REPUBLIC OF NAURU

ANTI-MONEY LAUNDERING AND TARGETED FINANCIAL SANCTIONS ACT 2023

No. 2 of 2023

An Act to strengthen Nauru's capacity to deter, detect and respond to money laundering, the financing of terrorism and proliferation financing and for related purposes.

Certified: [7 June 2023]

Table of Provisions

Enacted by the Parliament of Nauru as follows:

PART 1 – PRELIMINARY

1 Short title

This Act may be cited as the Anti-Money Laundering and Targeted Financial Sanctions Act 2023.

2 Commencement

This Act commences on the date it is certified by the Speaker.

3 Objectives

The objectives of this Act are to:

(a) provide for the effective legal, regulatory and operational measures for combating money laundering, terrorist financing and proliferation financing and other related threats in the Republic;

(b) provide for measures enabling the detection and prevention of money laundering, terrorist financing and proliferation financing;

(c) protect the financial system of the Republic from being used for money laundering and the financing of terrorism and proliferation financing;

(d) provide for and empower the Financial Intelligence Unit and certain other departments or government agencies to carry out their powers, functions and responsibilities under the Act or any other written law;

(e) enable the Republic to enforce targeted financial sanctions to prevent and arrest terrorism, terrorist financing and proliferation financing;

(f) make provision for reporting entities to establish procedures and commit resources to comply with the requirements of combatting money laundering, terrorist financing and proliferation financing;

(g) continue to further enhance the international reputation of the Republic where appropriate by the adoption of financial action task force and other mutually agreed relevant international commitments;

(h) facilitate cooperation amongst reporting entities domestically and internationally, with government agencies international partners which are vested with similar duties, functions and responsibilities;

(i) provide for the Financial Intelligence Unit to be the national coordination body for AML/CFT; and

(j) establish public confidence in the financial system of the Republic.

PART 2 – DEFINITIONS

4 Interpretation

(1) In this Act:

'account' means a facility or arrangement through which a reporting entity takes custody of or accepts deposits of property or allows returning, withdrawals or transfer of such property of a customer and includes:

(a) a facility or arrangement by which a reporting entity:

(i) pays, collects or draws on a bearer negotiable instrument on behalf of another person; or

(ii) provides secured storage facility to the customers to keep his or her property;

(b) a closed account, the records of which a reporting entity is required to maintain for 7 years;

(c) an inactive or dormant account; and

(d) an account with no balance;

'activity' means an act or omission made by a person;

'AML/CFT' means Anti-Money Laundering and Combatting the Financing of Terrorism and other financial crime, in or outside of the Republic;

'AML/CFT compliance programme' means an *AML*/CFT compliance programme developed under Section 19;

'bearer negotiable instruments' means:

(a) a bill of exchange;

(b) cheque;

(c) promissory note;

(d) bearer bond;

(e) travellers cheque;

(f) money order, postal order or similar order; or

(g) any other instrument prescribed by regulations;

'beneficial owner*'* has the same meaning given to it under Section 5 of the *Beneficial Ownership Act 2017* and any amendment to the definition under that Act shall *mutatis mutandis* apply to this Act;

'beneficiary entity' means a financial institution that receives a request from a person to receive an electronic currency transfer;

'business relationship' means a business, professional or commercial relationship of a customer that is:

(a) connected with the professional activities of a reporting entity; and

(b) expected, at the time when the initial contact is established, to have an element of duration;

'cash' means currency in physical form;

'criminal conduct' means conduct that:

(a) occurs in and constitutes an offence in the Republic for which the maximum penalty is a term of imprisonment of 2 years or more or the imposition of a fine of more than $5,000;

(b) occurred outside of the Republic, but had it occurred in the Republic, would constitute an offence in the Republic for which the maximum penalty under the law of the Republic is a term of imprisonment of 2 years or more or the imposition of a fine of more than $5,000;

(c) constitutes an offence under Section 234, 239, 242, 250, 251, 252, 253, 254 or 255 of the *Customs Act 2014*;

(d) constitutes an offence under Section 58 of the *Copyright Act 2019*;

(e) consists of the non-payment or evasion of any form of tax, duty or other statutory levy;

(f) consists of insider trading, including dealing in publicly traded property or securities whilst in possession of information, that is not generally available but, which would materially affect the price or value of the property or securities if it were generally available; or

(g) consists of market manipulation, being conduct involving entering into or carrying out two or more transactions for the purpose of influencing the price of the subject-matter of the transaction in order to induce other persons to buy, sell or subscribe for the same subject-matter;

'criminal property' means property, whether situated within or outside of the Republic, that is, in whole or in part and whether directly or indirectly, derived or realised from, obtained, used or intended to be used, in connection with criminal conduct and includes:

(a) any interest in such property;

(b) any dividend, other income or value accruing from or generated by such property; and

(c) property that was later converted, transformed or intermingled from such property;

regardless of who carried out the criminal conduct or who benefited from it;

'currency' means the following used in or outside the Republic:

(a) legal tender in physical or non-physical form; or

(b) tender that is customarily used and accepted as a medium of exchange;

'customer' in relation to a transaction, business relationship or an account, means the person in whose name or for whom the transaction, relationship or account is arranged, opened or undertaken and includes:

(a) a signatory to the transaction, relationship or account;

(b) any person who is authorised to conduct the transaction or control the relationship or account;

(c) any person who has been assigned or transferred a business relationship or account or rights or obligations under the transaction or relationship; or

(d) any other prescribed person or prescribed class of persons;

'customer due diligence' means the obligations that are imposed on reporting entities by Division 3 of Part 4;

'deal or dealing with property' includes:

(a) concealing property;

(b) disguising property;

(c) converting property;

(d) transferring property;

(e) removing property from the Republic;

(f) bringing property into the Republic;

(g) receiving property;

(h) acquiring property;

(i) using property;

(j) possessing property;

(k) engaging in a banking transaction relating to property;

(l) entering into an agreement, arrangement or understanding in relation to property; or

(m) consenting to, authorising or enabling any of the actions referred to in any of paragraphs (a) to (l).

'document' means any record of information and includes:

(a) anything on which there is writing;

(b) anything on which there are marks, figures, symbols or perforations having meaning for persons qualified to interpret them;

(c) anything from which sounds, images or writings can be produced, with or without the aid of anything else;

(d) a map, plan, drawing, photograph or similar thing;

(e) bearer negotiable instruments; or

(f) an electronic document;

'domestic electronic currency transfer' means an electronic currency transfer or a chain of electronic currency transfers, where the originating entity and the beneficiary entity are located in the Republic;

'electronic currency transfer' means a transaction carried out on behalf of a person who is the sender through a reporting entity by electronic means with a view to making an amount of currency available to a person who is the receiver, who may also be the sender at another reporting entity, but excludes:

(a) transfers and settlements between reporting entities where both the sender and the receiver are reporting entities acting on their own behalf; and

(b) credit and debit card transactions where the credit or debit card is issued within the Republic;

'false name' means a fictitious, pseudo name, incorrect, anonymous or any other name which is not a registered name under the *Births, Deaths and Marriages Registration Act 2017* or any other similar legislation in another country;

'fiat currency' means currency issued by a government as legal tender;

'financial crime' includes conduct that constitutes:

(a) the offence of money laundering provided for under Section 9;

(b) the offence of dealing with property reasonably suspected to be criminal property under Section 10;

(c) an offence under Section 125 for the breach of regulations made under Part 7;

(d) the offence of terrorism financing under Section 10 of the *Counter Terrorism and Transnational Organised Crime Act 2004*;

(e) the offence of provision of property or services to terrorist group under Section 11 of the *Counter Terrorism and Transnational Organised Crime Act 2004*;

(f) the offence of dealing with terrorist property under Section 12 of the *Counter Terrorism and Transnational Organised Crime Act 2004*;

(g) an offence under Part 9 of the *Crimes Act 2016*;

(h) the provision of financial support to persons, that attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery;

(i) the provision of financial support to countries or states that attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery where such conduct violates one or more resolutions of the United Nations Security Council;

(j) any other conduct or class of conduct prescribed by the regulations; or

(k) any conduct outside of the Republic that, had the conduct occurred in the Republic, would constitute an offence referred to in paragraphs (a) to (f) or an offence prescribed pursuant to paragraph (j),

whether or not criminal or other proceedings have been brought, in or outside of the Republic, in relation to that conduct;

'financial group' has the meaning given by Section 5;

'financial institution' means any natural or legal entity engaged in the conduct of the following activities or operations:

(a) accepting of deposits and other repayable cash or bearer negotiable instruments from the public, including private banking;

(b) lending, including, but not limited to, consumer credit, mortgage credit, factoring with or without recourse and financing of commercial transactions, including forfeiting;

(c) finance leasing;

(d) provision of a money or value transfer service;

(e) issuing and managing the means of payment which includes, credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic transactions and virtual currencies;

(f) issuing financial guarantees and commitments;

(g) trading in:

(i) bearer negotiable instruments;

(ii) foreign exchange;

(iii) exchange, interest rate and index instruments;

(iv) transferable securities; or

(v) commodity futures trading;

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

(i) individual and collective portfolio management;

(j) safekeeping and administration of currency, bearer negotiable instruments or liquid securities on behalf of other persons;

(k) investing, administering or managing funds or money on behalf of other persons;

(l) underwriting and placement of insurance, including insurance intermediation by agents and brokers;

(m) money and currency conversion; or

(n) provision of services in relation to virtual assets, including, but not limited to:

(i) the exchange between virtual assets and fiat currencies;

(ii) the exchange between one or more forms of virtual assets;

(iii) the transfer of virtual assets;

(iv) the safekeeping or administration of virtual assets or instruments enabling control over virtual assets; and

(v) the participation in and provision of financial services relating to an issuer's offer or sale of virtual assets;

'FIU' means the Financial Intelligence Unit established under the *Anti-Money Laundering Act 2008* and continued under Section 68;

'foreign financial intelligence body' means a foreign institution or agency which:

(a) has functions and powers similar to those of the FIU;

(b) is an institution or agency of:

(i) a foreign state; or

(ii) an international organisation established by the governments of various State;

'foreign law enforcement body' means a foreign institution or agency which:

(a) has law enforcement functions and powers; and

(b) is an institution or agency of:

(i) a foreign state; or

(ii) an international organisation established by the governments of various States;

'high value dealer' means a person who is in business of buying and selling the following articles by way of cash, transactions or series of related cash transactions:

(a) jewellery;

(b) watches;

(c) gold, silver or other precious metals;

(d) diamonds, sapphire and other precious metals;

(e) paintings;

(f) protected Republic or foreign objects;

(g) artistic and cultural artefacts; and

(h) any such other articles as may be prescribed;

'identification information' means:

(a) in the case of an individual, the person's full name, current or last known address and occupation; and

(b) in the case of a body corporate, other body or any other legal entity, its name, legal form, registration number, registered address and principal place of business where it is different from the registered address;

'intermediary entity' means a financial institution that receives a request to receive and transmit an electronic currency transfer on behalf of an originating entity and a beneficiary entity or another intermediary entity;

'international electronic currency transfer' means a single or a chain of electronic currency transfers that occur where one of the following parties to the transaction is located outside the Republic:

(a) the originating entity;

(b) the intermediary entity; or

(c) the beneficiary entity;

'knowledge' means for the purposes of a money laundering offence or any offence under this Act of having actual or constructive knowledge or knowledge capable of being acquired with reasonable inquiry;

'legal entity' includes a body, corporation, trust, association, organisation whether or not having its own establishing instrument, a statutory corporation or an entity established under any written law;

'Minister' means the Minister responsible for Justice and Border Control;

'money laundering' means to deal or dealing with property with the knowledge that it is criminal property;

'money or value transfer service' means a service that involves:

(a) the acceptance of currency, cheques, other monetary instruments or other stores of value; and

(b) the payment of a corresponding sum in currency or other form to a beneficiary by means of:

(i) a communication, message or transfer; or

(ii) through a clearing network to which the provider of the service belongs;

'occasional transaction' means any transaction that does not take place in the context of a business relationship;

'originating entity' means a financial institution that receives a request from a person to execute an electronic currency transfer;

'politically exposed person' has the meaning given by Section 6;

'property' means assets of any kind, whether real or personal, corporeal or incorporeal, moveable or immovable, tangible or intangible, whether situated within or outside the Republic and includes documents or instruments in electronic, digital or other form, evidencing title to or an interest in, any such assets:

(a) an enforceable right of action in relation to any such assets;

(b) a legal or equitable interest, in any such assets; and

(c) virtual currency or assets or non-fungible tokens;

'record' means any material on which data or information is recorded or marked and which is capable of being read or understood by a person, computer system or other device;

'reporting entity' has the meaning given by Section 7;

'Secretary' means the Secretary for Justice and Border Control;

'sender' means a person who requests a reporting entity to execute an electronic currency transfer;

'senior management' means:

(a) the directors of the reporting entity; or

(b) the key employees of the reporting entity who are appointed to ensure that the reporting entity is effectively controlled on a day to day basis and who have responsibility for overseeing the reporting entity's proper conduct;

'shell bank' means a bank that:

(a) is incorporated or licensed in a country in which the bank has no physical presence; and

(b) is not affiliated with a financial group that is subject to effective consolidated supervision;

'Supervisor' means the Financial Intelligence Supervisor appointed under Section 70;

'supervisory authority' means any body or agency having regulatory, supervisory or licensing authority over a reporting entity;

'suspicious activity report' means a report submitted under Section 59;

'suspicious transaction' means a transaction that gives rise to a reasonable suspicion that such transaction relates to the contravention of this Act;

'terrorist property' has the meaning given to it under the *Counter Terrorism and Transnational Organised Crime Act 2004*;

'transaction' has the meaning given by Section 8;

'value transfer services' means a service that involves the acceptance of currency, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in currency or other form, to a beneficiary by means of a communication, message or transfer or through a clearing network to which the provider of the service belongs;

'verifying evidence' means reliable official source documents, data, information or other evidence that is reasonably capable of verifying the identity of the person;

'verifying the identity' means verifying the accuracy of the identification information for the person using verifying evidence for the person; and

'virtual asset' means a digital representation of value that is digitally traded or transferred and that can be used for payment or investment purposes, but does not include digital representations of fiat currencies, securities and other financial assets.

(2) For the purposes of the definition of '***deal or dealing with property***', concealing or disguising property includes concealing or disguising its nature, source, location, disposition, movement or ownership or any rights in relation to it.

5 Meaning of "financial group"

(1) A group of 2 or more legal entities is a financial group where:

(a) the group consists of a parent company or other type of body;

(b) the parent company or that other type of body exercises control and coordinating functions over the rest of the group, including branches and subsidiaries, for the application of group policies and controls; and

(c) taken as a whole, the group satisfies the definition of a reporting entity.

(2) To avoid doubt, members of a financial group, including the parent company, branches and subsidiaries, can be in different countries.

6 Meaning of "politically exposed person"

(1) A person who is or has been entrusted with prominent public functions by a foreign country is a politically exposed person and includes but is not limited to:

(a) the President or the head of the government;

(b) a politician;

(c) a government official holding the office as the Head of Department;

(d) a judicial official;

(e) a senior military official;

(f) a senior executive of a State owned corporation;

(g) a senior political party official; or

(h) any other person as may be prescribed.

(2) A person who is or has been entrusted with a prominent function by an international organisation is a politically exposed person and includes but is not limited to a director, deputy director, a member of the board or governing body of the organisation and a person holding an equivalent position within the organisation.

(3) A person who is or has been entrusted by the Republic with prominent public functions is a politically exposed person and includes but is not limited to:

(a) the President of the Republic;

(b) the Speaker;

(c) a Minister;

(d) a Deputy Minister;

(e) the Deputy Speaker;

(f) a Member of Parliament;

(g) a head of a department;

(h) the Chief Justice and a judge of the Supreme Court;

(i) a Chief Executive Officer and the Chairperson of the Board of an instrumentality of the Republic or a prescribed public enterprise under the *Public Enterprise Act 2019;* and

(j) any other person as may be prescribed.

(4) A person who is a family member or close associate of a person referred to in subsection (1), (2) or (3) is a politically exposed person.

7 Meaning of "reporting entity"

A ***'reporting entity'*** means:

(a) any person that undertakes banking under the *Banking Act 1975*;

(b) a financial institution;

(c) a real estate agent;

(d) a person operating a casino or conducting a lottery, including those carried out over the internet;

(e) a high value dealer;

(f) trust or company service provider:

(i) forming bodies, partnerships or other legal arrangements;

(ii) acting as or arranging for another person to act as, a director or secretary of a corporation or a partner of a partnership or a similar position in relation to other bodies or legal arrangements;

(iii) providing a registered office, business address or accommodation, correspondence or administrative address for a corporation, partnership or other body or legal arrangements;

(iv) acting as, or arranging for another person to act as, a trustee of an express trust; or

(v) acting as, or arranging for another person to act as, a nominee shareholder for another person outside of the Republic;

(g) a legal practitioner or an accountant when they prepare for or carry out transactions for their clients relating to:

(i) buying or selling real estate;

(ii) managing client money, securities or other assets;

(iii) managing bank, savings or securities accounts;

(iv) organising contributions for the creation, operation or management of companies; or

(v) creating, operating or managing bodies or legal arrangements and buying and selling of business entities;

(h) a person collecting, holding, cashing in, remitting or delivering cash as part of a business providing payroll services; and

(i) excludes a person or class of persons prescribed under this Act.

8 Meaning of "transaction"

(1) A transaction is a deposit, withdrawal, exchange or transfer of property:

(a) in physical currency;

(b) by cheque, payment order or other instrument;

(c) by electronic or other non-physical means; or

(d) in satisfaction, in whole or part, of any contractual or other legal obligation.

(2) Without limiting subsection (1), a transaction includes the:

(a) the establishment of a business relationship;

(b) the opening of an account;

(c) the engagement of a service;

(d) any payment made in respect of a lottery, bet or other game of chance; or

(e) the establishment or creation of a body or legal arrangement.

PART 3 – MONEY LAUNDERING

9 Offence of money laundering

(1) A person shall not engage in money laundering.

(2) A person who contravenes subsection (1) commits an offence and shall be liable upon conviction:

(a) for an individual, to a fine not exceeding $500,000 or imprisonment for a term not exceeding 20 years, or to both; or

(b) for a body corporate, to a fine not exceeding $2,500,000.

10 Offence of dealing with property reasonably suspected to be criminal property

(1) A person shall not deal with property where it is reasonable to suspect that such property is criminal property.

(2) A person who contravenes subsection (1) commits an offence and shall be liable upon conviction:

(a) for an individual, to a fine not exceeding $60,000 or imprisonment for a term not exceeding 5 years, or to both; or

(b) for a body corporate, to a fine not exceeding $300,000.

(3) Without limiting subsection (1), it is reasonable to suspect that property is criminal property where:

(a) dealing with the property involves a number of transactions that are conducted to avoid reporting obligations under this Act or any other written law;

(b) dealing with the property involves using one or more accounts maintained in false names;

(c) the value of the property involved is grossly disproportionate to the person's lawful income and expenditure over a reasonable period of time within which the conduct occurs;

(d) dealing with the property involves a transaction to which reporting obligations attach under Section 59 or 62 or which exceeds the threshold for the reporting obligation under this Act and the person has:

(i) contravened those reporting obligations; or

(ii) given false or misleading information in purported compliance with those reporting obligations;

(e) dealing with the property involves an importation or exportation which is required by law to be reported and the person has:

(i) contravened his or her obligations under the law relating to making the report; or

(ii) given false or misleading information in purported compliance with those obligations; or

(f) the person has:

(i) stated that dealing with the property was engaged in on behalf, or at the request, of another person; or

(ii) not provided information enabling the other person to be identified.

11 Combining several contraventions in a single charge

A single charge of an offence against Section 9 or 10 constitutes an offence against either Section respectively even though it may include more than one instance of the person engaging in conduct, whether that conduct occurs at the same time or at different times.

12 Proof of criminal property

(1) For the purposes of proving criminal property under Sections 9 and 10 it shall not be necessary to establish:

(a) who committed the criminal conduct in relation to the property;

(b) that there is a conviction relating to the criminal conduct; or

(c) that the property had derived from particular criminal conduct but shall prove the general nature or type of criminal conduct from which the property had derived.

(2) For the purposes of proving criminal property under Sections 9 and 10, the prosecution may rely on evidence that the circumstances in which the property had been handled are such as to give rise to the inference that it can only be derived from criminal conduct.

13 Parallel investigations or proceedings

Nothing in this Part precludes the conduct of parallel investigations or proceedings of a criminal, civil or administrative nature arising from the same facts in relation to the same or different persons.

PART 4 – OBLIGATIONS OF REPORTING ENTITIES

Division 1 – Preliminary matters

14 Exemptions and modifications of this Part

(1) Subject to subsection (2), the Minister in consultation with the Cabinet may make a determination:

(a) exempting from any or all of the provisions of this Part:

(i) a reporting entity or class of reporting entities; or

(ii) an activity or class of activities; or

(b) modifying, the application of this Part to:

(i) a reporting entity or class of reporting entities; or

(ii) an activity or class of activities.

(2) A determination under subsection (1) shall not be made unless the Cabinet and the Minister are satisfied that:

(a) there is a low risk of financial crime in the circumstances covered by the determination; or

(b) the reporting entity or activity covered by the determination will be adequately regulated under anti-money laundering or combatting financing of terrorism laws and supervised by authorities of another country.

(3) The FIU shall work independently in ensuring that the arrangements in subsection (2)(b) are duly complied with.

(4) A determination made under this Section is valid for a period of 5 years, unless earlier revoked or rescinded by the Cabinet.

(5) A determination under this Section may be renewed from time to time, with or without any conditions, as the Cabinet may deem fit.

15 Obligation to comply notwithstanding secrecy obligations

Subject to Section 16, a reporting entity shall comply with the requirements of this Act, notwithstanding any obligation as to secrecy or other restriction on the disclosure of information imposed by any written law or otherwise.

16 Protection of legal professional privilege

Nothing in this Act requires a legal practitioner to disclose information, documents or communications that are protected by a law governing legal professional privilege.

17 Sanctions for directors and senior management of reporting entities that are not individuals

(1) This Section applies to a reporting entity that is not an individual.

(2) A director or other member of senior management of the reporting entity commits an offence under this Act where the following is deemed to have occurred:

(a) the act or omission constituting the offence took place with the actual knowledge or reckless disregard of the director or other member of senior management; and

(b) the director or other member of senior management, by act or omission, gave his or her authority, permission or consent to the act or omission constituting the offence.

(3) The maximum level of penalty that applies to the reporting entity applies to the director or other member of senior management concerned.

(4) A criminal proceeding may be taken against a reporting entity for an offence under this Act, notwithstanding a director or other member of senior management of the reporting entity not being charged with an offence.

18 Protection for actions undertaken in good faith

(1) This Section applies to:

(a) a reporting entity;

(b) an auditor or supervisory authority of a reporting entity;

(c) a director of a reporting entity;

(d) an officer, employee or agent of a reporting entity acting in the course of his or her employment or agency; and

(e) a person who previously held an office or position referred to under paragraphs (a) to (d).

(2) No civil, criminal or disciplinary proceedings shall be made against a person under subsection (1), for any act or omission made, where it:

(a) is done or omitted under this Act in good faith; or

(b) is in compliance with a lawful direction given by the FIU.

(3) A person to whom this Section applies is deemed, for the purposes of the prosecution of a financial crime, not to have been in possession at any time of information in a report made to the FIU under this Act, where the report:

(a) is true or accurate truthful to the best of the person's knowledge; and

(b) contains all relevant particulars requested by the FIU that are available to the person.

(4) Where an act or omission relates to a criminal conduct or suspicion of a criminal conduct, the protection of this Section applies, notwithstanding:

(a) the person affected did not know what criminal offence had been committed; and

(b) that the criminal conduct had actually occurred.

(5) The proceedings referred to in subsection (2) include proceedings for breach of a restriction on the disclosure of information imposed by a contract or by any written law.

Division 2 – Ongoing compliance obligations

19 General requirement for internal AML/CFT compliance programme

(1) A reporting entity shall develop and implement an AML/CFT compliance programme within 1 month after commencing business.

(2) The reporting entity's AML/CFT compliance programme shall:

(a) be recorded in writing setting out the internal procedures, policies including a business risk assessment conducted under Section 24 and;

(i) controls that the reporting entity establishes, operates and maintains to ensure that the reporting entity complies with its obligations under this Act;

(ii) manage and mitigate the risks identified in any business risk assessment undertaken under Section 24; and

(iii) meet the reporting entity's obligations under Sections 20 to 24;

(b) be approved by senior management of the reporting entity; and

(c) be disclosed to the directors, officers, employees and agents of the reporting entity.

(3) The reporting entity shall implement its AML/CFT compliance programme.

(4) The FIU may require by a notice to the reporting entity to provide the AML/CFT compliance programme which the reporting entity shall provide to the FIU within 14 working days after receiving the notice.

20 Financial crime compliance officer

(1) A reporting entity shall appoint an individual to be a financial crime compliance officer of the reporting entity, who for the purpose of this Section is also referred to as an officer.

(2) The functions of the officer are:

(a) to administer and maintain the reporting entity's AML/CFT compliance programme;

(b) to serve as the FIU's primary point of contact within the reporting entity;

(c) such other functions as may be assigned by the reporting entity to comply with the requirements of this Act or any other written law; and

(d) to ensure the reporting entity complies with the requirements of AML/CFT and this Act.

(3) The officer shall:

(a) be a member of senior management of the reporting entity;

(b) have a right of direct access to the directors or the managing board of the reporting entity;

(c) have sufficient time and resources to properly discharge his or her functions in relation to compliance of the requirements of financial crimes; and

(d) act independently in carrying out his or her functions.

(4) A reporting entity may appoint one or more deputy financial crime compliance officers to exercise the functions of the financial crime compliance officer in the officer's absence from work or to assist the officer with his or her duties.

(5) The reporting entity may adequately remunerate the office for carrying out his or her functions under this Act.

21 Independent audit of compliance

A reporting entity shall maintain appropriate procedures and adequate resources to independently and periodically, test and assess:

(a) the effectiveness of the reporting entity's AML/CFT compliance programme; and

(b) the reporting entity's compliance with its obligations under this Part.

22 Appointment of new director, officer, employee or agent

A reporting entity shall establish, maintain and operate screening procedures to enable the reporting entity to satisfy itself of the competence and integrity of a new appointment or newly appointed director, officer, employee or agent to oversee or undertake duties related to obligations under this Part.

23 Training

A reporting entity shall take appropriate steps to ensure that its directors, officers, employees and agents receive regular and adequate training having regard to their roles in:

(a) the risks of financial crime as they apply in the circumstances of the reporting entity;

(b) the reporting entity's AML/CFT compliance programme;

(c) any new developments, methods and trends in financial crime of relevance to the business of the reporting entity; and

(d) the requirements of this Act and how to recognise and report suspicious activity.

24 Business risk assessment of the reporting entity

(1) A reporting entity shall prepare a written business risk assessment as soon as reasonably practicable, but no later than 3 months after the date on which the reporting entity commences business.

(2) A business risk assessment by a reporting entity shall identify and assess the financial crime risks posed by:

(a) the customers, countries or geographic areas with which the reporting entity engages;

(b) the products, services, transactions and delivery channels utilised by the reporting entity;

(c) the nature, scale and complexity of the reporting entity's activities;

(d) any reliance on third parties for elements of the customer due diligence process;

(e) new products, business practices or delivery methods or systems proposed to be implemented by the reporting entity;

(f) developing technologies for both new and pre-existing products and services proposed to be used by the reporting entity;

(g) the impact of any new technologies; and

(h) any other relevant risk factor as may be prescribed.

(3) A reporting entity shall prepare its business risk assessment with reference to:

(a) any available risk assessment prepared by the FIU or other relevant authorities, whether in or outside of the Republic;

(b) guidelines published by the FIU;

(c) suspicious activity reports made under Section 59 and reports made under Section 61 that the reporting entity has prepared, and any analysis relating to such reports that have been conducted;

(d) open-source intelligence on the reporting entity's customers, in particular those with high net worth and those who are politically exposed persons;

(e) proprietary databases that provide customer due diligence information on politically exposed persons and high-risk customers; and

(f) court cases relating to the reporting entity's customers.

(4) A reporting entity shall, through its AML/CFT compliance programme, take appropriate measures to manage and mitigate the risks identified in:

(a) its business risk assessment; and

(b) relevant risk assessments prepared by the FIU and other relevant authorities, whether in or outside of the Republic.

(5) A reporting entity shall review its business risk assessment at least once every 12 months and keep it up to date.

(6) A reporting entity shall keep a record of:

(a) its business risk assessment and the underlying reasoning;

(b) its review of its business risk assessment and the underlying reasoning; and

(c) the methodology used to prepare and review its business risk assessment.

(7) A reporting entity shall identify and assess the financial crime risks that the reporting entity may be exposed to including identifying any risk factors.

(8) A business risk assessment shall be approved by the senior management of the reporting entity.

25 Compliance obligations for existing businesses

(1) This Section applies to a reporting entity where it is carrying on business on the date of commencement of this Act.

(2) The reporting entity shall:

(a) carry out a business risk assessment in accordance with Section 24 within 12 months after the commencement; and

(b) develop and implement an AML/CFT compliance programme within 12 months after such commencement.

26 Financial groups to implement group-wide AML/CFT compliance programme

(1) A financial group shall establish, operate and maintain a group-wide AML/CFT compliance programme.

(2) A group-wide AML/CFT compliance programme shall:

(a) be applicable and appropriate to all branches and majority-owned subsidiaries of the financial group;

(b) include the requirements referred to in Section 19;

(c) include policies and procedures for sharing information between members of the financial group required for the purposes of customer due diligence and AML/CFT risk management;

(d) include policies and procedures for branches and majority-owned subsidiaries to provide customer account and transaction information to the financial group when necessary; and

(e) have adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent disclosure of information contrary to the provisions of a law with confidentiality provisions.

(3) For the purpose of subsection (2)(c) and (d), ***'information'*** includes, but is not limited to:

(a) information and analysis of transactions or activities which appear unusual where such analysis is made;

(b) a suspicious activity report and its underlying information;

(c) the fact than a suspicious activity report has been submitted to the FIU; and

(d) other transaction information from branches and subsidiaries where necessary for AML/CFT purpose.

27 Foreign branches and majority-owned foreign subsidiaries to comply with this Part

(1) A reporting entity shall ensure that its foreign branches and majority-owned foreign subsidiaries located outside the Republic apply, to the extent permitted by the law of that foreign country, measures equivalent to those provided under this Part.

(2) Where the law of a foreign country does not permit the application of the equivalent measures provided under this Part, the reporting entity shall, as soon as is reasonably practicable, inform the FIU accordingly and take such additional measures as are permitted to implement the requirements of this Part.

28 Obligation to maintain records

(1) A reporting entity shall keep and maintain records of any matter required under this Act.

(2) Any record that is required to be kept under this Act shall be maintained in a manner and form that will enable the reporting entity to comply immediately with requests for information from the FIU or other law enforcement authorities.

(3) The Cabinet may make regulations to provide for further requirements for the keeping of records, including the list of records to be kept.

29 Period for keeping records

(1) Subject to subsection (4) a record required to be kept and maintained under Section 28 shall be kept for a minimum period of 7 years commencing from the date on which the:

(a) record was created;

(b) record was most recently updated or modified;

(c) account to which the record relates was closed; or

(d) business relationship to which the record relates ceased.

(2) The 7 year period referred to under subsection (1), commences from the latest date of any of the events referred to under paragraphs (a) to (d).

(3) A reporting entity that contravenes the requirements of this Section commits an offence and shall be liable upon conviction:

(a) for an individual, to a fine not exceeding $200,000 or imprisonment for a term not exceeding 10 years, or to both; or

(b) for a body corporate, to a fine not exceeding $1,000,000.

(4) The 7 year period referred to in subsection (1) is deemed not to have commenced where the record relates to an open account or ongoing business relationship, notwithstanding that the record itself was created and last modified more than 7 years ago.

Division 3 – Obligation to conduct customer due diligence

Subdivision 1 – Preliminary matters

30 Customer due diligence records

A reporting entity shall:

(a) keep a record of the process used to conduct customer due diligence under this Division and where required undertake analysis; and

(b) retain this record as part of its records under Division 2 of this Part.

31 When customer due diligence is not able to be completed

(1) Where a reporting entity is unable to comply with the customer due diligence required under this Act, the reporting entity shall not conduct a transaction, open an account or enter into a business relationship with such person, an agent or a beneficial owner.

(2) Where a business relationship exists with a reporting entity and the reporting entity is not able to comply with the customer due diligence requirement, the reporting entity shall terminate the existing business relationship.

(3) Subsections (1) and (2) are subject to a direction made under subsection (5).

(4) In complying with this Section, the reporting entity shall consider making a suspicious activity report in accordance with Division 5 of this Part.

(5) The FIU may direct in writing the manner in which the reporting entity shall manage a transaction, account or business relationship for the person and the reporting entity shall comply with the direction.

32 When customer due diligence risks tipping off customer

A reporting entity shall file a suspicious activity report in accordance with Division 5 of this Part, where the reporting entity:

(a) forms a suspicion that a financial crime is occurring; or

(b) reasonably believes that the performance of customer due diligence under this Division discloses or is likely to disclose, that suspicion to the customer concerned.

33 Reliance on third parties in relation to obligations under this Division

(1) This Section applies where a reporting entity relies on an intermediary entity or a third party to undertake the reporting entity's obligations under this Division or to introduce business to the reporting entity.

(2) The reporting entity shall:

(a) immediately obtain from the intermediary entity or third party:

(i) in the case of an individual, the identification information required by Section 37;

(ii) in the case of a body corporate, the identification information required by Sections 37 and 38;

(iii) in the case of a person acting in the capacity of a trustee, the identification information required by Sections 37 and 39;

(iv) the information required by Section 40; and

(v) the information required by Sections 41 and 42 and regulations made pursuant to Section 45, where applicable;

(b) ensure that verifiable copies of verifying evidence relating to the requirements of Sections 37, 38, 39, 40 and 42, where relevant are made available to it by the intermediary entity or third party upon the request of such reporting entity and without delay;

(c) assess whether:

(i) the location of the intermediary entity or third party is a high-risk location; and

(ii) the countries or geographical areas in which the intermediary entity or third party operates are high risk countries or geographical areas; and

(d) satisfy itself that:

(i) the intermediary entity or third party is supervised and has measures in place, to comply with the requirements set out in this Part; and

(ii) where the third party is located outside the Republic, it is regulated and supervised and has measures in place, to comply with requirements equivalent to those set out in this Part.

(3) A reporting entity is deemed to have satisfied the requirements of subsection (2) where the Minister certifies in writing that:

(a) the reporting entity relies on a third party that is part of the same financial group;

(b) the financial group applies customer due diligence, record-keeping and compliance measures that:

(i) meet the requirements of this Act or legal requirements that are to the standard of this Act; and

(ii) assess and respond financial crime; and

(c) the implementation of such policies is supervised at a group level by a competent authority, whether in or outside of the Republic.

(4) Notwithstanding the use of an intermediary entity or a third party, a reporting entity remains liable for any failure to undertake the reporting entity's obligations under this Division.

34 Customer due diligence for existing customers

(1) A reporting entity shall assess an existing customer's information and implement procedures under Subdivisions 2 and 3 where the reporting entity finds that it is necessary to do so for the purposes of mitigating risk.

(2) In making that assessment, the reporting entity shall consider:

(a) any previous due diligence undertaken;

(b) when that due diligence was last undertaken for existing customers; and

(c) the adequacy of the information, documents or data obtained.

35 Prohibition on false accounts

(1) A person shall not:

(a) open or operate an account with a reporting entity where the account is under a false name an anonymous or numbered account or is in a fictitious, false or incorrect name; or

(b) authorise, allow or facilitate the opening or the operation of an account, with a reporting entity where the account is an anonymous or numbered account or is in a fictitious, false or incorrect name.

(2) Where a person is known by 2 or more different names, the person shall not use one of those names in opening an account with a reporting entity where the person has not previously disclosed the other name or names to the reporting entity.

(3) Where a person using a particular name in the person's dealings with a reporting entity discloses to the reporting entity a different name or names by which he or she is commonly known, the reporting entity shall:

(a) make a record of the disclosure; and

(b) at the request of the FIU, give the FIU a copy of that record within 14 working days after receiving the request.

(4) A reporting entity shall not open, operate or maintain any anonymous or numbered account or any account which is in a fictitious, false or incorrect name.

(5) For the purposes of this Section a person opens an account in a false name where the person:

(a) in opening the account, or becoming a signatory to the account, uses a name other than the name by which the person is known; and

(b) does any act in relation to the account, whether by making a deposit, withdrawal or by way of communication with the reporting entity concerned or otherwise and in doing so, uses a name other than the name by which the person is known.

(6) Where before the commencement of this Act, a person opened an account in a false name, the person shall not continue to operate or maintain an account in such false name at the commencement of this Act.

36 Obligation to provide information within 14 days

Where a report is required under this Part to provide information to the FIU, the reporting entity shall provide such information to the FIU within 14 days of receiving the request.

Subdivision 2 – Standard customer due diligence

37 Obligation to identify and verify the identity of customers, agents and beneficial owners

(1) This Section applies to a reporting entity where:

(a) the reporting entity enters into a business relationship with a person;

(b) the reporting entity conducts:

(i) an occasional transaction for a person the value of which is $10,000 or more; or

(ii) a series of isolated transactions that appear to be linked and have a combined value of $10,000 or more; or

(c) the circumstances surrounding a business relationship of the reporting entity or a transaction or series of transactions conducted by the reporting entity give rise to:

(i) a reasonable suspicion of financial crime; or

(ii) a reasonable doubt about the veracity or adequacy of the identification and verification documentation or information the reporting entity had previously obtained.

(2) The reporting entity shall in relation to the following persons identify and verify the person's identity:

(a) the customer of the reporting entity in relation to the applicable activity referred to under subsection (1);

(b) an agent of the customer;

(c) a beneficial owner of the customer; and

(d) a beneficial owner of the property, that is the subject of the business relationship or occasional transaction or series of occasional transactions referred to under subsection (1).

(3) In the case of an agent of the customer referred to under subsection (2), the reporting entity shall also verify the authorisation of the agent to act on behalf of such customer.

(4) Subject to a direction under Section 31(5), the reporting entity shall comply with the requirements of subsection (2) before establishing a business relationship or conducting a transaction or series of transactions.

38 Due diligence for a customer, agent and beneficial owner that is a legal entity established by law or any other instruments

(1) This Section applies to a reporting entity where:

(a) the circumstances referred to under Section 37(1) apply to the reporting entity; and

(b) any of the persons referred to under Section 37(2) is a legal entity.

(2) The reporting entity shall develop and keep a record of its understanding of the nature of the legal entity's business, ownership and control structure.

(3) The reporting entity shall identify and verify:

(a) the laws that regulate and bind the legal entity; and

(b) the name of an individual with a senior management position in the legal entity.

(4) The reporting entity shall identify and take reasonable measures to verify the identity of the beneficial owners of the body through the following information:

(a) the identity of the individual who has a controlling ownership interest in the legal entity;

(b) the identity of the individual exercising control of the legal entity through other means where:

(i) there is doubt as to whether the individual with the controlling ownership interest is the beneficial owner; or

(ii) an individual does not exert control through ownership interests; or

(c) the identity of the individual who holds a position of senior managing official where an individual is not identified under paragraph (a) or (b).

39 Due diligence for customers acting as trustees and related persons

(1) This Section applies to a person who in his or her capacity as a trustee or related person:

(a) enters into a business relationship with a reporting entity; or

(b) in the absence of a business relationship, conducts through a reporting entity:

(i) a transaction with a value of $10,000 or more; or

(ii) a series of linked transactions that have a combined value of $10,000 or more.

(2) A person to whom this Section applies shall report to the reporting entity that he or she is acting as a trustee or related person when:

(a) entering into a business relationship with the reporting entity; or

(b) conducting a transaction or series of transactions.

(3) The reporting entity shall develop an understanding of:

(a) the nature of the trust, including but not limited to the:

(i) settlor of the trust;

(ii) trustee of the trust;

(iii) protector of the trust;

(iv) beneficiary or class of beneficiaries of the trust; and

(v) person exercising ultimate effective control over the trust; and

(b) the control structure of the trust.

(4) The reporting entity shall document its understanding and retain copies of the trust deed and any other document that provides evidence of such understanding.

(5) For the purposes of this Section, ***'related person'*** includes a director, officer, employee or agent of the trustee.

(6) This Section does not apply to a statutory trust established for the purposes of payment of royalties for phosphate and public trusts for management of estates of deceased persons.

40 Obligation to understand occasional transactions

(1) This Section applies to a reporting entity that conducts:

(a) an occasional transaction of the value of $10,000 or more; or

(b) a series of occasional transactions that appear to be linked and have a combined value of $10,000 or more.

(2) The reporting entity shall obtain sufficient information which allows it to understand the transaction or series of transactions and shall document the understanding.

41 Customer due diligence for the beneficiaries of insurance policies

(1) This Section applies to a reporting entity where the reporting entity issues an insurance policy.

(2) Where a beneficiary under the insurance policy is identified as a specifically-named individual or legal entity, the reporting entity shall record the name of the individual or legal entity.

(3) Where a beneficiary under the insurance policy is designated by characteristics or by class or by other means, the reporting entity shall obtain and record sufficient information concerning the beneficiary to satisfy the reporting entity that it will be able to establish the identity of the beneficiary at the time of any payout under the insurance policy.

(4) At the time of any payout to a beneficiary under the insurance policy, the reporting entity shall identify the beneficiary and verify the identity of the beneficiary and any beneficial owner of the beneficiary.

(5) The reporting entity shall file a suspicious activity report with the FIU where the reporting entity is unable to comply with a requirement under subsection (2), (3) or (6).

(6) The reporting entity shall take reasonable measures to determine whether a beneficiary under the insurance policy or any beneficial owner of the beneficiary of any insurance policy issued by it is a politically exposed person.

(7) Where the reporting entity determines that a beneficiary under the insurance policy or any beneficial owner of the beneficiary is a politically exposed person, the reporting entity shall, before making a payment to the beneficiary or beneficial owner:

(a) obtain the approval of senior management to make the payment;

(b) conduct enhanced due diligence in accordance with Section 43 on the business relationship with the beneficiary or beneficial owner; and

(c) consider making a suspicious activity report.

42 Ongoing customer due diligence obligations

(1) A reporting entity shall conduct ongoing due diligence in respect of all of its business relationships.

(2) In conducting ongoing due diligence, a reporting entity shall:

(a) scrutinise transactions carried out on behalf of its customers to ensure that such transactions are consistent with:

(i) the reporting entity's knowledge of its customers;

(ii) the source of its customers' property; and

(iii) the business and risk profile of its customers; and

(b) ensure that documents, data and information collected under the customer due diligence process are kept up-to-date and relevant, by undertaking reviews of existing records.

(3) Additional requirements may be prescribed relating to conducting ongoing customer due diligence.

Subdivision 3 – Enhanced and simplified customer due diligence

43 Enhanced customer due diligence obligations

(1) A reporting entity shall conduct enhanced customer due diligence before or during the course of:

(a) establishing or continuing a business relationship referred to under subsection (2); or

(b) conducting a transaction.

(2) The enhanced customer due diligence obligations apply to a business relationship or transaction where the customer, agent, beneficial owner of the customer or the beneficiary in the case of a life insurance policy:

(a) is a resident of a country:

(i) where there is a high risk of financial crime;

(ii) in which there are no adequate systems in place to prevent or deter financial crime; or

(iii) that is the subject of information provided by the FIU to a reporting entity in accordance with Section 85(k);

(b) is involved in a business activity that involves a high risk of financial crime;

(c) in the case of a body, has an unusual or excessively complex ownership structure which is not proportionate to the nature of the business;

(d) is a politically exposed person;

(e) could, in the circumstances, be suspected on reasonable grounds to be involved in financial crime, either within or outside of the Republic; or

(f) satisfies any other criteria published or provided by the FIU that is determined to be high-risk by the FIU.

(3) The enhanced customer due diligence obligations also apply to a reporting entity where the reporting entity is required to conduct further analysis under Section 61.

(4) The reporting entity shall establish and use systems and processes to determine whether any of the circumstances referred to in subsection (2) or (3) are present in relation to a business relationship or a transaction.

(5) In conducting enhanced customer due diligence, the reporting entity shall:

(a) obtain senior management approval before:

(i) establishing the business relationship or continuing the business relationship where it already exists; or

(ii) conducting the transaction;

(b) take reasonable measures to establish that financial crime is not involved in the procurement or proposed use of the:

(i) wealth of the customer or beneficial owner of the customer for the business relationship; or

(ii) funds for the transaction;

(c) keep a record of the measures taken under any previous requirement and record the findings made;

(d) file a suspicious activity report; and

(e) conduct enhanced ongoing monitoring of the business relationship to assess whether expenditure is occurring in a manner consistent with a legitimate process of expenditure given the reporting entity's understanding of the customer.

(6) In subsection (5)(b), ***'reasonable measures'*** may include:

(a) obtaining additional information about the customer, such as occupation, volume of assets, and information available through public databases and the internet and updating more regularly the identification data of the customer or beneficial owner;

(b) obtaining additional information on the intended nature of the business relationship;

(c) obtaining information on the source of funds or source of wealth of the customer;

(d) obtaining information on the reasons for intended or performed transactions; or

(e) requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar customer due diligence standards.

(7) In undertaking enhanced customer due diligence, the reporting entity shall have regard to any guidance provided or published by the FIU in relation to enhanced customer due diligence.

(8) Additional requirements relating to conducting enhanced customer due diligence may be prescribed by regulations.

44 Enhanced customer due diligence deemed not completed

(1) Where the reporting entity is unable to establish the matters referred to under Section 43(5)(b), enhanced customer due diligence is deemed not completed.

(2) Where enhanced customer due diligence is deemed not completed, the reporting entity shall comply with the requirements of Section 31.

45 Simplified customer due diligence obligations

(1) Simplified due diligence obligations and requirements shall be met by reporting entities as may be prescribed.

(2) Simplified due diligence shall not be undertaken where there is a suspicion of money laundering or terrorist financing or where higher-risk scenarios as may be prescribed apply.

Subdivision 4 – Due diligence in relation to correspondent banking relationships and shell banks

46 Correspondent banking due diligence

(1) Before entering into a business relationship or isolated transaction that involves correspondent services, a reporting entity shall:

(a) assess the suitability of the respondent entity by taking the steps outlined in subsection (2);

(b) ensure that a member of senior management approves establishing the correspondent services relationship; and

(c) clearly understand and document the respective AML/CFT responsibilities of each respondent entity.

(2) A reporting entity shall in relation to correspondent banking due diligence take the following steps:

(a) obtain sufficient information about the respondent entity to understand fully the nature of its business;

(b) determine from publicly available information:

(i) the reputation of the respondent entity;

(ii) the quality of the supervision to which it is subject; and

(iii) whether it has been subject to investigation or regulatory action in respect of financial crime; and

(c) assess the respondent entity's financial crime controls and ascertain whether they are adequate and effective.

(3) Where the correspondent services involve a payable-through account, the reporting entity shall be satisfied that the respondent entity:

(a) has taken customer due diligence measures to the standard required by this Act with respect to every customer having direct access to the account; and

(b) will provide the reporting entity with the relevant evidence of identity upon request.

(4) For the purposes of this Section, ***'correspondent services'*** means banking services provided by a bank in the Republic to a respondent entity in another country.

47 Shell banks

(1) A reporting entity shall not establish, continue or conduct a business relationship or occasional transaction with a shell bank.

(2) A reporting entity shall take appropriate measures to satisfy itself that its respondent entities do not permit their accounts to be used by shell banks.

Subdivision 5 – Enforcement

48 Offence for contravention under this Division

A reporting entity which contravenes any provision of this Division commits an offence and shall be liable upon conviction:

(a) for an individual, to a fine not exceeding $200,000 or imprisonment for a term not exceeding 10 years, or to both; or

(b) for a body corporate, to a fine not exceeding $1,000,000.

Division 4 – Obligations of financial institutions in relation to electronic currency transfers

49 Application of Division

This Division applies to a reporting entity which is a financial institution.

50 Overview of customer due diligence for electronic currency transfers

(1) A reporting entity is not required to verify the identity of a person under Sections 52 to 55, where the reporting entity has previously identified the identity of a person:

(a) for the purposes of carrying out customer due diligence under Division 3 of this Part; or

(b) under any other provision of this Act.

(2) Subsection (1) does not apply where there are reasonable grounds for the reporting entity to doubt the adequacy or accuracy of the documents, data or information previously obtained.

51 Records for electronic currency transfers

A reporting entity shall maintain records of the information required to be obtained under this Division for electronic currency transfers in accordance with Sections 28 and 29.

52 Requirements for originating entity-electronic currency transfer

(1) This Section applies to a reporting entity, where the entity is an originating entity for an electronic currency transfer of an amount in currency equal to or greater than $1,000.

(2) The originating entity shall identify the sender of the transfer by obtaining the following identity information:

(a) the sender’s full name;

(b) any one of:

(i) the sender's account number;

(ii) a unique transaction reference number where the sender does not have an account; or

(iii) such other identifying information prescribed by the regulations that allows the transaction to be traced back to the sender; and

(c) any one of the sender's:

(i) address;

(ii) customer identification or account number;

(iii) date of birth;

(iv) passport number; or

(v) any other prescribed form of identity.

(3) The originating entity shall, in the case of a domestic electronic currency transfer, provide the information specified in subsections (2)(a) and (c) within 3 working days after:

(a) the request is made by the beneficiary entity to execute the electronic currency transfer; or

(b) the FIU makes a request to the originating entity for that information.

(4) The originating entity shall, in the case of an international electronic currency transfer, identify the receiver of the electronic currency transfer by obtaining the following identity information:

(a) the receiver's full name; and

(b) any one of:

(i) the receiver's account number;

(ii) a unique transaction reference number where the receiver does not have an account; or

(iii) such other identifying information as may be prescribed that allows the transaction to be traced back to the receiver.

(5) An originating entity shall:

(a) verify the sender's identity so that it is satisfied that the information obtained under subsection (2) is correct; and

(b) verify the sender's identity before ordering the electronic currency transfer.

(6) Where several international electronic currency transfers from a single sender are put in one file for transmission to multiple receivers, the originating entity shall ensure that the file contains the:

(a) required and verified sender information and required receiver information that is traceable within the receiver country; and

(b) sender's account number or such other information as may be prescribed that allows the transaction to be traced back to the sender.

(7) An originating entity shall transmit with the electronic currency transfer to an intermediary entity:

(a) the identity information about the sender that it had obtained under subsection (2) and verified under subsection (5); and

(b) in the case of an international electronic currency transfer, the identity information about the receiver that it had obtained under subsection (4).

(8) An originating entity shall not execute a currency transfer where the information requirements under subsections (2) and (5) are not met.

(9) An originating entity shall retain records of all sender and receiver information that accompanies an electronic currency transfer and shall comply with the record keeping requirements in this Part.

53 Requirements for originating entity-electronic currency transfer of less than $1,000

(1) This Section applies to a reporting entity that is an originating entity for an international electronic currency transfer of an amount in currency less than $1,000.

(2) In identifying the sender of the transfer, an originating entity shall obtain the following identity information:

(a) the name of the sender; and

(b) the sender's account number or such other information as may be prescribed which allows the transaction to be traced back to the sender.

(3) In identifying the receiver of the transaction, an originating entity shall obtain the following identity information:

(a) the name of the receiver; and

(b) the receiver's account number or such other identifying information as may be prescribed that allows the transaction to be traced back to the receiver.

(4) Where the circumstances are such as to give rise to a reasonable suspicion of financial crime, the originating entity shall:

(a) verify the information obtained in relation to the sender; and

(b) file a suspicious activity report.

(5) An originating entity shall transmit with the electronic currency transfer, the information the originating entity had obtained under subsections (2) and (3) to an intermediary entity.

(6) An originating entity shall not execute the currency transfer where the originating entity cannot meet the information requirements under subsections (2), (3) and (4).

54 Requirements for intermediary entity-electronic currency transfer

(1) This Section applies to a reporting entity where the reporting entity is an intermediary entity for an electronic currency transfer.

(2) An intermediary entity shall transmit the identity information that it receives from the originating entity under Sections 52 or 53 with the electronic currency transfer.

(3) An intermediary entity shall take reasonable measures to identify international electronic currency transfers that lack any of the information required under Section 52.

(4) An intermediary entity shall have risk-based policies and procedures for determining when to:

(a) execute, reject or suspend an electronic currency transfer which lacks any of the information required under Section 52 to accompany the transfer; and

(b) take follow up action and the nature of such action.

(5) An intermediary entity shall retain records of all sender and receiver information that accompanies an electronic currency transfer in accordance with the record keeping requirements in this Part.

55 Requirements for beneficiary entity-electronic currency transfer

(1) This Section applies to a reporting entity where the reporting entity is a beneficiary entity for an electronic currency transfer.

(2) In the case of an electronic currency transfer of an amount in currency equal to or greater than $1,000, a beneficiary entity shall verify the receiver's identity and satisfy itself that the information obtained by an originating entity under Section 52(4) is correct.

(3) A beneficiary entity shall use reasonable measures to identify international electronic currency transfers that lack any of the information required under Sections 52 and 53 to accompany an international electronic currency transfer.

(4) A beneficiary entity shall have risk-based policies and procedures for determining when to:

(a) execute, reject or suspend an electronic currency transfer which lacks any of the information required under Sections 52 and 53 to accompany the transfer; and

(b) take follow up action and the nature of such action.

(5) A beneficiary entity shall retain records of all sender and receiver information that accompany an electronic currency transfer and shall comply with the record keeping requirements in this Part

56 Additional information may be prescribed

The Cabinet may make regulations prescribing additional information required to be provided by reporting entities in fulfilment of their obligations under this Division.

57 Requirements for reporting entities controlling the sending and receiving side of an electronic currency transfer

(1) This Section applies to a reporting entity that provides a money or value transfer service.

(2) Where a reporting entity controls both the sending and the receiving side of an electronic currency transfer, the reporting entity shall consider all information required to be obtained under Sections 52 to 54 relating to the sender and the receiver in order to determine whether to file a suspicious activity report.

(3) Where the reporting entity determines that a suspicious activity report should be filed the reporting entity shall:

(a) file the report in any country affected by the electronic currency transfer; and

(b) make all relevant transaction information available to the relevant authorities in the country affected.

(4) A reporting entity shall have policies and procedures in place to ensure that it does not contravene the requirements of Part 7.

58 Offence for contravention under this Division

A person or reporting entity which contravenes any provision of this Division commits an offence and shall be liable upon conviction:

(a) for an individual, to a fine not exceeding $200,000 or imprisonment for a term not exceeding 10 years or to both; or

(b) for a body corporate, to a fine not exceeding $1,000,000.

Division 5 – Reporting obligations in relation to suspicious activity

59 Obligation to report suspicious activity

(1) This Section applies to a reporting entity where the reporting entity:

(a) knows or suspects on reasonable grounds that:

(i) any transaction conducted by or through the reporting entity or attempted transaction may be related to the commission of financial crime or criminal conduct;

(ii) an account or business relationship with the reporting entity or an account or business relationship that is attempted to be established with the reporting entity, may be related to the commission of a financial crime or criminal conduct;

(iii) any activity conducted by or through the reporting entity or attempted activity may be related to the commission of financial crime or criminal conduct;

(iv) any property related to any transaction, account, business relationship or activity is criminal property;

(v) the reporting entity has information that may be relevant to an act related to the commission of a financial crime;

(vi) the reporting entity has information that may be relevant to an investigation or prosecution of a person for financial crime or criminal conduct or may be of assistance in the enforcement of the laws of the Republic; or

(vii) a series of transactions conducted by or through the reporting entity or attempted transactions have been structured in such a way as to avoid reporting obligations under this Division; or

(b) is required under another provision of this Part to make a suspicious activity report.

(2) The reporting entity shall have regard to any applicable guidance published or provided by the FIU in assessing whether one or more of the circumstances referred to in subsection (1) has occurred.

(3) Subsequent to the occurrence of one of the circumstances referred to in subsection (1), the reporting entity shall no later than 2 working days after its occurrence submit a suspicious activity report to the FIU.

(4) The report shall:

(a) be in such form, contain such details and be provided to the FIU in such manner as may be prescribed; and

(b) be prepared with regard to any applicable guidance published or provided by the FIU.

(5) The FIU may request further information from a reporting entity in relation to a report provided to the FIU under this Section.

(6) Upon receiving the request under subsection (5), a reporting entity shall, within 14 working days give the FIU any further information that the reporting entity has about any of the circumstance referred to in subsection (1).

60 Suspicious activity report not filed

Where a reporting entity is required by this Part to consider making a suspicious activity report but decides not to do so, the reporting entity shall record the circumstances and reasons for its decision.

61 Obligation to analyse suspicious activity

(1) A reporting entity that knows or suspects on reasonable grounds that any of the circumstances provided in Section 59(1)(a) has occurred, shall conduct further analysis to confirm or refute the relevant suspicion.

(2) The reporting entity shall provide the results of the further analysis to the FIU.

(3) Where the analysis does not refute the suspicion, the reporting entity shall conduct enhanced due diligence in accordance with Section 43 and report that it has undertaken enhanced due diligence to the FIU.

(4) The reporting entity must provide the results of the further analysis under subsection (3) to the FIU within 14 days or such longer period as the FIU allows in writing, after the suspicious activity report is made.

62 Obligation to report certain transactions

(1) This Section applies to a reporting entity where the reporting entity is requested to conduct:

(a) an international electronic currency transfer;

(b) a domestic electronic currency transfer to the value of $10,000 or more;

(c) any transaction involving cash to the value of $10,000 or more; or

(d) a series of transactions which have been structured in a manner that causes reasonable suspicion to have been structured to avoid meeting the threshold referred to in paragraph (b) or (c).

(2) The reporting entity shall make a report of the transfer, transaction or series of transactions to the FIU within 7 days after conducting such transfer, transaction or series of transactions.

(3) The report shall be:

(a) in such form, contain such details and be transmitted to the FIU in such manner as may be prescribed; and

(b) prepared with regard to any applicable guidance published or provided by the FIU.

(4) The FIU may request further information from a reporting entity in relation to a report provided to the FIU under this Section.

(5) Upon receiving the request under subsection (4), a reporting entity shall, within 14 working days give the FIU any further information that the reporting entity has about the transfer, transaction or series of transactions or the parties related to such activity or attempted activity.

63 FIU direction in relation to a report made under this Division

(1) Where a reporting entity has made a suspicious activity report under Section 59 or a report under Section 61 to the FIU, the FIU may issue a written direction to the reporting entity directing the manner in which the activity or attempted activity or property, the subject of the report shall be dealt with by the reporting entity.

(2) Without limiting subsection (1), the FIU may direct that the reporting entity shall:

(a) not continue further with the customer due diligence;

(b) not continue further with the business relationship or transaction;

(c) conduct enhanced due diligence;

(d) conduct enhanced monitoring of the business relationship or transaction; or

(e) conduct any other course of action specified by the FIU in the direction.

64 Obligation of supervisory authority or auditor to report suspicious activity

(1) This Section applies where a supervisory authority or an auditor of a reporting entity has reasonable grounds to suspect that information that it has concerning any activity or attempted activity may:

(a) be relevant to an investigation or prosecution of a person or persons for a financial crime or criminal conduct;

(b) be of assistance in the enforcement of this Act;

(c) be related to the commission of financial crime or criminal conduct; or

(d) amount to a financial crime.

(2) The supervisory authority or the auditor of the reporting entity shall report the activity or attempted activity to the FIU.

(3) The supervisory authority or the auditor shall comply with the requirements of Section 59(2) to (6) as if it were a reporting entity.

65 False or misleading statements

Where a person makes a suspicious activity report under Section 59 or 64, or a report under Section 61, the person shall not:

(a) include in the report or any associated communications with the FIU any statement that the person knows or ought to know, is false or misleading in any particular; or

(b) omit from the report or associated communications with the FIU any matter or thing the person knows or ought to know would result in a statement which is false or misleading in a material particular.

66 Obligation not to disclose suspicious activity reports and related information

(1) This Section applies to:

(a) a reporting entity;

(b) an auditor or supervisory authority of a reporting entity;

(c) a director of the reporting entity;

(d) an officer, employee or agent of the reporting entity acting in the course of his or her employment or agency; and

(e) a person who was previously a person referred to in paragraphs (a) to (d).

(2) Where a person who knows of or suspects on reasonable grounds any of the matters referred to in Section 59(1), has occurred or has received a request

under Section 62(4), the person shall not, apart from complying with the reporting obligations under this Act, disclose to any other person:

(a) the knowledge or suspicion;

(b) any details of the request;

(c) that a report under this Act has been or may be, made to the FIU;

(d) that other information required under this Act has been or may be given, to the FIU;

(e) the contents or likely contents of any report under this Act relating to that suspicious activity; and

(f) information that might identify any person who has:

(i) handled that suspicious activity;

(ii) prepared any report regarding that suspicious activity; or

(iii) provided any information to the FIU regarding that suspicious activity.

(3) A person to whom this Section applies shall not intentionally do any act which by word or conduct, may cause another person to infer any of the circumstances set out in subsection (2).

(4) Subsection (2) does not apply to a disclosure made:

(a) to a person who has made or is required to make, a report or provide information under this Act for any purpose connected with the performance of that person's duties relating to this Act;

(b) to a lawyer for the purpose of obtaining legal advice or representation in relation to the disclosure;

(c) to a supervisory authority or auditor of the relevant reporting entity;

(d) to the FIU or any person assisting the FIU in the performance of its duties;

(e) to any police officer engaged in the investigation of a financial crime; or

(f) for the purposes of discouraging the customer from engaging in conduct that constitutes or may constitute as:

(i) evasion of a tax or law that deals with tax; or

(ii) an offence against a law of the Republic.

(5) Subject to subsection (6) a person who receives information in accordance with subsection (4), shall keep such information confidential.

(6) Nothing in this Section prevents a person from disclosing information to a court where:

(a) the person discloses the information for the purposes of or in the course of, any proceedings before the court; and

(b) the court is satisfied that it is necessary in the interests of justice for that person to disclose the information.

67 Offence for contravention under this Division

A reporting entity or person which contravenes any provision of this Division, commits an offence and shall be liable upon conviction:

(a) for an individual, to a fine not exceeding $200,000 or imprisonment for a term not exceeding 10 years or to both; or

(b) for a body corporate, a fine not exceeding $1,000,000.

PART 5 – FINANCIAL INTELLIGENCE UNIT

Division 1 – Financial Intelligence Unit

68 Continuance of the Financial Intelligence Unit

The Financial Intelligence Unit established by Section 7 of the *Anti-Money Laundering Act* 2008 shall continue in existence within the Department of Justice and Border Control.

69 Functions of the Financial Intelligence Unit

(1) The FIU shall have the following functions:

(a) to enforce this Act;

(b) to supervise the compliance of reporting entities with this Act;

(c) to receive and analyse suspicious activity reports and other information available to it, whether by any means or under any law, in order to identify activity that may constitute or may relate to a financial crime or criminal conduct and to carry out any further investigations it considers necessary;

(d) to disseminate information derived from analysis and reports of information received under paragraph (c) to domestic and foreign law enforcement bodies or foreign intelligence bodies;

(e) to enquire into conduct that constitutes as or relates to financial crime or is suspected to do so;

(f) to conduct related inquiries, investigations, analysis and oversight;

(g) to identify, analyse and assess on an ongoing basis financial crime trends, patterns and risks of relevance to the Republic, including in relation to new technologies, business practices and products;

(h) to coordinate with supervisory authorities and other authorities in the Republic that have a role in combatting financial crime or criminal conduct;

(i) to engage in an arrangement, understanding or any mutual cooperation with similar foreign entities in other countries or international bodies on matters relating to financial crime or criminal conduct;

(j) where necessary, may commence proceedings in any court established in the Republic for the purposes of enforcing any part of this Act or any other written law, in the performance of its functions;

(k) to ensure that reporting entities, supervisory authorities, other competent authorities and the public at large are adequately informed about the trends, patterns and risks of financial crime and the appropriate responses; and

(l) such other functions which may be given to the FIU by any written law, the Cabinet or the Minister.

(2) The Financial Intelligence Unit shall have all such powers that are necessary to give effect to or for carrying out its functions under subsection (1).

70 Office of the Supervisor of FIU

(1) There shall be a Financial Intelligence Supervisor who shall be the head of the FIU.

(2) The Supervisor shall be appointed by the Minister in consultation with the Cabinet.

(3) The terms and conditions of the office of the Supervisor shall be determined by the Cabinet.

(4) The Supervisor shall be appointed for a period of 3 years and may be reappointed for any further term.

(5) The Supervisor reports to the Secretary.

71 Appointment of officers of the FIU

(1) Subject to subsection (3), the Chief Secretary in consultation with the Secretary shall, in writing, appoint an officer of the FIU on such terms and conditions determined in consultation with the Supervisor.

(2) Subject to subsection (3), the Supervisor may, in writing, appoint an authorised person to exercise powers, duties and functions of the FIU specified in the authorisation, subject to the direction and supervision of the Supervisor or such other person as the Supervisor specifies in such authorisation.

(3) A person appointed under subsection (1) or (2) shall be endorsed by the Supervisor as having the necessary security clearance levels and understanding of his or her roles and functions, including his or her responsibilities in handling and disseminating sensitive and confidential information, before his or her appointment.

(4) An officer of the FIU may exercise all of the functions, duties and powers, of the FIU under this Part, subject to the direction and supervision of the Supervisor.

(5) An authorised person is deemed to be an officer of the FIU when acting within the scope of the authorisation.

(6) An officer of the FIU and an authorised person shall report to the Supervisor on the exercise of his or her powers and functions and advise the Supervisor on any matter relating to financial crime or criminal conduct.

72 Removal of the Supervisor from office

(1) Subject to subsection (2) the Cabinet may terminate or suspend the Supervisor from office where the Cabinet is satisfied that the Supervisor:

(a) has a physical or mental incapacity that affects the performance of his or her duty;

(b) neglected his or her duty;

(c) is incompetent;

(d) has committed a misconduct whether or not such amounts to the breach of any law; or

(e) has committed conduct that brings the FIU or the Republic into disrepute.

(2) Before the Cabinet may consider removing the Supervisor, the allegation against him or her shall be conducted before the Resident Magistrate.

(3) The Resident Magistrate shall conduct such hearing as may be necessary and report his or her findings to the Secretary to the Cabinet and the Secretary.

(4) The Supervisor shall be accorded with the right of natural justice before the Resident Magistrate.

(5) Where the Supervisor shall be removed for physical or mental incapacity, a health practitioner with requisite qualification shall provide a medical report of the Supervisor's incapacity and that such incapacity will impair him or her from performing the functions or exercising the powers of the office.

73 Immunity of Supervisor and officers of FIU for acting in good faith

The Supervisor and officers of the FIU acting under this Act or any other written law, shall not be liable for any criminal, civil or administrative liability for act done or ordered to be done in the discharge of the functions and powers, whether or not within the limits of his or her functions or powers, provided that he or she at the time in good faith believed himself or herself to have the requisite functions and powers.

74 Independence of the Financial Intelligence Unit

(1) The FIU shall perform all such functions and exercise all such powers under this Act or any other written law independently.

(2) The Secretary shall from time to time issue administrative directions to the FIU.

(3) The Supervisor and other officers of the FIU report to the Secretary for administrative purposes.

(4) For avoidance of doubt, no person shall give directions or obstruct the FIU from acting independently in carrying out its functions and powers under this Act.

(5) The FIU shall have its own budget as part of the budget of the Department for Justice and Border Control and the budget shall be utilised as required under the *Public Finance (Control and Management) Act 1997* and the respective appropriation law.

75 Annual audit of the FIU by Auditor General

(1) The FIU shall be subject to examination and audit by the Auditor General, conducted pursuant to the *Audit Act 1973*.

(2) The Auditor General or any person acting on behalf of or under the direction of the Auditor General shall not use or disclose any information obtained or to which they have had access to in the course of an audit.

(3) Subsection (2) does not apply to a disclosure required for the purposes of exercising powers or performance of functions under the *Audit Act 1973*.

76 Annual Report of the FIU

(1) The FIU shall submit an Annual Report to the Minister within 3 months from the end of the financial year.

(2) The Minister shall present the report to the Cabinet no later than 30 days from the receipt of the report.

(3) The format and content of the annual report of the FIU shall be determined by the Supervisor in consultation with the Secretary.

Division 2 – Powers of the Financial Intelligence Unit

Subdivision 1 – Powers to monitor compliance

77 Powers relating to information exchange with domestic authorities

The FIU shall have the power:

(a) to collect any information that the FIU considers relevant to financial crime or criminal conduct, whether or not publicly available, including information from commercially available databases and databases maintained by the Government;

(b) to request information from any law enforcement agency, supervisory authority or instrumentality; and

(c) to enter into any agreement or arrangement with any domestic law enforcement agency, supervisory authority or instrumentality regarding the exchange and sharing of information.

78 Power to conduct inspection

(1) The FIU may with notice conduct an inspection in person or by way of requesting the furnishing of documents or information of a reporting entity for the purposes of:

(a) monitoring the reporting entity's compliance; and

(b) enforcement of this Act and combatting terrorism and proliferation financing.

(2) Without limiting subsection (1), an inspection includes:

(a) an examination of the records of the reporting entity;

(b) making inquiries concerning the business and affairs of the reporting entity;

(c) the power to enter property for the purposes of conducting an examination;

(d) a review of the reporting entity's procedures, systems and controls; and

(e) a review of the business risk assessment produced by the reporting entity and its AML/CFT compliance program and policies.

(3) For the purposes of subsection (1), an authorised officer of the FIU may:

(a) at any reasonable time enter any premises, in which the officer reasonably believes contain records relevant to ensuring compliance with this Act;

(b) use or cause to be used any computer system or data processing system in the premises to examine any data contained in or available to the system;

(c) reproduce any record or cause it to be reproduced from the data, in the form of a printout or other intelligible output and remove the printout or other output for examination or copying;

(d) use or cause to be used any copying equipment in the premises to make photocopies, electronic or digital copies of any records; and

(e) request information from any officer or employee of the reporting entity.

(4) The powers set out in this Section shall be exercised only so far as is reasonably necessary to confirm compliance, by the reporting entity, with this Act.

(5) The owner, occupier or any person found to be lawfully in control of the premises referred to in subsection (3)(a) shall:

(a) give any officer of the FIU all reasonable assistance to enable them to carry out their responsibilities; and

(b) furnish an officer of the FIU with any information that they may reasonably require for the purposes of this Act.

(6) The FIU may transmit any information from or derived from, an inspection to the appropriate law enforcement authorities or supervisory authorities where the FIU has reasonable grounds to suspect that the information is:

(a) suspicious;

(b) relevant to an investigation for non-compliance with the financial crime or criminal conduct; or

(c) relevant to the duties and functions of the law enforcement or supervisory authority in question.

(7) A person shall not obstruct, hinder or fail to cooperate with the FIU in the lawful exercise of the powers under subsection (1), (2), (3) or (5).

(8) A person who contravenes subsection (7), commits an offence and shall be liable upon conviction:

(a) for an individual, to a fine not exceeding $20,000 or imprisonment of not more than 2 years or to both; or

(b) for a senior management of a body corporate, to a fine not exceeding $100,000 or imprisonment of not more than 5 years, or to both.

79 Power to require reporting entity to produce certain information

(1) For the purpose of this Act, the FIU may require a reporting entity to provide information to the FIU relating to the reporting entity's obligations under this Act.

(2) The information includes but is not limited to:

(a) copies of internal policies, procedures and control measures relevant to detection and prevention of financial crime and criminal conduct;

(b) copies of business risk assessments relevant to risks of financial crime and criminal conduct;

(c) copies of training material related to detection and prevention of financial crime provided by the reporting entity to its directors, officers, employees and agents;

(d) copies of results, reports or other information from independent testing and auditing of a reporting entity's internal policies, procedures and control measures relevant to detection and prevention of financial crime or criminal conduct; and

(e) statistical information relating to a reporting entity's products or services, customer base or transaction types.

(3) Subject to subsection (4), the FIU shall give a reporting entity written notice of when it shall provide the information required under subsection (1) and the reporting entity shall provide the information within the period specified in the notice which must be at least 14 working days after the date of the notice.

(4) The FIU may require a reporting entity to report information under this Section to the FIU on an annual or bi-annual basis and in such form as required by the FIU.

(5) A reporting entity shall not:

(a) fail to provide the information required under this Section;

(b) provide information that the reporting entity knows is false or misleading in a material particular; or

(c) fail to comply with subsection (3) or (4).

(6) A reporting entity which contravenes subsection (5) commits an offence and shall be liable upon conviction:

(a) for an individual, to a fine not exceeding $20,000 or imprisonment for a term not exceeding 2 years or to both; or

(b) for a senior management of a body corporate, to a fine not exceeding $100,000 or imprisonment of not more than 5 years, or to both.

80 Power to require certain persons to produce information relating to business relationships, accounts and transactions

(1) This Section applies to information relating to:

(a) a business relationship with a reporting entity;

(b) an account with a reporting entity or the property held in or transacted through such an account; or

(c) a transaction conducted by or through a reporting entity.

(2) The FIU may require any or all of the following persons to provide information under subsection (1):

(a) a customer of the reporting entity for the business relationship, account or transaction concerned;

(b) a beneficial owner of the customer;

(c) a beneficial owner of any of the property the subject of the business relationship, account or transaction; or

(d) a director, officer, employee or agent of any person referred to in paragraph (a), (b) or (c).

(3) The FIU shall give the person written notice of when the person shall provide the information and the person shall provide such information within the period specified in the notice which shall be at least 14 working days after the date of the notice.

(4) A person shall not:

(a) fail to provide the information;

(b) provide relevant information that the person knows is false or misleading in a material particular; or

(c) fail to comply with subsection (3).

(5) A person who contravenes this subsection (4) commits an offence and shall be liable upon conviction:

(a) for an individual, to a fine not exceeding $20,000 or imprisonment for a term not exceeding 2 years or to both; or

(b) for a senior management of a body corporate, to a fine not exceeding $100,000 or imprisonment of not more than 5 years, or to both.

Subdivision 2 – Powers to enforce compliance

81 Performance orders

(1) The FIU may apply to the Supreme Court for an order requiring a person to do an act to comply with this Act, which shall be commenced by way of a civil proceeding.

(2) The Supreme Court may grant an order requiring a person to do an act under this Act where it is satisfied that:

(a) a person has refused or failed to do an act; and

(b) the refusal or failure is a contravention of this Act.

(3) An order granted by the Supreme Court under subsection (2) may relate to an officer, employee or agent of the person.

(4) An application made under subsection (1) may be made *ex parte* and the Supreme Court may grant an interim order under subsection (2).

(5) For the purposes of this Section, the *Civil Procedure Rules 1972* or any other rules of the Supreme Court shall apply.

82 Restraining injunctions

(1) The FIU may apply to the Supreme Court for an injunction restraining a person from engaging in conduct in contravention of this Act, which shall be commenced by way of a civil proceeding.

(2) The Supreme Court may grant an injunction restraining a person from engaging in conduct that contravenes this Act where it is satisfied that:

(a) a person has engaged in any conduct; and

(b) the conduct is a contravention of this Act.

(3) An injunction under subsection (2) may relate to a director, officer, employee or agent of the person.

(4) An application made under subsection (1) may be made *ex parte* and the Supreme Court may grant an interim injunction under subsection (2).

(5) For the purposes of this Section, the *Civil Procedure Rules 1972* or any other rules of the Supreme Court shall apply.

83 Relationship between offences and other enforcement measures

Criminal proceedings for an offence under this Act may be commenced against a person in relation to conduct, whether or not an action to impose a non-criminal enforcement measure under this Subdivision has been commenced against the person, in relation to the same or substantially the same conduct.

Subdivision 3 – Duties of the Financial Intelligence Unit and other supervisory authority

84 Statistics and records

(1) The FIU shall maintain all records relating to its activities for at least 7 years.

(2) The FIU shall maintain statistics on the effectiveness and efficiency of the Republic's framework for anti-money laundering and combatting the financing of terrorism and other financial crime, including in relation to:

(a) suspicious activity reports received and disseminated;

(b) financial crime investigations, prosecutions and convictions;

(c) property frozen, seized and confiscated; and

(d) mutual legal assistance or other international requests for co-operation made and received.

85 Guidance and feedback

The FIU shall for the purpose of assisting reporting entities, issue guidelines to reporting entities in relation to their obligations under this Act, including:

(a) customer identification;

(b) record keeping and reporting obligations;

(c) identifying suspicious transactions or suspicious activities;

(d) provide training programmes and training to reporting entities in relation to their obligations under this Act;

(e) provide feedback to reporting entities and other relevant agencies relating to their compliance with this Act;

(f) ensure that reporting entities, supervisory authorities and other relevant authorities are aware of financial crime trends, patterns and risks of relevance to the Republic, including in relation to new technologies, business practices and products;

(g) publicise new developments, including information on current techniques, methods and trends in financial crime;

(h) inform reporting entities on the circumstances that give rise to an obligation to conduct enhanced due diligence in accordance with Section 43;

(i) detail appropriate procedures and controls to prevent the misuse of technological developments for the purposes of financial crime;

(j) inform reporting entities about weaknesses in the systems relating to anti-money laundering or combatting the financing of terrorism of other countries; and

(k) educate the public and create awareness on matters relating to financial crime, in particular in the context of the Republic.

86 Protection and dissemination of information

(1) The FIU shall establish rules and policies relating to the protection and dissemination of information.

(2) Any rules and policies established under subsection (1) shall be published in the Gazette.

87 Non-disclosure

(1) This Section applies to a person while the person is or after the person ceases to be, the Supervisor or an officer of the FIU.

(2) A person to whom this Section applies shall not disclose any knowledge, information or matter which has been obtained by him or her in the performance of his or her duties or functions or the exercise of his or her powers, under this Act.

88 Fit and proper person controls

(1) A supervisory authority shall ensure that:

(a) it verifies and maintains up to date records of the beneficial ownership and control and the source of funds used to pay the capital of the reporting entities it supervises; and

(b) it makes beneficial ownership and control information of the reporting entities it supervises available to the FIU when requested.

(2) A supervisory authority shall ensure that the following are fit and proper persons to hold those positions on an initial and ongoing basis:

(a) the directors, chief executives, senior managers or persons in other equivalent positions in the reporting entity; and

(b) the beneficial owners of the reporting entity.

(3) The FIU or the supervisory authority may determine and publish fit and proper criteria for the purpose of subsection (2).

Subdivision 4 – International cooperation

89 International cooperation

(1) The FIU may cooperate with foreign governments and international organisations on matters related to its functions or powers, including to:

(a) request information;

(b) receive requests for information; and

(c) receive or provide information.

(2) The FIU shall not refuse a request for assistance from a foreign government or international organisation on any of the following grounds:

(a) the request is considered to involve fiscal matters;

(b) laws require reporting entities to maintain secrecy or confidentiality, except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies;

(c) there is an inquiry, investigation or proceeding underway in the requesting country, unless the assistance would impede that inquiry, investigation or proceeding; and

(d) the nature or civil, administrative, law enforcement or other status of the requesting counterpart authority is different from that of its foreign counterpart.

(3) The FIU may refuse a request for assistance where in the opinion of the FIU the requesting foreign government or international organisation is not adequately able to protect the confidentiality of any information that has been requested.

90 Disclosure of reports and information to certain foreign bodies

(1) The FIU may disclose to a foreign financial intelligence body or a foreign law enforcement body any or all of the following:

(a) a report prepared or causes to be prepared by the FIU or received by the FIU;

(b) any information derived from the report;

(c) any analysis the FIU conducts or causes to be conducted; or

(d) any other information the FIU receives.

(2) A disclosure made under subsection (1) shall be made on the basis of the FIU's assessment, where it is satisfied there are reasonable grounds to suspect that the report, information or analysis would be relevant to any of the purposes set out under subsection (3).

(3) The reference to purposes in subsection (2) are for:

(a) investigating or prosecuting financial crime, an offence that is substantially similar to an offence constituting a financial crime, or criminal conduct;

(b) detecting, investigating or prosecuting any other offence under the law of any country;

(c) enforcing or taking action under a law relating to proceeds of crime in any country; or

(d) supervising and enforcing compliance with this Act or combatting the financing of terrorism in any country.

(4) The FIU shall disclose any such report, information or analysis on such terms and conditions as are set out in the relevant arrangement or understanding entered into under Section 91 between the FIU and the foreign financial intelligence body or foreign law enforcement body.

(5) Where an arrangement or understanding under Section 91 has not been entered into, the FIU may disclose any report, information or analysis on such terms and conditions as may be agreed upon by the FIU and the foreign financial intelligence body or foreign law enforcement body at the time of the disclosure.

(6) The agreed terms and conditions referred to in subsection (4) shall include:

(a) restrictions on the use of the report, information or analysis for the purposes referred to in subsection (3);

(b) a stipulation that the report, information or analysis is to be treated in a confidential manner and not to be further disclosed without the express consent of the FIU; and

(c) provisions concerning the uses to which the report, information or analysis may be put and the other bodies with which the information may be shared.

91 Power to enter into arrangement or understanding with certain foreign financial intelligence bodies

(1) The FIU may, with the approval of the Cabinet, enter into an arrangement or understanding with a foreign financial intelligence body or a foreign law

enforcement body regarding the exchange of reports, information or analysis between the FIU and the foreign financial intelligence body or the foreign law enforcement body.

(2) The report, information or analysis exchanged under subsection (1) shall be a report, information or analysis that the FIU, the foreign financial intelligence body or the foreign law enforcement body has reasonable grounds to suspect would be relevant for any of the purposes provided under Section 90(3).

(3) An arrangement or understanding entered into under subsection (1) shall include the following:

(a) restrictions on the use of the report, information or analysis for the purposes provided under Section 90(3);

(b) a stipulation that the report, information or analysis shall be treated confidential and is not to be further disclosed without the express consent of the FIU; and

(c) provisions concerning the use of the report, information or analysis and the other bodies with which the report, information or analysis may be shared.

92 Application of confidentiality provisions

The confidentiality provisions referred to in Sections 90(6) and 91(3) apply to:

(a) a request to the FIU for a report, information or analysis;

(b) a request by the FIU for a report, information or analysis; and

(c) a report, information or analysis shared by the FIU with a foreign counterpart or shared with the FIU by a foreign counterpart, whether or not shared in response to a request referred to in paragraph (a) or (b).

93 Use of powers for gathering information

The FIU may use the powers granted to it under Subdivisions 1 and 2 of this Division for the purpose of gathering information to share with a foreign counterpart.

PART 6 – MUTUAL LEGAL ASSISTANCE IN RELATION TO MONEY LAUNDERING

94 Co-operation with a Foreign State

(1) A request for mutual assistance by a foreign State in relation to a financial crime, criminal conduct or targeted financial sanctions shall be made to the Minister.

(2) Subject to Section 99, where a foreign State makes a request under subsection (1), the Minister may direct the Secretary for Justice to:

(a) immediately execute the request; or

(b) inform the foreign State making the request of any reason:

(i) for not executing the request immediately; or

(ii) for delaying the execution of the request.

95 Republic may obtain search warrant

For the purpose of executing the request as directed in the warrant, the Republic may upon production to the Resident Magistrate of a request received pursuant to Section 104, apply for a warrant to:

(a) enter any premises belonging to, in the possession or control of any person named in the warrant; and

(b) search the premises and remove any document, material or other thing.

96 Property tracking and monitoring orders

The Republic may apply to the Resident Magistrate for an order that:

(a) a person in possession, control of or who owns any document the subject of the request, deliver to the Secretary such document that is relevant to:

(i) identifying, locating or quantifying any property; or

(ii) identifying or locating any document necessary for the transfer of any property; and

(b) a reporting entity immediately produce to the Secretary all information obtained by the reporting entity about any business transaction conducted by or for a person the subject of the request with the reporting entity during such period before or after the date of the order as the Resident Magistrate directs.

97 Restraining and forfeiture of property

Subject to Section 99, the Republic, upon application to the Supreme Court for a request for a restraining or forfeiture of property of or in the possession or under the control of a person named in the request, may obtain an order:

(a) restraining the property of or in the possession or under the control of the person named in the request;

(b) giving directions as to the disposal of that property for the purpose of:

(i) determining any dispute as to ownership of the property or any part;

(ii) its proper administration during the period of restraint;

(iii) the payment of debts due to creditors prior to the request; and

(iv) the payment of monies to that person for the reasonable subsistence of that person and his or her family; or

(c) forfeiting the property of any person named in the request.

98 Request accompanied by an evidence order

(1) Subject to Section 99, the Republic may, upon application the Supreme Court and for a request accompanied by an order referred to in subsection (2) obtain an order directed to that person in the same terms as in the order accompanying the request.

(2) The order is an order issued by a court of the requesting State directed to any person within the jurisdiction of the Supreme Court to appear before or any provide any document or material in his or her possession, power or control to the court of the requesting State for the purpose of giving evidence in specified proceedings in that court.

(3) Upon being served with an order issued under subsection (1) the person served shall for the purposes of the order:

(a) appear before or provide any document or material to the Supreme Court; or

(b) appear before the court of the requesting State,

in accordance with the directions in the order.

(4) Where a person served with an order issued under subsection (1) elects to appear before the court of the requesting State and fails to comply with any direction in the order he or she shall be deemed immediately to have appeared before the Supreme Court as provided in subsection (3)(a).

(5) The Supreme Court shall conduct such proceedings as are necessary to take the evidence of any person appearing before it pursuant to subsection (3)(a).

(6) For the purposes of this Part, such evidence shall subsequently be transmitted by the Secretary to the requesting State.

99 Limitations on compliance with request

(1) The Secretary may refuse to comply with a request where:

(a) the action sought by the request is inconsistent with the Constitution;

(b) the execution of the request is likely to prejudice the national interest and security; or

(c) where the document or material requested is prohibited from being disclosed pursuant to any bilateral, multilateral or other obligations of the Republic to another State.

(2) The Secretary shall not refuse solely to comply with a request on the ground that the request relates to an offence that relates to matters of taxation or currency.

(3) The provisions of Section 97 apply only to property coming into the possession or under the control of a person after the commencement of this Part.

100 Requests to other States

The Minister on behalf of the Republic may issue to a foreign State a request accompanied, if required, by an order issued in accordance with Section 101.

101 Issuing evidence order against foreign resident

(1) The Secretary upon application to a Judge of the Supreme Court may in respect of any proceedings for a money laundering offence apply for an order directed to any person resident in a foreign State to attend or provide any document or material in his or her possession or under his or her power and control to:

(a) the Supreme Court; or

(b) subject to the approval of the foreign State, to the court of the foreign State,

for the purpose of giving evidence in relation to those proceedings.

(2) An order that is granted may be sent to the appropriate authorities in a foreign State in the form of a request that the foreign State provide such assistance as may be necessary to give effect to the order.

102 Evidence pursuant to a Request

Any evidence taken pursuant to a request made under Section 101 in any proceedings in a court of a foreign State shall be received by a court in the Republic as prima facie evidence in any proceedings to which such evidence relates.

103 Requests

A request shall be in writing, including in electronic form dated and signed by or on behalf of the person making the request but a request sent by other electronic form shall lapse at the expiration of 14 days if the original had not by then been received by the Secretary.

104 Requirements for request

A request shall:

(a) confirm that an investigation or prosecution is being conducted into a suspected criminal conduct, financial crime or money laundering offence or that a person has been convicted of such criminal conduct, financial crime or a money laundering offence;

(b) state the grounds on which any person is being investigated or prosecuted for the suspected criminal conduct, financial crime or money laundering offence referred to in paragraph (a) or give details of the convictions of the person referred to in paragraph (a);

(c) give particulars sufficient to identify any person referred to in paragraph (b);

(d) give particulars sufficient to identify any financial institution or other person believed to have information, documents or material, of assistance to the investigation or prosecution referred to in paragraph (a);

(e) request the person or entity to whom the request is addressed to obtain from a financial institution or other person referred to in paragraph (d) all and any information, documents or material of assistance to the investigation or prosecution referred to in paragraph (a);

(f) specify the manner in which and to whom, any information, documents or material obtained pursuant to the request is to be produced;

(g) state whether or not a restraining or forfeiture order is required; or

(h) contain such other information as may assist the execution of the request.

105 Request for forfeiture

A request for forfeiture shall have attached to it a copy of the final forfeiture order of the Supreme Court and a statement signed by a Judge of that Court to the effect that no further appeal against such order can be made.

106 Request not to be invalidated

(1) A request received in the Republic shall not be invalidated for the purpose of commencing any legal proceedings by reason of any failure to comply with Section 104 where the Secretary is satisfied that there is sufficient compliance to enable him or her to properly execute the request.

(2) Nothing in this Section shall derogate from the power of the Supreme Court to refuse to make an order where it considers that any such failure is such that an order ought not, in the circumstances, be made.

PART 7 – TARGETED FINANCIAL SANCTIONS

Division 1 – Preliminary

107 Definitions for this Part

In this Part:

'Administrator' means a person appointed as an Administrator under Section 118;

'asset' means funds, property, financial assets and economic resources of every kind, whether tangible or intangible, corporeal or incorporeal, moveable or immovable, actual or potential, however acquired, including:

(a) currency, including virtual or digital currency;

(b) precious metals and precious stones;

(c) real property and chattels;

(d) vehicles, including vessels, aircraft and motor vehicles;

(e) oil and other natural resources;

(f) legal documents or instruments in any form, including electronic or digital, evidencing title to or interest in or right to claim an asset, including bank credits, traveller's cheques, bank cheques, money orders, shares, securities, bonds, debt instruments, drafts and letters of credit;

(g) any other asset which potentially may be used to obtain funds, goods or services; and

(h) any interest, dividend, income or value accruing from, generated by or derived from an asset;

'de-list' means to revoke the designation of a person or entity so that targeted financial sanctions no longer apply to that person or entity;

'designated person or entity' means a person or entity designated under Section 109 or Section 110 to whom targeted financial sanctions apply*;*

'frozen asset' or ***'freezable asset'*** means an asset that cannot be dealt with as a result of targeted financial sanctions and includes but is not limited to the following:

(a) assets that are wholly or jointly, directly or indirectly, owned or controlled by:

  (i) a designated person or entity; or

  (ii) a person or entity acting on behalf of or at the direction of, a designated person or entity;

(b) assets derived or generated from assets listed in paragraph (a);

(c) vessels designated as freezable assets by the United Nations Security Council or its committees under resolution 2270 or resolution 2321 or

successor resolutions to those resolutions, on the basis that the vessels are owned or controlled by a designated person or entity; or

(d) assets prescribed by regulations as frozen assets or freezable assets.

'resolution' means a United Nations Security Council resolution adopted pursuant to Article 41 of the Charter of the United Nations;

'successor resolution' means a resolution that clarifies, amends, adds to or rescinds matters contained in a preceding resolution dealing with the same subject matter;

'targeted financial sanctions' means:

(a) measures that restrict dealing in assets or the making available of assets or financial or related services; or

(b) other restrictions or prohibitions directly or indirectly related to or for the benefit of designated persons or entities; and

'UNSC' means the United Nations Security Council.

108 Responsibility of the Cabinet in relation to resolutions listed in Schedule 1

The Cabinet may make regulations under Section 128 prescribing prohibited conduct that contravene, or impose obligations for complying with, resolutions listed in Schedule 1.

Division 2 – Targeted financial sanctions

109 UNSC designation and de-listing

(1) The designation of a person or entity for targeted financial sanctions by the UNSC or its committees under a resolution or successor resolution of such listed in Schedule 1 has immediate effect.

(2) The de-listing of a person or entity by the UNSC or its committees under a resolution or successor resolution of such listed in Schedule 1 has immediate effect.

110 Designation by the Minister

(1) The Minister shall designate a person or entity for targeted financial sanctions where the Minister has reasonable grounds to believe that the criteria for designation prescribed by regulations has been met.

(2) The designation of a person or entity by the Minister has immediate effect.

111 Appeal of designation made by the Minister

(1) A person or entity designated by the Minister may apply to the Minister to be de-listed.

(2) The application shall be in writing and provide any information in the possession of the designated person or entity relevant to the Minister's consideration of the application.

(3) The Minister is not required to consider another application by a designated person or entity where the person or entity has made a previous application under this Section, 12 months before the date of the other application.

112 Review of designation by Minister

The Minister shall review the grounds for a designation made by the Minister every 3 years after the date the designation was made.

113 De-listing by the Minister

(1) The Minister shall de-list a person or entity where, after consideration of an application under Section 111 or a review under Section 112 or at any other time, the Minister is satisfied that:

(a) there are no longer reasonable grounds for a designation;

(b) the designated person is deceased; or

(c) the designated entity no longer exists.

(2) The de-listing of a person or entity by the Minister has immediate effect.

114 Proposal for designation to the UNSC

(1) The Minister may submit a proposal to the UNSC or its committees to designate a person or entity for targeted financial sanctions, where the Minister has reasonable grounds to believe that the criteria for designation under a resolution or successor resolution of such listed in Schedule 1, has been met.

(2) The Minister may submit a proposal for designation, whether or not the Minister has designated the person or entity under Section 110.

115 Materials on which designations may be based

(1) In considering whether to designate or de-list a person or entity or to propose a designation to the UNSC or its committees, the Minister may consider any relevant information from any relevant source, either foreign or domestic, including information held by an intelligence agency or the police.

(2) A foreign or domestic intelligence agency or the police may provide information, including security classified material, to the Minister for the purpose of enabling the Minister to carry out his or her functions under this Part.

116 Notice of rights to a designated person or entity

(1) The Minister shall use his or her best endeavours to provide written notice to a designated person or entity where the person or entity is:

(a) located in the Republic;

(b) a citizen of the Republic wherever located;

(c) a body corporate incorporated under a law of the Republic; or

(d) a body corporate incorporated under a foreign law and that has a presence in the Republic.

(2) The notice shall be provided within a reasonable time after the date of the designation and after sufficient time has been allowed for targeted financial sanctions to be applied.

(3) The notice shall contain information necessary to inform the designated person or entity of their rights, including:

(a) the grounds for the designation which may be made publicly available;

(b) the consequences of the designation;

(c) avenues and procedures for appealing the designation; and

(d) avenues for seeking access to an asset or financial or related service.

117 Power to seize assets

(1) The Supreme Court may grant an order for a police officer to search for and seize a frozen asset where there is a reasonable risk that the asset will dissipate.

(2) The Supreme Court may grant the order only on application by or on behalf of the Minister.

(3) Where during the course of a search for frozen assets, an officer finds an asset that he or she has reasonable grounds to believe could have been included in the Supreme Court's order, had its existence been known at the time the order was made, the officer may seize the asset and the order is deemed to have authorised such seizure.

118 Management of seized assets

(1) The Minister shall use his or her best endeavours to maintain the value of an asset seized under Section 117 and for such purpose may appoint an Administrator to manage a seized asset.

(2) An administrator appointed under subsection (1) has all the powers necessary to diligently and in good faith, manage a seized asset.

(3) An asset seized under Section 117 shall only be retained by the Minister or the administrator for as long as the asset remains a frozen asset or until such time, as required by the administrator to complete his or her functions in relation to the asset.

(4) Where an administrator is not appointed, the Secretary shall perform the functions of the administrator under this Act.

119 Destruction or disposal of seized assets

The Minister or administrator may destroy or dispose of an asset seized under Section 117 where:

(a) the asset is a vessel seized pursuant to resolution 1718 or a successor resolution to that resolution or another asset prescribed by regulations;

(b) maintenance of the asset is not reasonably feasible; and

(c) the UNSC or its committee has approved the destruction or disposal of the asset.

Division 3 – Supervision

120 Supervisory Responsibility

(1) The FIU is responsible for supervising compliance with regulations made under Section 128.

(2) The FIU has the following supervisory functions in relation to regulations under this Part:

(a) to monitor and enforce compliance, including by referring matters for criminal investigation where appropriate;

(b) to specify such forms or notices as are necessary to monitor and enforce compliance; and

(c) to provide publicly available guidance to promote compliance.

121 Power to require information or documents to be given

(1) The FIU may, for the purpose of supervising compliance with regulations under this Part, issue a written notice requiring a person to provide information or documents of the kind, by the time and in the manner, specified in the notice.

(2) A person may, before the time specified in the notice, request the FIU to vary a notice by extending the time specified or in any other manner.

(3) The FIU may vary the notice where it considers it appropriate to do so.

(4) A person shall comply with a notice notwithstanding any other law or contractual obligation, other than a law governing legal professional privilege.

122 Power to conduct on-site inspection

(1) The FIU may, with or without prior notice, request entry into real property used for a commercial purpose, for the purpose of conducting an on-site inspection to monitor compliance with regulations under this Part.

(2) The FIU shall produce official identification and a written notice of the on-site inspection no later than at the time that the request for entry is made.

(3) During an on-site inspection, the FIU may require information or documents to be provided for inspection.

(4) A person shall comply with a request for information or documents notwithstanding any other law or contractual obligation, other than a law governing legal professional privilege.

123 Financial Intelligence Unit may copy documents

Where a person provides a document to the FIU under Section 121 or 122, the FIU:

(a) may make and keep a copy of the document; and

(b) shall return the original document to the person within a reasonable time.

Division 4 – Enforcement

124 Offence for failure to comply with a requirement to provide information or documents

(1) A person required to provide information or documents under Division 3 shall not:

(a) fail to provide the information or documents;

(b) provide false or misleading information or documents; or

(c) destroy, deface or conceal documents with the intention of evading such requirement under Division 3 to provide documents.

(2) A person who contravenes subsection (1) commits an offence and shall be liable upon conviction:

(a) for an individual, to a fine not exceeding $20,000 or imprisonment for a term not exceeding 2 years or to both; or

(b) for a body corporate, to a fine not exceeding 100,000 or where the contravention involves one or more transactions, an amount equivalent to the value of the transactions, whichever is greater.

125 Offence against regulations

A person who engages in conduct that contravenes a regulation under this Part commits an offence shall be liable upon conviction:

(a) for an individual, to a fine not exceeding $200,000 or imprisonment for a term not exceeding 20 years or to both; or

(b) for a body corporate, to a fine not exceeding $1,000,000 or where the contravention involved one or more transactions, an amount equivalent to the value of the transactions, whichever is greater.

Division 5 – Other matters

126 Disclosure of information

The Minister or the FIU may only disclose information obtained under this Part or regulations, for the purpose of administering or supervising compliance with this Part or regulations or for a law enforcement or regulatory purpose, to any of the following:

(a) a relevant government department;

(b) a foreign government agency;

(c) a public international organisation to which the Republic is a party;

(d) the UNSC or its committees; or

(e) bodies operating under the authority of the UNSC as specified in a resolution.

127 Protection from liability

(1) No civil or criminal proceedings shall be taken against a person if the person has, in good faith and with reasonable care, engaged in conduct in compliance or in purported compliance, with this Part or regulations.

(2) No civil or criminal proceedings may be made against the Minister or the FIU for anything done or omitted to be done, in good faith, in the performance of the Minister's or the FIU's functions or the exercise of the Minister's or the FIU's powers under this Part or regulations.

128 Regulations for this Part

(1) The Cabinet may make regulations as are necessary or expedient to give effect to this Part.

(2) Without limiting subsection (1), regulations may give effect to this Part by prescribing the following matters:

(a) designating persons, entities or assets;

(b) prohibiting dealings with assets or the making available of assets;

(c) prescribing frozen assets or freezable assets;

(d) prohibiting the supply, sale, procurement or transfer of goods or services;

(e) prohibiting commercial or other activities related to certain persons or entities;

(f) authorising access to assets, goods or services;

(g) imposing obligations for complying with resolutions or successor resolution of such listed in Schedule 1;

(h) amending Schedule 1; or

(i) providing administrative procedures.

(3) To avoid doubt, the validity or operation of another Act or regulations made under another Act, is not affected merely because the Act or regulations give effect to a resolution under Article 41 or any other Article of the Charter of the United Nations.

PART 8 – MISCELLANEOUS

129 Application of this Act to the Proceeds of Crime Act 2004

(1) The process, procedure and enforcement of the confiscation, forfeiture, determination of competing interest of persons or disposal of criminal property as required under this Act, are to be made in accordance with the *Proceeds of Crime Act 2004*.

(2) The references to the offences and description of property which is the subject of proceeds of crime described under this Act *mutatis mutandis* are to be treated as applying with reference to any tainted property under the *Proceeds of Crime Act 2004.*

130 Regulations

Without limiting Section 128, the Cabinet may make regulations to prescribe matters that are required or permitted by this Act to be prescribed or are necessary or convenient to be prescribed, for carrying out or giving effect to this Act and generally for achieving the purposes of this Act.

PART 9 – REPEAL, SAVINGS AND TRANSITIONAL PROVISIONS AND CONSEQUENTIAL AMENDMENTS

131 Definitions

In this Part, '***repealed Act***' means the *Anti-Money Laundering Act 2008*.

132 Repeal of Act

The *Anti*-Money *Laundering Act 2008* is repealed.

133 Financial Intelligence Unit agreements and arrangements

(1) This Section applies to an agreement or arrangement entered into by the Financial Intelligence Unit under Section 11 of the repealed Act where the agreement or arrangement was in force immediately before the commencement of this Act.

(2) The agreement or arrangement continues in force as if it had been entered into by the FIU under this Act.

134 Financial institution reports

(1) This Section applies to a report made by a financial institution under Section 17 of the repealed Act.

(2) The report continues to have effect as if it had been made by the financial institution under this Act.

135 Legal proceedings under repealed Act

(1) This Section applies to a legal proceeding that had been instituted under the repealed Act but had not been finally determined immediately before the commencement of this Act.

(2) The legal proceeding shall continue on and after the commencement of this Act as if the *Anti-Money Laundering Act 2008* had not been repealed.

136 Investigations under repealed Act

(1) This Section applies to an investigation that had been instituted under the repealed Act but had not been finally determined immediately before the commencement of this Act.

(2) The investigation shall continue on and after the commencement of this Act as if the *Anti-Money Laundering Act 2008* had not been repealed.

137 Appointment under the repealed Act

(1) This Section applies to an appointment made under the repealed Act that was in force immediately before the commencement of this Act.

(2) The appointment continues in force on and after the commencement of this Act as if it had been made under this Act.

138 Regulations made under repealed Act

Any regulation, rule order or other subordinate legislation made under the repealed Act shall continue in force on and after the commencement of this Act as if such had been made under this Act.

139 Other matters under the repealed Act

(1) This Section applies to any other matter done or made under the repealed Act that was in effect immediately before the commencement of this Act.

(2) The matter continues to have effect on and after the commencement of this Act as if it had been done or made under this Act.

140 Consequential amendments of other written laws

All references under any written law to '*Anti Money Laundering Act 2008*' shall be deleted and substituted with '*Anti-Money Laundering and Targeted Financial Sanctions Act 2023*'.

SCHEDULE 1

UNITED NATIONS SECURITY COUNCIL RESOLUTIONS

(Section 109)

Item	Resolution
1	Resolution 1267 (1999) of the Security Council, adopted on 15 October 1999.
2	Resolution 1989 (2011) of the Security Council, adopted on 17 June 2011.
3	Resolution 2253 (2015) of the Security Council, adopted on 17 December 2015.
4	Resolution 1988 (2011) of the Security Council, adopted on 17 June 2011.
5	Resolution 1373 (2001) of the Security Council, adopted on 28 September 2001.
6	Resolution 1737 (2006) of the Security Council, adopted on 27 December 2006.
7	Resolution 2231 (2015) of the Security Council, adopted on 20 July 2015.
8	Resolution 1718 (2006) of the Security Council, adopted on 14 October 2006.

9 Resolution 2087 (2013) of the Security Council, adopted on 22 January 2013.

10 Resolution 2094 (2013) of the Security Council, adopted on 7 March 2013.

11 Resolution 2270 (2016) of the Security Council, adopted on 2 March 2016.

12 Resolution 2321 (2016) of the Security Council, adopted on 30 November 2016.

13 Resolution 2375 (2017) of the Security Council, adopted on 11 September 2017.