individual's full legal name, any former names and any other names used by the individual;

(b) the principal residential address of the individual; and

(c) the individual's—

(i) date of birth;

(ii) place of birth;

(iii) nationality; and

(iv) gender.

(5) Where a financial business determines that an individual whose identity it is required to verify presents a high level of risk, the financial business shall, using evidence from at least two independent sources, verify the individual's—

(a) nationality or address; and

(b) government issued identity number or other government identifier.

(6) A document used to identify the identity of an individual must be in a language understood by those employees of the financial business who are responsible for verifying the individual's identity.

Identification information, legal entities

16. (1) This regulation and regulations 17 and 18 apply to a legal entity other than a foundation.

(2) A financial business shall obtain the following identification information with respect to a legal entity that it is required by the AML/CFT Regulations or this Code to identify—

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(a) the full name of the legal entity and any trading names that it uses;

(b) the date of the incorporation, registration or formation of the legal entity;

(c) any official identifying number;

(d) the registered office or, if it does not have a registered office, the address of the head office of the legal entity;

(e) the name and address of the registered agent of the legal entity (or equivalent), if any;

(f) the mailing address of the legal entity;

(g) the principal place of business of the legal entity;

(h) the names of the directors of the legal entity;

(i) identification information on those directors who have authority to give instructions to the financial business concerning the business relationship or occasional transaction;

(j) identification information on individuals who are the ultimate holders of 10% or more of the legal entity.

(3) Where a financial business determines that a legal entity that it is required to identify presents a higher level of risk, the financial business shall obtain such additional identification information with respect to the legal entity as it consider appropriate.

(4) Where subregulation (3) applies, but without limiting it, a financial business shall obtain identification information on every director of the legal entity.

(5) Where identification information on an individual, as a director or beneficial owner, is required to be obtained, regulation 13 applies.

Verification of identity, legal entities

17. (1) A financial business shall—

(a) verify the identity of a legal entity where required by the AML/CFT Regulations to do so; and

(b) take reasonable measures to verify the identity of the beneficial owners of the legal entity.

(2) Where a financial business determines that a legal entity, the identity of which it is required to verify, presents a low risk, the financial business shall, using evidence from at least one independent source verify—

(a) the name of the legal entity;

(b) the official identifying number; and

(c) the date and country of its incorporation, registration or formation.

(3) Where a financial business determines that a legal entity, the identity of which it is required to verify, presents a higher level of risk, the financial business shall verify—

(a) the address of the registered office, or head office, of the legal entity, as applicable; and

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(b) the address of the principal place of business of the legal entity, if different from its registered office or head office.

(4) Where a financial business determines that a legal entity, the identity of which it is required to verify, presents a high level of risk, the financial business shall verify such other components of the legal entity's identification, as it considers appropriate.

(5) A document used to identify the identity of a legal entity or its beneficial owners must be in a language understood by those employees of the financial business who are responsible for verifying their identity.

Verification of directors and beneficial owners

18. (1) A financial business shall in all cases verify the identity of any director of the legal entity specified in regulation 16(2).

(2) Where the financial business determines that the legal entity presents more than a low level of risk, it shall verify such additional components of the identity of the legal entity as it considers appropriate.

(3) Where subregulation (2) applies, but without limiting it, a financial business shall verify the identity of each director and each beneficial owner of the legal entity.

(4) Where the identity of an individual, as director or beneficial owner, is required to be verified, regulation 14 applies.

Identification information, trusts and trustees

19. (1) Where a financial business is required by the AML/CFT Regulations or this Code to identify a trust, it shall—

(a) obtain the following identification information—

(i) the name of the trust;

(ii) the date of the establishment of the trust;

(iii) any official identifying number;

(iv) identification information on each trustee of the trust;

(v) the mailing address of the trustees;

(vi) identification information on each settlor of the trust; and

(vii) identification information on each protector or enforcer of the trust; and

(b) obtain confirmation from the trustees that they have provided all the information requested and that they will update the information in the event that it changes.

(2) For the purpose of this Code, "settlor" includes a person who, as settlor, established the trust and any person who has, at any time, subsequently settled assets into the trust.

(3) Where a financial business determines that any business relationship or occasional transaction concerning the trust that it is required to identify presents a higher level of risk, the financial business shall obtain such additional identification information as it consider appropriate.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(4) Where subregulation (3) applies, but without limiting it, a financial business shall obtain identification information on—

(a) each beneficiary with a vested right; and

(b) each beneficiary, and each person who is an object of a power, who the financial business determines presents a higher level of risk.

(5) Identification information required to be obtained on any person under this regulation shall be obtained in accordance with regulation 14 if the person is an individual, regulation 16 if the person is a legal entity or regulation 21 if the person is a foundation.

Verification of identity, trusts and trustees

20. (1) Where a financial business is required by the AML/CFT Regulations or this Code to verify the identity of a trust, it shall verify—

(a) the name and date of establishment of the trust;

(b) the identity of each trustee, settlor and protector or enforcer of the trust; and

(c) the appointment of the trustee and the nature of his duties.

(2) Where a financial business determines that a trust, the identity of which it is required to verify, presents a higher level of risk, the financial business shall—

(a) take reasonable measures to verify the identity of each person specified in regulation 19(1); and

(b) verify such other components of the legal entity's identification as it considers appropriate.

(3) A document used to verify the identity of a trust or a person specified in this regulation must be in a language understood by those employees of the financial business who are responsible for verifying the identity of the trust or person concerned.

(4) A person whose identity is required by this regulation to be verified shall—

(a) if the person is an individual, be verified in accordance with regulation 15

(b) if the person is a legal entity, be verified in accordance with regulation 17 ; or

(c) if the person is a foundation, be verified in accordance with regulation 22.

Identification information, foundations

21. (1) A financial business shall obtain the following identification information with respect to a foundation, that it is required by the AML/CFT Regulations or this Code to identify—

(a) the full name of the foundation;

(b) the date and country of the establishment, registration, formation or incorporation of the foundation;

(c) any official identifying number;

(d) the registered address, or equivalent, of the foundation or, if the foundation does not have a registered address (or equivalent), the address of the head office of the foundation;

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(e) the mailing address of the foundation, if different from its registered address or equivalent;

(f) the principal place of business of the foundation, if different from its registered address or equivalent;

(g) the name and address of the registered agent of the foundation, if any;

(h) the name and address of the Secretary, or equivalent, of the foundation, if any;

(i) the names of the Foundation Council members (or equivalent) and, if any decision requires the approval of any other persons, the names of those persons;

(j) identification information on those Foundation Council members (or equivalent) who have authority to give instructions to the financial business concerning the business relationship or occasional transaction;

(k) identification information on the guardian of the foundation (or equivalent), if any; and

(*l*) identification information on the founder or founders, on any other person who has contributed to the assets of the foundation and on any person to whom the rights of the founder or founders have been assigned.

(2) Where a financial business determines that a foundation that it is required to identify presents a higher level of risk, the financial business shall obtain such additional identification information with respect to the foundation as it considers appropriate.

(3) Where subregulation (2) applies, but without limiting it, a financial business shall obtain identification information on—

(a) every Foundation Council member of the foundation, or equivalent;

(b) any other persons whose approval is required for any decision;

(c) any beneficiaries of the foundation.

(4) Identification information required to be obtained on any person under this regulation shall be obtained in accordance with regulation 14 if the person is an individual or regulation 16 if the person is a legal entity.

Verification of identity, foundations

22. (1) Where a financial business is required by the AML/CFT Regulations or this Code to verify the identity of a foundation, it shall—

(a) verify the identity of the foundation; and

(b) take reasonable measures to verify the identity of persons concerned with the operation of the foundation.

(2) Where a financial business determines that a foundation the identity of which it is required to verify presents a low risk, the financial business shall, using evidence from at least one independent source, verify—

(a) the name of the foundation and any official identifying number;

(b) the date and country of the foundation's establishment, registration, formation or incorporation.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(3) Where a financial business determines that a foundation, the identity of which it is required to verify, presents a higher level of risk, the financial business shall verify—

(a) the registered address office of the foundation, or the equivalent, or in the case of a foundation that does not have a registered address, the address of the head office of the foundation; and

(b) the address of the principal place of business of the foundation, if different from its registered office or head office.

(4) Where a financial business determines that a foundation, the identity of which it is required to verify, presents a high level of risk, the financial business shall verify such other components of the foundation's identification, as it considers appropriate.

(5) A document used to identify the identity of a foundation or persons concerned with the foundation must be in a language understood by those employees of the financial business who are responsible for verifying their identity.

(6) A person whose identity is required by this regulation or regulation 22 to be verified shall—

(a) if the person is an individual, be verified in accordance with regulation 15 ; or

(b) if the person is a legal entity, be verified in accordance with regulation 17 .

Verification of persons concerned with a foundation

23. (1) A financial business shall in all cases verify the identity of—

(a) any Foundation Council member (or equivalent) specified in regulation 21(1)(i);

(b) the founder or founders, on any other person who has contributed to the assets of the foundation and on any person to whom the rights of the founder or founders have been assigned; and

(c) the guardian of the foundation (or equivalent).

(2) Where the financial business determines that the foundation presents more than a low level of risk, it shall verify such additional components of the identity of the foundation, as it considers appropriate.

(3) Where subregulation (2) applies, but without limiting it, a financial business shall verify the identity of—

(a) each Foundation Council member (or equivalent) of the foundation and, if any decision requires the approval of any other persons, those persons;

(b) any beneficiaries of the foundation.

Non face-to-face business

24. Where a financial business applies customer due diligence measures to, or carries out ongoing monitoring with respect to, an individual who is not physically present, the financial business, in addition to complying with the AML/CFT Regulations and this Code with respect to customer due diligence measures, shall—

(a) perform at least one additional check designed to mitigate the risk of identity fraud; and

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(b) apply such additional enhanced customer due diligence measures or undertake enhanced ongoing monitoring, as the financial business considers appropriate (if any).

Certification of documents

25. (1) A financial business shall not rely on a document as a certified document unless—

(a) the document is certified by an individual who is subject to professional rules of conduct which provide the financial business with a reasonable level of comfort as to the integrity of the certifier;

(b) the individual certifying the document certifies that—

(i) he has seen original documentation verifying the person's identity or residential address;

(ii) the copy of the document (which he certifies) is a complete and accurate copy of that original; and

(iii) where the documentation is to be used to verify identity of an individual and contains a photograph, the photograph contained in the document certified bears a true likeness to the individual requesting certification;

(c) the certifier has signed and dated the copy document, and provided adequate information so that he may be contacted in the event of a query; and

(d) in circumstances where the certifier is located in a higher risk jurisdiction, or where the financial business has some doubts as to the veracity of the information or documentation provided by the applicant, the financial business has taken steps to check that the certifier is real.

Exceptions to due diligence requirements

26. Where a financial business does not apply customer due diligence measures before establishing a business relationship or carrying out an occasional transaction in reliance on regulation 14 of the AML/CFT Regulations, the financial business shall obtain and retain documentation establishing that regulation 14 applies.

Intermediaries and introducers

27. (1) Before relying on an intermediary or an introducer to apply customer due diligence measures in accordance with regulation 14 of the AML/CFT Regulations with respect to a customer, a financial business shall—

(a) satisfy itself that the intermediary or introducer is a regulated person or a foreign regulated person and has procedures in place to undertake customer due diligence measures in accordance with, or equivalent to, the AML/CFT Regulations and this Code;

(b) assess the risk of relying on the intermediary or introducer with a view to determining—

(i) whether it is appropriate to rely on the intermediary or introducer; and

(ii) if it considers it is so appropriate, whether it should take any additional measures to manage that risk;

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(c) obtain adequate assurance in writing from the intermediary or introducer that—

(i) the intermediary or introducer has applied the customer due diligence measures that the financial business for which the financial business intends to rely on it;

(ii) the intermediary or introducer is required to keep, and does keep, a record of the evidence of identification relating to each of the customers of the intermediary or introducer;

(iii) the intermediary or introducer will, without delay, provide the information in that record to the financial business at the request of the financial business; and

(iv) the intermediary or introducer will, without delay, provide the information in the record for provision to the Commission, where requested by the Commission;

(d) where the financial business intends to rely on an introducer, immediately obtain in writing from the introducer—

(i) confirmation that each introduced customer is an established customer of the introducer; and

(ii) sufficient information, including information verifying the identity or ultimate beneficial owner, if not a natural person, about each introduced customer to enable it to assess the risk of money laundering and terrorist financing involving that customer; and

(e) where the financial business intends to rely on an intermediary, immediately obtain in writing sufficient information, including information verifying the identity or ultimate beneficial owner, if not a natural person, about the customer for whom the intermediary is acting to enable the financial business to assess the risk of money laundering and terrorist financing involving that customer.

(2) A financial business shall—

(a) make and retain records—

(i) detailing the evidence that it relied upon in determining that the introducer is a regulated person, together with that evidence or copies of it; and

(ii) detailing the risk assessment carried out under paragraph (1)*(b)* and any additional risk mitigation measures it considers appropriate; and

(b) retain in its records—

(i) the assurances obtained under subregulation (1)*(c)* and the confirmations that it has obtained under subregulation (1)*(d)*; and

(ii) the information that it has sought and obtained under subregulation (1)*(d)* and *(e)*.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

PART 4

MONITORING CUSTOMER ACTIVITY

Ongoing monitoring policies, systems and controls

28. (1) The ongoing monitoring policies, systems and controls established by a financial business in accordance with regulation 17 of the AML/CFT Regulations shall—

(a) provide for a more thorough scrutiny of higher risk customers including politically exposed persons;

(b) be designed to identify unusual and higher risk activity or transactions and require that special attention is paid to higher risk activity and transactions;

(c) require that any unusual or higher risk activity or transaction is examined by an appropriate person to determine the background and purpose of the activity or transaction;

(d) require the collection of appropriate additional information; and

(e) be designed to establish whether there is a rational explanation, an apparent economic or visible lawful purpose, for unusual or higher risk activity or transactions identified, and require a written record to be kept of the conclusions of the financial business.

(2) When conducting ongoing monitoring, a financial business shall regard the following as presenting a higher risk—

(a) complex transactions;

(b) unusual large transactions;

(c) unusual patterns of transactions, which have no apparent economic or lawful purpose;

(d) activity and transactions—

(i) connected with countries which do not, or insufficiently apply, the FATF Recommendations; or

(ii) which are the subject of UN or EU countermeasures; and

(e) activity and transactions that may be conducted with persons who are the subject of UN or EU sanctions and measures.

PART 5

REPORTING SUSPICIOUS ACTIVITY AND TRANSACTIONS

Reporting procedures

29. (1) A financial business shall establish and maintain reporting procedures that—

(a) communicate the identity of the MLRO to its employees;

(b) require that a report is made to the MLRO of any information or other matter coming to the attention of any employee handling relevant business which, in

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

the opinion of that person, gives rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering or terrorist financing;

(c) require that a report is considered promptly by the MLRO in the light of all other relevant information for the purpose of determining whether or not the information or other matter contained in the report gives rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion of money laundering or terrorist financing;

(d) allow the MLRO to have access to all other information which may be of assistance in considering the report; and

(e) provide for the information or other matter contained in a report to be disclosed as soon as is reasonably practicable and in any event, within twenty-four hours by the MLRO to the Anti-Money Laundering Committee in writing, where the MLRO knows, suspects or has reasonable grounds to know or suspect that another person is engaged in or attempted to engage in money laundering or terrorist financing regardless of the amount of the transaction.

(2) For the purposes of this regulation, MLRO includes any deputy MLRO that may be appointed.

Internal reporting procedures

30. (1) A financial business shall establish internal reporting procedures that provide that—

(a) where a customer fails to supply adequate customer due diligence information, or adequate documentation verifying identity (including the identity of any beneficial owners), consideration should be given to making a suspicious activity report;

(b) include the reporting of all suspicious transactions, including attempted transactions regardless of the amount of the transaction and business that has been refused;

(c) require employees to make internal suspicious activity reports containing all relevant information in writing to the MLRO as soon as it is reasonably practicable and in any event, within twenty-four hours after the information comes to their attention;

(d) require suspicious activity reports to include as full a statement as possible of the information giving rise to knowledge or reasonable grounds for suspicion of money laundering or terrorist financing activity and full details of the customer;

(e) provide that reports are not filtered out by supervisory staff or managers so that they do not reach the MLRO;

(f) require suspicious activity reports to be acknowledged by the MLRO.

(2) A financial business must establish and maintain arrangements for disciplining any employee who fails, without reasonable excuse, to make an internal suspicious activity report where he has knowledge or reasonable grounds for suspicion of money laundering or terrorist financing.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

Evaluation of SARs by MLRO

31. A financial business shall ensure that—

(a) all relevant information is promptly made available to the MLRO on request so that internal suspicious activity reports are properly assessed;

(b) each suspicious activity report is considered by the MLRO in light of all relevant information; and

(c) the MLRO documents the evaluation process followed and reasons for the decision to make a report or not to make a report to the Anti-Money Laundering Committee.

Reports to Anti-Money Laundering Committee

32. (1) A financial business shall require the MLRO to make external suspicious activity reports directly to the Anti-Money Laundering Committee as soon as practical and in any event, within 24 hours, that—

(a) include the information specified in subregulation (2); and

(b) are in such form as may be prescribed or specified by the Anti-Money Laundering Committee.

(2) The information required to be included in a report to the Anti-Money Laundering Committee for the purposes of subregulation (1) is—

(a) full details of the customer and as full a statement as possible of the information giving rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion;

(b) if a particular type of criminal conduct is suspected, a statement of this conduct;

(c) where a financial business has additional relevant evidence that could be made available, the nature of this evidence; and

(d) such statistical information as the Anti-Money Laundering Committee may require.

PART 6

EMPLOYEE TRAINING AND AWARENESS

Training and vetting obligations

33. (1) A financial business shall—

(a) provide appropriate basic AML/CFT awareness training to employees whose duties do not relate to the provision of relevant business;

(b) establish and maintain procedures that monitor and test the effectiveness of its employees' AML/CFT awareness and the training provided to them;

(c) vet the competence and probity of employees whose duties relate to the provision of relevant business at the time of their recruitment and at any

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

subsequent change in role and that their competence and probity is subject to ongoing monitoring;

(d) provide training, to temporary and contract staff and, where appropriate, the staff of any third parties fulfilling a function in relation to a financial business under an outsourcing agreement; and

(e) provide employees with adequate training in the recognition and handling of transactions at appropriate frequencies.

(2) The training provided by a financial business shall—

(a) be tailored to the business carried out by the financial business and relevant to the employees to whom it is delivered, including particular vulnerabilities of the financial business;

(b) cover the legal obligations of employees to make disclosures under section 127 of POCO and explain the circumstances in which such disclosures must be made;

(c) explain the risk-based approach to the prevention and detection of money laundering and terrorist financing;

(d) highlight to employees the importance of the contribution that they can individually make to the prevention and detection of money laundering and terrorist financing; and

(e) be provided to employees as soon as practicable after their appointment.

PART 7

RECORD KEEPING

Interpretation for this Part

34. In this Part "records" means records that a financial business is required to keep by the AML/CFT Regulations or this Code.

Manner in which records to be kept

35. (1) A financial business shall ensure that its records are kept in such manner that—

(a) facilitates ongoing monitoring and their periodic updating;

(b) ensures that they are readily accessible to the financial business in the TCI; and

(c) enables the Commission, internal and external auditors and other competent authorities to assess the effectiveness of systems and controls that are maintained by the financial business to prevent and detect money laundering and the financing of terrorism.

(2) Where records are kept other than in legible form, they must be kept in such manner that enables them to be readily produced in the TCI in legible form.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

Transaction records

36. (1) Records relating to transactions with customers shall contain the following information concerning each transaction carried out—

(a) the name and address of the customer;

(b) if the transaction is a monetary transaction, the currency and the amount of the transaction;

(c) if the transaction involves a customer's account, the number, name or other identifier for the account;

(d) the date of the transaction;

(e) details of the counterparty, including account details;

(f) the nature of the transaction;

(g) details of the transaction; and

(h) any conclusions reached as a result of an examination conducted in accordance with regulation 28(1)*(c)* and *(e)*.

(2) A financial business shall, together with its records concerning a business relationship or occasional transaction, keep for the minimum period specified in regulation 19 of the AML/CFT Regulations, all customer files and business correspondence relating to the relationship or occasional transaction.

(3) The transaction records kept by a financial business shall—

(a) contain sufficient details to enable a transaction to be understood; and

(b) enable an audit trail of the movements of incoming and outgoing funds or asset movements to be readily constructed.

(4) A financial business shall maintain records for securities and derivatives transactions for each transaction that identify—

(a) the client—

(i) name of the account holder, including the identity of the beneficial owner; and

(ii) person authorised to transact business;

(b) the amount purchased or sold;

(c) the time of the transaction;

(e) the price of the transaction; and

(f) the individual and the bank or broker and brokerage house that handled the transaction.

Records concerning suspicious transactions, etc.

37. (1) A financial business shall keep for a period of five years from the date a business relationship ends, or for five years from the date that an occasional transaction was completed, records containing, with respect to that business relationship or transaction—

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(a) any internal suspicious activity reports and supporting documentation;

(b) the decision of the MLRO concerning whether to make a suspicious activity report to the Anti-Money Laundering Committee and the basis of that decision;

(c) details of any reports made to the Anti-Money Laundering Committee;

(d) records concerning reviews of and the conclusions reached in respect of —

(i) complex transactions;

(ii) unusual large transactions;

(iii) unusual patterns of transactions, which have no apparent economic or visible lawful purpose; and

(iv) customers and transactions connected with countries which do not apply, or insufficiently apply, the FATF Recommendations or are the subject of UN or EU countermeasures.

(2) A financial business shall keep records of all enquiries relating to money laundering or terrorist financing made to it by the Anti-Money Laundering Committee for a period of at least five years from the date that the enquiry was made.

Records concerning policies, systems and controls and training

38. (1) A financial business shall keep records documenting its policies, systems and controls to prevent and detect money laundering for a period of at least five years from the date that the policies, systems and controls are superseded or otherwise cease to have effect.

(2) A financial business shall keep records for at least five years detailing all dates on which training on the prevention and detection of money laundering and the financing of terrorism was provided to employees, the nature of the training and the names of employees who received the training.

Outsourcing

39. (1) If a financial business outsources record keeping to a third party, the financial business remains responsible for compliance with the record keeping requirements of the AML/CFT Regulations and this Code.

(2) A financial business shall not enter into outsourcing arrangements or place reliance on third parties to keep records where access to records is likely to be impeded by confidentiality or data protection restrictions.

Reviews of record keeping procedures

40. A financial business shall—

(a) periodically review the accessibility of, and condition of, paper and electronically retrievable records and consider the adequacy of the safekeeping of records; and

(b) periodically test procedures relating to the retrieval of records.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

PART 8

CORRESPONDENT BANKING

Application of this Part

41. This Part applies to a bank.

Restrictions on correspondent banking

42. A bank that is, or that proposes to be, a correspondent bank shall—

(a) not enter into or not maintain relationships with any respondent bank that is a shell bank;

(b) not maintain relationships with any respondent bank that itself provides correspondent banking services to shell banks;

(c) apply customer due diligence measures on respondent banks using a risk-based approach that takes into account, in particular—

(i) the respondent's domicile;

(ii) the respondent bank's ownership and management structure;

(iii) the respondent bank's customer base, including its geographic location, its business, including the nature of services provided by the respondent bank to its customers, whether or not relationships are conducted by the respondent on a non face-to-face basis and the extent to which the respondent bank relies on third parties to identify and hold evidence of identity on, or to conduct other due diligence on, its customers;

(d) determine from publicly available sources the reputation of the respondent bank and the quality of its supervision;

(e) assess the respondent bank's anti-money laundering and terrorist financing systems and controls to ensure that they are consistent with the requirements of the FATF Recommendations;

(f) not enter into a new correspondent banking relationship unless it has the prior approval of senior management;

(g) ensure that the respective anti-money laundering and counter terrorist financing responsibilities of each party to the correspondent relationship are understood and properly documented;

(h) ensure that the correspondent relationship and its transactions are subject to annual review by senior management;

(i) be able to demonstrate that the information obtained in compliance with the requirements set out in this regulation is held for all existing and new correspondent relationships; and

(j) not enter into a correspondent banking relationship where it has knowledge or suspicion that the respondent or any of its customers is engaged in money laundering or the financing of terrorism.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

Payable through accounts

43. Where a correspondent bank provides customers of a respondent bank with direct access to its services, whether by way of payable through accounts or by other means, it shall ensure that it is satisfied that the respondent bank—

(a) has undertaken appropriate customer due diligence and, where applicable, enhanced customer due diligence in respect of the customers that have direct access to the correspondent bank's services; and

(b) is able to provide relevant customer due diligence information and verification evidence to the correspondent bank upon request.

PART 9

WIRE TRANSFERS

Interpretation

44. (1) For the purposes of this Part—

"batch file transfer" means several individual transfers of funds which are bundled together for transmission;

"full originator information", with respect to a payee, means the name and account number of the payer, together with—

(a) the payer's address; and

(b) either—

(i) the payer's date and place of birth; or

(ii) the customer identification number or national identity number of the payer or, where the payer does not have an account, a unique identifier that allows the transaction to be traced back to that payer;

"intermediate payment service provider" means a payment service provider, neither of the payer nor the payee, that participates in the execution of transfer of funds;

"payee" means a person who is the intended final recipient of transferred funds;

"payer" means a person who holds an account and allows a transfer of funds from that account or, where there is no account, a person who places an order for the transfer of funds;

"payment service provider" means a person whose business includes the provision of transfer of funds services;

"transfer of funds" means a transaction carried out on behalf of a payer through a payment service provider by electronic means with a view to making funds available to a payee at a payment service provider, irrespective of whether the payer and the payee are the same person; and

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

"unique identifier" means a combination of letters, numbers or symbols determined by the payment service provider, in accordance with the protocols of the payment and settlement or messaging system used to effect the transfer of funds.

Scope of this Part

45. Subject to regulation 43, this Part applies to a transfer of funds in any currency which is sent or received by a payment service provider that is established in the TCI.

Exemptions

46. (1) Subject to subregulation (2), a transfer of funds carried out using a credit or debit card is exempt from this Part if—

(a) the payee has an agreement with the payment service provider permitting payment for the provision of goods and services; and

(b) a unique identifier, allowing the transaction to be traced back to the payer, accompanies the transfer of funds.

(2) A transfer of funds is not exempt from the application of this Part if the credit or debit card is used as a payment system to effect the transfer.

(3) A transfer of funds is exempt from this Part if the transfer is carried out using electronic money, the amount transacted does not exceed $1,000 and where the device on which the electronic money is stored—

(a) cannot be recharged, the maximum amount stored in the device is $200; or

(b) can be recharged, a limit of $2,500 is imposed on the total amount that can be transacted in a calendar year, unless an amount of $1,000 or more is redeemed in that calendar year by the bearer of the device.

(4) For the purposes of this regulation, electronic money is money as represented by a claim on the issuer which—

(a) is stored on an electronic device;

(b) is issued on receipt of funds of an amount not less in value than the monetary value issued; and

(c) is accepted as means of payment by persons other than the issuer.

(5) A transfer of funds made by mobile telephone or any other digital or information technology device is exempt from this Part if—

(a) the transfer is pre-paid and does not exceed $1,000;

(b) the transfer is post-paid;

(c) the payee has an agreement with the payment service provider permitting payment for the provision of goods and services;

(d) a unique identifier, allowing the transaction to be traced back to the payer, accompanies the transfer of funds; and

(e) the payment service provider of the payee is a licensee.

(6) A transfer of funds is exempt if—

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(a) the payer withdraws cash from the payer's own account;

(b) there is a debit transfer authorization between two parties permitting payments between them through accounts, provided a unique identifier accompanies the transfer of funds to enable the transaction to be traced back;

(c) it is made using truncated cheques;

(d) it is a transfer to the Government of, or a public body in, the TCI for taxes, duties, fines or charges of any kind; or

(e) both the payer and the payee are payment service providers acting on their own behalf.

Payment service provider of payer

47. (1) Subject to regulation 43, the payment service provider of a payer shall ensure that every transfer of funds is accompanied by the full originator payer information.

(2) paragraph (1) does not apply in the case of a batch file transfer from a single payer, where some or all of the payment service providers of the payees are situated outside the TCI, if—

(a) the batch file contains the complete information on the payer; and

(b) the individual transfers bundled together in the batch file carry the account number of the payer or a unique identifier.

(3) The payment service provider of the payer shall, before transferring any funds, verify the full originator information on the basis of documents, data or information obtained from a reliable and independent source.

(4) In the case of a transfer from an account, the payment service provider may deem verification of the full originator information to have taken place if it has complied with the provisions of the AML/CFT Regulations and this Code relating to the verification of the identity of the payer in connection with the opening of that account.

(5) In the case of a transfer of funds not made from an account, the full originator information on the payer shall be deemed to have been verified by a payment service provider of the payer if—

(a) the transfer consists of a transaction of an amount not exceeding $1,000;

(b) the transfer is not a transaction that is carried out in several operations that appear to be linked and that together comprise an amount exceeding $1,000; and

(c) the payment service provider of the payer does not suspect that the payer is engaged in money laundering, terrorist financing or other financial crime.

(6) The payment service provider of the payer shall keep records of full originator information on the payer that accompanies the transfer of funds for a period of at least five years.

(7) Where the payment service provider of the payer and the payee are situated in the TCI, a transfer of funds need only be accompanied by—

(a) the account number of the payee; or

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(b) a unique identifier that allows the transaction to be traced back to the payer, where the payer does not have an account number.

(8) Where this regulation applies, the payment service provider of the payer shall, upon request from the payment service provider of the payee, make available to the payment service provider of the payee the full originator information within three working days, excluding the day on which the request was made.

(9) Where a payment service provider of the payer fails to comply with a request to provide the full originator information within the period specified in subregulation (8), the payment service provider of the payee may notify the Commission, either or both of which shall require the payment service provider of the payer to comply with the request immediately.

(10) Without prejudice to subregulation (9), where a payment service provider of the payer fails to comply with a request, the payment service provider of the payee may—

(a) issue such warning to the payment service provider of the payer as may be considered necessary;

(b) set a deadline to enable the payment service provider of the payer to provide the required full originator information;

(c) reject future transfers of funds from the payment service provider of the payer;

(d) restrict or terminate its business relationship with the payment service provider of the payer with respect to transfer of funds services or any mutual supply of services.

Payment service provider of payee

48. (1) The payment service provider of the payee shall verify that fields within the messaging or payment and settlement system used to effect the transfer in respect of the full originator information on the payer have been completed in accordance with the characters or inputs admissible within the conventions of that messaging or payment and settlement system.

(2) The payment service provider of the payee shall put in place effective procedures for the detection of any missing or incomplete full originator information.

(3) In the case of batch file transfers, the full originator information is required only in the batch file and not in the individual transfers bundled together in it.

(4) Where the payment service provider of the payee becomes aware that the full originator information on the payer is missing or incomplete when receiving transfers of funds, the payment service provider of the payee shall—

(a) reject the transfer,

(b) request for the full originator information on the payer, or

(c) take such course of action as the Commission directs, after it has been notified of the deficiency discovered with respect to the full originator information of the payer,

unless where doing so would result in contravening POCO or the Anti-terrorist Financing Order.

(5) A missing or an incomplete information shall be a factor in the risk-based assessment of a payment service provider of the payee as to whether a transfer of funds or any

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

related transaction is to be reported to the Anti-Money Laundering Committee as a suspicious transaction or activity with respect to money laundering or terrorist financing.

(6) The payment service provider of the payee shall keep records of any information received on the payer for a period of at least five years.

Intermediary payment service provider

49. (1) This regulation applies where the payment service provider of the payer is situated outside the TCI and the intermediary service provider is situated within the TCI.

(2) An intermediary payment service provider shall ensure that any information it receives on the payer that accompanies a transfer of funds is kept with that transfer.

(3) Where this regulation applies, an intermediary service provider may use to send a transfer to the payment service provider of the payee a system with technical limitations which prevents the information on the payer from accompanying the transfer of funds.

(4) Where, in receiving a transfer of funds, the intermediary payment service provider becomes aware that information on the payer required under this Part is incomplete, the intermediary payment service provider may only use a payment system with technical limitations if the intermediary payment service provider (either through a payment or messaging system, or through another procedure that is accepted or agreed upon between the intermediary payment service provider and the payment service provider of the payee) provides confirmation that the information is incomplete.

(5) An intermediary payment service provider that uses a system with technical limitations shall, if the payment service provider of the payee requests, within three working days after the day on which the intermediary payment service provider receives the request, make available to the payment service provider of the payee all the information on the payer that the intermediary payment service provider has received, whether or not the information is the full originator information.

(6) An intermediary payment service provider that uses a system with technical limitations which prevents the information on the payer from accompanying the transfer of funds shall keep records of all the information on the payer that it has received for a period of at least five years.

———————

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

NON-PROFIT ORGANISATIONS REGULATIONS

ARRANGEMENT OF REGULATIONS

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

PART VI

MISCELLANEOUS

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

NON-PROFIT ORGANISATIONS REGULATIONS
– SECTIONS 174 AND 175

(Legal Notices 12/2013 and 50 /2014)

Commencement

[21 November 2014]

PART I

PRELIMINARY

Short title

1. (1) These Regulations may be cited as the Non-Profit Organisations Regulations 2014 and shall, except for Part V, come into operation on publication.

(2) Part V shall come into operation on such date as the Governor may appoint by notice published in the *Gazette*.

Interpretation

2. (1) In these Regulations—

"FATF" means the international body known as the Financial Action Task Force on Money Laundering;

"FATF Recommendations" means the FATF Recommendations, February 2012 and such amendments as may from time to time be made to them;

"fiduciary" means—

(a) a trustee of the trust, where the non-profit organisation is established as a trust;

(b) a director of the company, where the non-profit organisation is established as a company;

(c) a person responsible for all aspects of the management and administration of the unincorporated association, where the non-profit organisation is established by an unincorporated association; or

(d) a person not covered in paragraphs *(a)*, *(b)* and *(c)*, where the non-profit organisation is established by that person;

"gross annual income" during any period, means the total income of the non-profit organisation from any source during the twelve months immediately preceding the first day of that period, including, but not limited to—

(a) income received from the provision of goods or services;

(b) rental income;

(c) interest and other income derived from its investments;

(d) donations of money or other property made to the organisation;

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

"NPO legislation" means—

(a) the Proceeds of Crime Ordinance;

(b) terrorist financing legislation and any Ordinances, regulations and other laws relating to terrorism and terrorist financing that are applicable to non-profit organisations;

(c) these Regulations; and

(d) an Anti-money Laundering and Terrorist Financing Code issued under section 175*(b)* of the Ordinance that is applicable to non-profit organisations;

"NPO Register" means the register of non-profit organisations established and kept under regulation 5;

"NPO Supervisor" means the supervisory authority specified under regulation 3;

"Ordinance" means the Proceeds of Crime Ordinance.

(2) Unless otherwise provided terms used in these Regulations shall have the same meaning as defined in the Ordinance.

PART II

NPO SUPERVISOR

Prescribed supervisory authority

3. The Financial Services Commission is prescribed as the NPO Supervisor.

Functions and duties of NPO Supervisor

4. The functions of the NPO Supervisor are—

(a) to act as the registration, supervision and enforcement authority for non-profit organisations operating in the Islands;

(b) to monitor compliance—

(i) by non-profit organisations with the registration requirements of these Regulations; and

(ii) by registered non-profit organisations with the NPO legislation;

(c) to monitor the effectiveness of the NPO legislation in—

(i) protecting non-profit organisations from being used for terrorist financing or money laundering; and

(ii) ensuring the compliance of the Government with the FATF Recommendations, as they apply to non-profit organisations;

(d) to undertake periodic reviews of the non-profit sector in the Islands for the purpose of identifying the features and types of non-profit organisations that are at risk of being used for terrorist financing or money laundering;

(e) to undertake outreach to non-profit organisations with the objective of protecting the non-profit sector in the Islands from being used for terrorist financing or money laundering; and

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(f) to discharge such other functions as may be assigned to the NPO Supervisor under the Ordinance, these Regulations or any other Ordinance.

(2) The outreach activities undertaken by the NPO Supervisor shall include—

(a) raising awareness of non-profit organisations concerning the risks of their being used for terrorist financing or money-laundering and the measures available to protect against such abuse; and

(b) promoting transparency, accountability, integrity and public confidence in the administration and management of non-profit organisations.

(3) Where the NPO Supervisor forms the view that the NPO legislation is not effective in protecting non-profit organisations from being used for terrorist financing or money laundering, the NPO Supervisor shall make a report to the Governor in Cabinet recommending appropriate changes to the NPO legislation.

PART III

REGISTRATION OF NON-PROFIT ORGANISATIONS

Register to be kept

5. (1) The NPO Supervisor shall establish and keep a Register of non-profit organisations.

(2) The NPO Register shall contain the following information in respect of each non-profit organisation that has been registered—

(a) its full name, address in the Islands, telephone number and e-mail address (if any);

(b) a summary of its purpose, objectives and activities;

(c) the names of the persons who own, control or direct the non-profit organisation;

(d) the date of its registration and, if applicable, de-registration;

(e) whether it is incorporated or unincorporated and, if incorporated, the number with which it is registered under the Companies Ordinance;

(f) if the non-profit organisation is not incorporated—

(i) the address in the Islands that it has given as its address for the service of notices and other document; and

(ii) the address where it keeps its records; and

(g) such other information as the NPO Supervisor considers appropriate.

(3) The NPO Supervisor shall maintain a file in respect of each registered non-profit organisation (whether currently registered or not) in which shall be kept the following—

(a) originals or notarised copies of the non-profit organisation's constitutional documents and by-laws, as amended from time to time, and, if incorporated, the official document certifying its incorporation; and

(b) other documents, correspondence and material relevant to the non-profit organisation as the NPO Supervisor considers appropriate.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(4) The NPO Register and the information contained in any document filed with the NPO Supervisor may be kept in such manner as the NPO Supervisor considers appropriate, by means of a device or facility that—

(a) records or stores information magnetically, electronically or by other means; and

(b) permits the information recorded or stored to be inspected and reproduced in legible and usable form.

(5) A person may, during normal business hours on payment of a fee of $50, require the NPO Supervisor to provide details of the information entered on the NPO Register in respect of a registered non-profit organisation.

Requirement to register

6. (1) Subject to subregulation (2), a non-profit organisation shall be registered in the NPO Register if it is—

(a) incorporated, formed or otherwise established in the Islands; or

(b) administered in or from within the Islands.

(2) A non-profit organisation is exempted from the requirement to be registered under this Regulation if the non-profit organisation—

(a) has a gross annual income not exceeding $10,000 and assets not exceeding $20,000 in value; and

(b) has been issued with a certificate of exemption pursuant to subregulation (4).

(3) A non-profit organisation can at any time apply in writing to the NPO Supervisor for a certificate of exemption from the requirement for registration by submitting an application in the form specified by the NPO Supervisor and such documents as the NPO Supervisor may specify.

(4) The NPO Supervisor shall issue a certificate of exemption to a non-profit organisation which makes an application under subregulation (3) if the NPO Supervisor is satisfied that the requirements under subregulation (2)*(a)* are met and if the NPO Supervisor is satisfied that the non-profit organisation poses no risk of facilitating terrorist-financing or money-laundering, having regard to one or more of the following matters—

(a) the length of time it has operated as a non-profit organisation without indication of having facilitated terrorist-financing or money-laundering;

(b) the nature of its activity or its manner of functioning;

(c) the identity or type of its members;

(d) its affiliation with organisations outside the Islands or lack thereof.

(5) Where an unregistered non-profit organisation—

(a) is found not to qualify under subregulation (2)*(a)*; or

(b) qualifies under subregulation (2)*(a)*, but is unable to demonstrate to the satisfaction of the NPO Supervisor that it poses no risk of facilitating terrorist-financing or money laundering,

the NPO Supervisor shall give written notice to the non-profit organisation that it is does not qualify for exemption from the requirement to be registered and unless the non-profit

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

organisation, within thirty days after the date of the notice, shows good reason to the satisfaction of the NPO Supervisor why it should be exempted, it shall be required to be registered.

(6) Where the NPO Supervisor reasonably determines—

(a) that an exempted non-profit organisation poses a risk of facilitating terrorist-financing or money-laundering; or

(b) that an exempted non-profit organisation has a gross annual income and assets that exceed the amounts specified in paragraph (2)*(a)*,

the NPO Supervisor shall give written notice to the non-profit organisation stating that it will no longer be exempted from the requirement to be registered and unless the non-profit organisation, within fourteen days after the date of the notice, shows good reason to the satisfaction of the NPO Supervisor why it should continue to be exempted, the non-profit organisation shall no longer be exempted from the provisions of these Regulations and, where it is in possession of a certificate of exemption, shall immediately return the certificate to the NPO Supervisor.

(7) An application for a certificate of exemption shall be accompanied by an application fee of $150.

(8) A non-profit organisation that operates when not registered or exempted under this regulation commits an offence and is liable on summary conviction to a fine of $30,000.

Application to register

7. (1) Application may be made to the NPO Supervisor to register a non-profit organisation or a proposed non-profit organisation.

(2) The application shall be—

(a) in writing and in the form specified by the NPO Supervisor;

(b) signed by a person acting on behalf of the non-profit organisation; and

(c) accompanied by—

(i) such documents or information as may be specified by these Regulations or as the NPO Supervisor may reasonably require; and

(ii) a non-refundable registration fee of $150.

(3) The NPO Supervisor may require an applicant to—

(a) submit such additional documents and information, in addition to what is specified in subregulation (2)*(c)*(i), as the NPO Supervisor may reasonably require to determine the application, and such documents and information shall be in such form as the NPO Supervisor may require; and

(b) verify any document or information provided in support of an application in such manner as the NPO Supervisor may specify.

(4) If, before the determination by the NPO Supervisor of an application or before the registration of a non-profit organisation—

(a) there is a material change in any information or documentation provided by or on behalf of the applicant to the NPO Supervisor in connection with the application; or

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(b) the applicant discovers that any such information or documentation is incomplete, inaccurate or misleading,

the applicant shall, as soon as reasonably practicable, give the NPO Supervisor written particulars of the change or of the incomplete, inaccurate or misleading information or documentation.

(5) Where an application is made to register a non-profit company, the NPO Supervisor shall satisfy himself that the applicant is duly registered under Part V of the Companies Ordinance.

Registration

8. (1) Following the receipt of an application and registration fee under regulation 7 and any additional documents or information that it has required under regulation 7(3)*(a)*, unless the NPO Supervisor refuses the application under regulation 9(1), the NPO Supervisor shall—

(a) if the application is for the registration of an established non-profit organisation, register the non-profit organisation in the NPO Register and provide the applicant and the non-profit organisation with a certificate of registration; or

(b) if the application relates to a proposed non-profit organisation, provide the applicant with written notice of its intention to register the proposed non-profit organisation, provided that the non-profit organisation is established within a period of twenty-one days from the date of the notice.

(2) Subject to subregulation (3), if—

(a) the NPO Supervisor provides notice of its intention to register a proposed non-profit organisation; and

(b) within twenty-one days of the date of the notice, the NPO Supervisor is provided with satisfactory evidence that the proposed non-profit organisation has been established,

the NPO Supervisor shall register the non-profit organisation, and provide the applicant and the non-profit organisation with a certificate of registration.

(3) Every non-profit organisation registered under these Regulations shall keep—

(a) its certificate of registration at the address listed in the NPO Register; and

(b) in the case of a non-profit organisation that is not incorporated, the address specified in regulation 5(2)(ii)),

and produce it for inspection, without charge, at the request of any person.

(4) Notwithstanding subregulation (2), the NPO Supervisor may refuse to register a non-profit organisation if, following the provision of a notice under paragraph (1)*(b)*, the NPO Supervisor forms the opinion that there are grounds under regulation 9(1) for refusing the application for registration.

Refusal of application to register

9. (1) The NPO Supervisor may refuse an application for registration if—

(a) the application does not comply with regulation 7(2);

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(b) the applicant fails to provide any information or documents required by the NPO Supervisor under regulation 7(3);

(c) the NPO Supervisor is of the opinion that—

(i) the non-profit organisation is not, or the proposed non-profit organisation will not be a non-profit organisation within the meaning of the Ordinance;

(ii) the non-profit organisation or proposed non-profit organisation is being used for terrorist financing or money-laundering or it is intended or likely that it will be used for such purpose;

(iii) it is contrary to the public interest for the non-profit organisation to be registered; or

(iv) any of the persons involved in the establishment or operation of the non-profit organisation has been convicted of an offence involving dishonesty;

(d) the non-profit organisation, having previously been registered under these Regulations, has been de-registered under regulation 10.

(2) If the NPO Supervisor refuses an application for registration, it shall send the applicant a written notice of refusal, stating the grounds for its refusal.

De-registration

10. (1) The NPO Supervisor shall de-register a registered non-profit organisation if—

(a) the non-profit organisation is convicted of an offence under the Ordinance, the terrorist financing legislation or these Regulations;

(b) a civil forfeiture order is made against the non- profit organisation under the Ordinance or the terrorist financing legislation;

(c) a forfeiture order is made against the NPO under article 15 or 16 of the Anti-terrorist Financing Order;

(d) subject to subregulation (3), a person authorised on behalf of the non-profit organisation requests that the non-profit organisation be de-registered; or

(e) the non-profit organisation has been struck off the Companies Register.

(2) The NPO Supervisor may de-register a registered non-profit organisation if, in the opinion of the NPO Supervisor the non-profit organisation—

(a) has breached these Regulations or an Anti-money Laundering and Terrorist Financing Code made under section 175*(b)* of the Ordinance, that applies to it;

(b) no longer exists or is not carrying out, and is not likely to carry out, the activities specified for the non-profit organisation in the NPO Register; or

(c) is being used, or may in the future be used, for, or to assist in, terrorist financing or money laundering.

(3) The NPO Supervisor shall not de-register a non-profit organisation under subregulation (1)*(d)* if the NPO Supervisor is of the opinion that the de-registration of the NPO would hinder the NPO Supervisor in the exercise of its functions.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(4) Subject to subregulation (5), before de-registering a non-profit organisation under any provision of this regulation other than subregulation (1)*(d)*, the NPO Supervisor shall give written notice to the non-profit organisation stating—

(a) the grounds upon which it intends to de-register the non-profit organisation; and

(b) that unless the non-profit organisation, by written notice, shows good reason why it should not be de- registered, it will be de-registered on a date not less than fourteen days after the date of the notice.

(5) If it is not practicable for the NPO Supervisor to give notice to the non-profit organisation under subregulation (4) or where there has been no response from the non-profit organization within the time specified in subregulation (4), the NPO Supervisor shall publish a notice in the *Gazette* to the effect that it intends to de-register the non-profit organisation.

(6) Where the NPO Supervisor de-registers a non-profit organisation, the NPO Supervisor shall mark the name of the non-profit organisation in the NPO Register as de-registered, showing the date of its de-registration.

PART IV

OBLIGATIONS OF NON-PROFIT ORGANISATIONS

Change of information to be provided to NPO Supervisor

11. (1) If there is a change in any information provided to the NPO Supervisor, whether the information was provided before or after its registration, or directly or indirectly by the registered non-profit organisation, the non-profit organisation shall give the NPO Supervisor written notice of the change, as soon as reasonably practicable.

(2) Changes required to be provided under this regulation include changes to the non-profit organisation's purposes, objectives and activities.

Records

12. (1) Every non-profit organisation, whether registered or exempted, shall keep—

(a) records of—

(i) its purpose, objectives and activities;

(ii) the identity of the persons who control or direct its activities, including, as appropriate, senior officers, directors and trustees;

(iii) the identity, credentials and good standing of its beneficiaries and associate non-profit organisations; and

(b) financial records that—

(i) show and explain its transactions, within and outside the Islands, and that are sufficiently detailed to show that its funds have been used in a manner consistent with its purposes, objectives and activities; and

(ii) show the source of its gross annual income.

(2) A non-profit organisation shall keep the records specified under subregulation (1) for a period of at least five years.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(3) A non-profit organisation that contravenes this regulation commits an offence and is liable on summary conviction to a fine of $20,000.

Provision of records to the NPO Supervisor

13. (1) The NPO Supervisor may, on the grounds specified in subregulation (2), by written notice to a non-profit organisation, require it to produce any record that the non-profit organisation is required to keep under regulation 12.

(2) The NPO Supervisor may give notice under sub-regulation (1) only where it has reasonable cause to suspect that the non-profit organisation is being used, or may in the future be used, for, or to assist in, terrorist financing or money laundering.

(3) A notice given under subregulation (1)—

(a) shall specify—

(i) the records which the NPO Supervisor requires to be produced;

(ii) the place where the records specified in the notice shall be produced to the NPO Supervisor, which may be by inspection at the premises of the non-profit organisation; and

(iii) the period within which the records shall be produced; and

(b) may require the documents to be produced to a person or persons specified in the notice.

(4) The NPO Supervisor may require the person who produced the records or any person who appears to be an officer or employee of the non-profit organisation or otherwise associated with it, to provide an explanation of the records.

(5) The NPO Supervisor may take copies or extracts of the records produced under this regulation or may retain the original records for a period not exceeding—

(a) a period of one year; or

(b) such longer period as the Court, on the application of the NPO Supervisor, may specify.

(6) Disclosure of records under this regulation shall not be treated as a breach of any enactment, rule of law or agreement restricting the disclosure of information and shall not give rise to civil proceedings.

(7) A non-profit organisation that fails to comply with a notice issued under paragraph (1) commits an offence and is liable on summary conviction to a fine of $50,000.

(8) A person required to provide an explanation of any records produced under this regulation who, without reasonable excuse, fails to provide the explanation, commits an offence and is liable on summary conviction to a fine of $50,000.

Accounts

14. (1) A registered non-profit organisation shall prepare and submit annually to the NPO Supervisor, financial statements of the organisation's revenue and expenditure.

(2) The registered non-profit organisation shall submit—

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(a) financial statements, certified by an accountant, where the gross annual income of the non-profit organisation exceeds $500,000; or

(b) financial statements, in a form approved by the NPO Supervisor, where the gross annual income of the non-profit organisation does not exceed $500,000.

(3) The financial statements required by paragraph (2) shall include—

(a) a list of donors who have donated in excess of $10,000 as a single donation or cumulatively, during the year; and

(b) a breakdown of any funds raised, or donations received, and disbursed, by any association of person operating under and subject to the control of the non-profit organisation.

(4) The statements required by subregualtion (2*)* shall be submitted, within six months after the end of the year or its financial year, unless prior written approval of an extension has been granted by the NPO Supervisor.

(5) A registered non-profit organisation shall pay to the NPO Supervisor a fee of $100 upon submitting its financial statements.

Power to require an audit

15. (1) Where the NPO Supervisor has reasonable cause to suspect that a non-profit organisation is being used, or may in the future be used, for, or to assist in, terrorist financing or money laundering, it may, by written notice to the non-profit organisation, require an audit of its accounts to be investigated and audited by an independent auditor appointed by the non-profit organisation with the approval of the NPO Supervisor.

(2) An auditor appointed in accordance with subregulation (1) shall—

(a) have the right of access to all books, accounts and documents relating to the non-profit organisation that are in the possession or under the control of the directors and persons acting or having concern in the management and administration of the non-profit organisation or of the property or income of the non-profit organisation or to which the directors and such persons have access;

(b) be entitled to require from any person referred to in paragraph *(a)* or any past or present member, officer or servant of the non-profit organisation, such information and explanation as he thinks necessary for the performance of his duties; and

(c) at the conclusion of, or during the progress of, the audit make such reports to the NPO Supervisor on the audit or the accounts or affairs of the non-profit organisation as the auditor thinks the case requires, and send a copy of the report to the persons referred to in paragraph *(a)*.

(3) The expenses of an audit under subregulation (1), including the remuneration of the auditor, shall be paid by the non-profit organisation.

(4) A person commits an offence if he—

(a) fails to afford an auditor any facility to which he is entitled under subregulation (2);

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(b) fails to make full disclosure to the NPO Supervisor of all material facts required to be disclosed under this Ordinance in respect of a non-profit organisation; or

(c) knowingly makes—

(i) a false statement of a material fact; or

(ii) a statement containing information that is misleading in light of the circumstances in which it was made.

(5) A person who commits an offence under subregulation (4) is liable on summary conviction to a fine of $5,000 or to a term of imprisonment for six months, or to both.

PART V

ENFORCEMENT ACTION

NPO Supervisor may take disciplinary action

16. (1) For the purposes of this Part—

(a) "disciplinary violation" means a contravention of—

(i) a provision of the Anti-Money Laundering and Terrorist Financing Regulations specified in those Regulations as a disciplinary violation; or

(ii) a provision of an Anti-Money Laundering and Terrorist Financing Code specified in the relevant Code as a disciplinary violation;

(b) the imposition of an administrative penalty becomes final on the earliest of—

(i) the payment by the non-profit organisation of the penalty;

(ii) the date when, in accordance with regulation 17(5), the non-profit organisation is considered to have committed the disciplinary violation; or

(iii) the dismissal of any appeal of the non-profit organisation, provided that the time for any further appeal has expired.

(2) The NPO Supervisor may take disciplinary action against a non-profit organisation if it is satisfied that the non-profit organisation has committed a disciplinary violation.

(3) The NPO Supervisor takes disciplinary action against a non-profit organisation by imposing an administrative penalty on it.

(4) The administrative penalty imposed on a non-profit organisation in respect of a disciplinary violation shall be a sum no greater than the maximum sum specified—

(a) in the case of a contravention specified in sub- regulation (1)*(a)*(i), in the Anti-Money Laundering and Terrorist Financing Regulations;

(b) in the case of a contravention specified in sub- regulation (1)*(a)*(ii), in the relevant Anti-Money Laundering and Terrorist Financing Code.

(5) A violation that is committed or continued on more than one day constitutes a separate violation for each day on which it is committed or continued.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(6) The NPO Supervisor shall not take disciplinary action against a non-profit organisation in respect of a disciplinary violation committed more than two years prior to the date upon which it sends a notice to the non-profit organisation under regulation 17.

(7) If the conduct or omission that constitutes a disciplinary violation also constitutes an offence, the taking of disciplinary action against a non-profit organisation does not prevent the non-profit organisation being also prosecuted for the offence.

Notice of intention to take disciplinary action

17. (1) If the NPO Supervisor intends to take disciplinary action against a non-profit organisation, it shall send a notice of its intention to the non-profit organisation which—

(a) sets out the alleged disciplinary violation and the relevant facts surrounding the violation;

(b) sets out the penalty it intends to impose for the violation; and

(c) advises the non-profit organisation of its right to make written representations to the NPO Supervisor in accordance with subregulation (2).

(2) A non-profit organisation that receives a notice under subregulation (1) may, within twenty-eight days of the date upon which it receives the notice, send written representations to the NPO Supervisor disputing the facts of the alleged disciplinary violation or the administrative penalty or both.

Disciplinary action

18. (1) After the expiration of twenty-eight days from the date that the NPO Supervisor sent a notice under regulation 17 to a non-profit organisation, the NPO Supervisor may take disciplinary action against that non-profit organisation by sending it a penalty notice stating—

(a) the disciplinary violation in respect of which the notice is issued;

(b) the date on which notice of intention to take disciplinary action in respect of that violation was sent to the non-profit organisation;

(c) the amount of the administrative penalty for the violation;

(d) a date, not less than twenty-eight days after the date of the penalty notice, by which the non-profit organisation shall pay the penalty to the NPO Supervisor; and

(e) that if the non-profit organisation does not pay the penalty or exercise its rights of appeal under section 176 of the Proceeds of Crime Ordinance, it will be considered to have committed the violation and that it is liable for the penalty set out in the notice.

(2) Before taking disciplinary action against a non-profit organisation under subregulation (1), the NPO Supervisor shall consider any written representations that it has received from the non-profit organisation and, where it receives such representations, it must provide reasons for the action that it takes.

(3) A non-profit organisation that receives a penalty notice under subregulation (1) shall pay the penalty stated to the NPO Supervisor on or before the date specified in the notice or appeal the notice under section 176 of the Proceeds of Crime Ordinance.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(4) If the non-profit organisation pays the administrative penalty, it is considered to have committed the violation and the disciplinary action is over.

(5) A non-profit organisation that neither pays the administrative penalty nor appeals the notice within twenty-eight days is considered to have committed the disciplinary violation and is liable for the penalty.

(6) If the NPO Supervisor imposes an administrative penalty on a non-profit organisation, the NPO Supervisor shall, after the imposition of the penalty has become final, advertise the imposition of the penalty by publication in the *Gazette*.

Recovery of administrative penalty

19. (1) An administrative penalty constitutes a debt to the NPO Supervisor and may be recovered in the court.

(2) The NPO Supervisor may, after the imposition of a penalty has become final, issue a certificate certifying the unpaid amount of any debt referred to in subregulation (1) and the registration of the certificate in the court has the same effect as a judgment of the court for a debt of the amount specified in the certificate together with the costs of registration.

PART VI

MISCELLANEOUS

Confidentiality

20. (1) A person shall keep confidential all information relating to a non-profit organisation which he has acquired in his capacity as an employee of the Financial Services Commission, except as required for an inquiry in respect of any matter under these Regulations or the Ordinance or on the order of a court of competent jurisdiction.

(2) A person who contravenes subregulation (1) commits an offence and is liable on summary conviction to a fine of $10,000.

Offence, false and misleading information

21. A person who, with intent to deceive or for any purpose of these Regulations—

(a) provides any information, makes any representation or submits any document or return that he knows to be false or materially misleading or does not believe to be true; or

(b) recklessly provides any information, makes any representation or submits any document or return that is false or materially misleading,

commits an offence and is liable on summary conviction to a fine of $50,000.

Non-applicability

22. These Regulations do not apply to a non-profit orgainsation that—

(a) does not solicit funds from the general public or receive concession from the Government or any statutory body in the pursuit of its objects; and

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai

(b) has as its fiduciary, management body or other service provider a person that is regulated by the Financial Services Commission under the Trustees Licensing Ordinance, the Company Management (Licensing) Ordinance or any other relevant law.

© Crown Copyright 2018
Copying/unauthorised distribution strictly prohibited.
Printed under Authority by The Regional Law Revision Centre Inc.
www.lawrevision.ai