GUIDE

An introduction to the Cayman AML/CFT/CPF regime

Last reviewed: August 2024

Contents

1 Key legislation

The key components of the Cayman Islands' anti-money laundering (**AML**), countering the financing of terrorism (**CFT**) and countering proliferation financing (**CPF**) framework include the following statutes:

- Anti-Corruption Act (as amended);
- Anti-Money Laundering Regulations (as amended, the **AML Regulations**);
- Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing in the Cayman Islands (February 2024) (as amended, the **Guidance Notes**);
- Misuse of Drugs Act (2017 Revision);
- Penal Code (as amended);
- Proceeds of Crime Act (as amended) (the **PCA**);
- Proliferation Financing (Prohibition) Act (2017 Revision) (the **PFPA**); and
- Terrorism Act (as amended) (the **Terrorism Act**),

together with certain Overseas Territories Orders passed by the Government of the United Kingdom implementing United Nations or European Union sanctions or restrictive measures against countries, regimes or individuals deemed to be in violation of international law. These Orders have the force of law in the Cayman Islands once passed by UK parliament[1].

The AML/CFT/CPF legislation criminalises money laundering, terrorist financing and proliferation financing[2] and imposes penalties and criminal sanctions for these offences. The commission of those offences may lead to enforcement actions and/or prosecution. The main offences under the AML/CFT/CPF legislation are summarised briefly below.

2 Outline of the offences

2.1 Money laundering offences

The main money laundering offences under the PCA are summarised briefly below.

- Section 133 of the PCA creates the offence of concealing, disguising, converting or transferring criminal property, or removing criminal property from the Cayman Islands. Property is **criminal property** if it constitutes the proceeds of criminal conduct and the alleged offender knows or suspects that it constitutes the proceeds of criminal conduct[3].
- Section 134 of the PCA creates the offence of entering into or becoming concerned in an arrangement which the relevant person knows or suspects facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person.
- Under Section 135 of the PCA, a person commits an offence if he/she acquires, uses or has possession of criminal property.
- Sections 136 and 137 of the PCA create offences for failing to make a disclosure to the Financial Reporting Authority (the **FRA**) or a nominated officer as soon as reasonably practicable where:
  - a person knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in criminal conduct; and
  - the information on which the knowledge or suspicion is based came to that person in the course of a business in the regulated sector, or other trade, profession, business or employment.

[1] A list of the Orders in force in the Cayman Islands is maintained by the FRA at http://www.fra.gov.ky/. Whilst the sanctions programs maintained by the US Treasury Department's Officer of Foreign Assets Control (OFAC) do not have force of law in the Cayman Islands, these sanctions should be taken into consideration where an entity is connected to US persons or entities, or conducts business with any US persons or entities.

[2] **Proliferation financing** refers to the act of providing funds or financial services which are used, in whole or in part, for the development or production, or the facilitation of the development or production, of nuclear, radiological, biological or chemical weapons or systems for their delivery, in contravention of national or, where applicable, international laws.

[3] Section 144(3) of the PCA.

- Section 139 of the PCA creates the offence of tipping off a target or third party about a suspicion, investigation or proposed investigation into money laundering, which is likely to prejudice such an investigation.

A person who commits an offence under Sections 133, 134 or 135 of the PCA is liable, on summary conviction, to a fine of US$6,098 and/or imprisonment for a term of two years or, on conviction on indictment, to a fine and/or to imprisonment for a term of fourteen years.

A person who commits an offence under Sections 136, 137 or 139 of the PCA is liable, on summary conviction, to a fine of US$6,098 and/or imprisonment for a term of two years or, on conviction on indictment, to a fine and/or to imprisonment for a term of five years.

2.2 Terrorist financing offences

The main terrorist financing offences under the Terrorism Act are summarised briefly below.

- Section 19 of the Terrorism Act makes it an offence for a person to provide or collect property (or attempt to do so) with the intention or knowledge that the property be used:
  - to carry out an act of terrorism;
  - by a terrorist to facilitate that person's terrorism-related acts or membership in a terrorist organisation; or
  - by a terrorist organisation.
- Under Section 20 of the Terrorism Act, it is an offence to:
  - use property for the purposes of terrorism;
  - possess terrorist property[4] and intend that the property be used, or have reasonable cause to suspect that it may be used, for the purposes of the financing of acts of terrorism, terrorists or terrorist organisations;
  - possess or acquire terrorist property with the knowledge, or with reasonable cause to suspect, that the property has been used, directly or indirectly, in the commission of the financing of acts of terrorism, terrorists or terrorist organisations; or
  - acquire property as a result of or in connection with acts of terrorism.
- Under Section 21 of the Terrorism Act, a person commits an offence if he:
  - enters into or becomes concerned in an arrangement by which terrorist property is, or is to be, made available to another; and
  - knows or has reasonable cause to suspect that the property will or may be used for the purposes of the financing of acts of terrorism, terrorists or terrorist organisations.
- Under Section 22 of the Terrorism Act, a person commits an offence if he/she enters into or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property by concealment, removal from the jurisdiction or transfer to nominees.
- Sections 23 and 25 of the Terrorism Act impose an obligation to disclose to the FRA or a police constable, as soon as reasonably practicable, a suspicion or belief that another person has committed an offence under Sections 19 to 22 of the Terrorism Act. Failure to make a disclosure in accordance with those sections is an offence.

A person who commits an offence under Sections 19 to 22 of the Terrorism Act is liable, on summary conviction, to a fine of US$4,878 and two years' imprisonment or, on conviction on indictment, to a fine and to fourteen years' imprisonment.

A person who commits an offence under Sections 23 or 25 of the Terrorism Act is liable, on summary conviction, to a fine of US$4,878 and six months' imprisonment or, on conviction on indictment, to a fine and to five years' imprisonment.

---

[4] Terrorist property is defined in Section 18 of the Terrorism Act as property that is the proceeds of, or used in, or intended or allocated for use in, the financing of acts of terrorism, terrorists or terrorist organisations.

2.3 Proliferation finance offences

Section 2B of the PFPA requires that a person who has in their possession, custody or control in the Cayman Islands, any funds or resources or is otherwise dealing with funds or economic resources that are:

- wholly or partly owned or controlled, directly or indirectly, by a designated person[5]; or
- derived or generated from funds or economic resources owned or controlled, directly or indirectly by a designated person,

to immediately freeze all such funds or economic resources and ensure that such funds or economic resources are not made available, whether directly or indirectly, to or for the benefit of the designated person.

Details of any freezing actions taken in accordance with the PFPA must be disclosed to the FRA as soon as reasonably practicable under Section 2C of the PFPA.

Failure to comply with the requirements of Sections 2B or 2C of the PFPA is an offence, giving rise on summary conviction to a fine of US$60,976 or US$12,195, respectively. A person who fails to comply with Section 2B is liable on conviction on indictment to a fine of US$85,366 or imprisonment for a term of three years, or both. Alternatively, the FRA may impose civil penalties in relation to a breach of Sections 2B(1) or 2C in such amount as it considers appropriate.

Where there is a risk of proliferation activities in relation to any country, the FRA may issue directions to persons in the financial sector under the PFPA and impose requirements such as conducting enhanced due diligence measures, monitoring designated persons or restricting financial service providers from entering into or continuing business relationships with designated persons. The PFPA imposes both civil and criminal sanctions for failure to comply with such obligations.

The FRA has issued Guidance on Targeted Financial Sanctions for the public, which can be accessed here.

3 The AML Regulations and the Guidance Notes

The AML Regulations require persons conducting "relevant financial business" (as defined in the PCA) to establish systems to detect money laundering, terrorist financing and proliferation financing, and therefore assist in the prevention of abuse of their financial products and services. This is in the commercial interests of those businesses and it also protects the reputation of the Cayman Islands. Those requirements are discussed in more detail in section 5 of this memorandum.

A breach of the AML Regulations may lead, on summary conviction, to a fine of US$609,756 or, on conviction on indictment, to a fine and to two years' imprisonment.

The Guidance Notes are designed to assist all persons conducting relevant financial business, referred to as financial service providers or FSPs, in complying with the AML Regulations. They are intended to supplement and clarify the requirements of the AML Regulations and the PCA. FSPs are expected to follow the Guidance Notes in developing an effective AML/CFT/CPF framework suitable to their business. Failure to do so, may result in the relevant supervisory authority seeking an explanation and concluding that the FSP is carrying on business in a manner that may give rise to enforcement actions under the applicable legislation.

Under the AML Regulations, the Guidance Notes will be taken into account by a court determining whether a person has complied with the AML Regulations.

[5] Designated person is defined in the PFPA as meaning a person, including any subsidiary or other entity owned or controlled by that person, to whom anti-proliferation financing measures issued by the Security Council of the United Nations relate.

4 Administrative fines

In addition to the sanctions and penalties outlined above, a breach of certain (not all) provisions of the AML Regulations may lead to administrative fines being imposed pursuant to the AML Regulations or the Monetary Authority (Administrative Fines) Regulations (as amended).

The amount of the fine imposed depends upon the categorisation of the relevant breach as minor, serious or very serious. The table below details the fines which may be imposed and the limitation periods relating to the three categories of breaches.

Breach	*Fine(s)*	*Limitation period*[6]
Minor	'Initial' fixed fine of US$6,098 The supervisory authority also has a discretion to impose one or more additional fines of US$6,098 each, up to a cumulative cap of US$24,390 for a single minor breach	6 months
Serious	A single fine up to a maximum of US$60,976 for individuals or US$121,951 for corporate bodies	2 years
Very serious	A single fine up to a maximum of US$121,951 for individuals or US$1,219,512 for corporate bodies	2 years

It is important to note that breaches committed by a corporate body with the consent, connivance or neglect of a director, manager, secretary, partner or other similar individual/officer can also lead to fines against such persons.

The supervisory authority has discretion as to whether to impose a fine, and the amount of a fine, in relation to serious and very serious breaches only. A process for imposing an administrative fine as well as an appeal mechanism are stipulated.

5 Requirements of the AML Regulations

5.1 Regulation 5

Under Regulation 5 of the AML Regulations, an FSP must:

- maintain the following procedures in relation to the relevant financial business, which should be appropriate to the size of the business and the money laundering, terrorist financing and proliferation financing risks to which the FSP is exposed:
  - adoption of a risk-based approach as set out in Part III of the AML Regulations to monitor financial activities, including categories of activities which are considered to be high risk (see section 5.2 below for more detail);
  - identification and verification procedures in relation to customers[7], in accordance with Part IV of the AML Regulations;
  - adequate systems to identify risk in relation to persons, countries and activities, which shall include checks against all applicable sanctions lists;

[6] These limitation periods run from the date on which the supervisory authority became aware of the commission of the relevant breach. A supervisory authority will be deemed to have become aware of a breach when it first received information from which the breach can reasonably be inferred.

[7] Customer is defined in the AML Regulations as meaning a person who is in a business relationship, or is carrying out a one-off transaction, with a person who is carrying out a relevant financial business in the Cayman Islands.

- adoption of risk management procedures concerning the conditions under which a customer may utilise the business relationship prior to verification;
- observance of the list of countries, published by any competent authority, which are non-compliant, or do not sufficiently comply, with the recommendations of the Financial Action Task Force;
- procedures for the assessment of one-off transactions and the ongoing monitoring of business relationships for the purposes of preventing, countering and reporting money laundering, terrorist financing and proliferation financing, and procedures allowing the identification of assets subject to targeted financial sanctions applicable to the Cayman Islands;
- procedures to ensure compliance with targeted financial sanctions applicable to the Cayman Islands;
- record-keeping procedures in accordance with Part VIII of the AML Regulations;
- internal reporting procedures in accordance with Regulation 34 of the AML Regulations (see section 5.3 below);
- other internal controls procedures, including an appropriate risk-based independent audit function, as may be appropriate for the ongoing monitoring of business relationships or one-off transaction for the purpose of forestalling and preventing money laundering, terrorist financing and proliferation financing; and
- procedures to screen employees to ensure high standards when hiring;

◦ comply with the identification and record-keeping requirements of Parts IV and VIII of the AML Regulations (see section 5.4 below);

◦ take appropriate measures from time to time to make employees aware of:
  - the procedures listed above; and
  - the money laundering, terrorist financing and proliferation financing legislation and targeted financial sanctions;

◦ provide employees from time to time with training in the recognition and treatment of transactions carried out by, or on behalf of, any person who is or who appears to be engaged in money laundering, terrorist financing or proliferation financing, or whose assets are subject to targeted financial sanctions; and

◦ appoint an Anti-Money Laundering Compliance Officer (**AMLCO**) (see section 5.5 below).

5.2 The risk-based approach

The risk-based approach stipulated by the AML Regulations requires an FSP to take steps to identify, assess and understand its money laundering, terrorist financing and proliferation financing risks in relation to:

◦ the entity's customers;

◦ the countries or geographic areas in which those customers reside or operate;

◦ the products, services and transactions of the FSP; and

◦ the delivery channels[8] of the FSP.

Guidance on conducting business risk assessments can be found at Sections 2 and 3 of Part II (General AML/CFT Guidance) of the Guidance Notes.

[8] **Delivery** channel in this context means the way or means whereby an FSP carries on its business relationship with a customer; ie, directly or through other means such as email, internet, intermediary or any correspondent institution.

5.3 Suspicious activity reporting procedures

FSPs are required to establish suspicious activity reporting procedures, both:

- internally, to enable employees of the FSP to report suspicious activity to the entity's Money Laundering Reporting Officer (**MLRO**) (or in the MLRO's absence, the Deputy Money Laundering Reporting Officer or **DMLRO**) for review and investigation; and
- externally, pursuant to which the MLRO/DMLRO, following investigation and a determination that the circumstances warrant it, report suspicious activity to the FRA.

Filing a suspicious activity report with the MLRO/DMLRO or, by the MLRO/DMLRO, with the FRA, can act as a defence to the various offences under the AML/CFT/CPF legislation.[9] As part of the requirement to establish suspicious activity reporting procedures, an FSP must appoint the MLRO and DMLRO, who cannot be the same person.

5.4 Customer due diligence procedures

The customer due diligence procedures required by Parts IV to VIII of the AML Regulations require that persons carrying out relevant financial business identify, and verify the identity of, their customers, persons acting on behalf of those customers and, in certain circumstances, the beneficial owners of the customers and their source of funds.

Identification of customers is required to be completed when establishing a business relationship or when carrying out a one-off transaction valued in excess of US$12,195 or by wire transfer, where there is a suspicion of money laundering or terrorist financing, or where there are doubts regarding the veracity or adequacy of previously obtained customer identification data.

However, verification of identity may, in accordance with the AML Regulations, be completed after the establishment of the business relationship, provided that:

- verification occurs as soon as reasonably practicable;
- it is essential not to interrupt the normal conduct of business; and
- the money laundering or terrorist financing risks are effectively managed.

The AML Regulations provide for different levels of customer due diligence for customers with different risk profiles, with enhanced due diligence being required where higher risk(s) are identified, including specific requirements for sanctions screening where higher proliferation financing risks are identified.

5.5 Role of the AMLCO

The responsibilities of the AMLCO include the following:

- being the point of contact with the supervisory and other competent authorities in the Cayman Islands;
- responding promptly to any requests for information from such authorities;
- reviewing, developing and maintaining the AML/CFT/CPF systems and procedures in-line with the evolving requirements of the Cayman Islands' AML/CFT/CPF regime;
- maintaining certain required records/registers, including a high risk customer and transaction register and a politically exposed person register;
- ensuring regular (at least annual) audits of the FSP's AML/CFT/CPF programme;
- advising the FSP's management of any AML/CFT/CPF compliance issues that need to be brought to their attention; and
- reporting periodically (and, in any event, at least annually) to the FSP's management on the entity's AML/CFT/CPF systems and controls.

[9] Note from 2 January 2025 this defence will only apply if the FRA has consented to the act.

6 Group-wide implications

The AML Regulations require a financial group[10] or other person carrying out relevant financial business through a similar financial group arrangement to implement group-wide programmes against money laundering and terrorist financing which are applicable (and appropriate) to all branches and majority-owned subsidiaries of the financial group.

Contacts

A full list of contacts specialising in regulatory law in the Cayman Islands can be found here.

[10] Financial group is defined in the AML Regulations as meaning a group that consists of a parent company or any other type of legal person, exercising control and coordinating functions over the rest of the group for the application of group supervision together with branches or subsidiaries that are subject to anti-money laundering policies and procedures at the group level.

2021934/78196373/1