

EXTRAORDINARY

OFFICIAL GAZETTE
THE BAHAMAS

PUBLISHED BY AUTHORITY

NASSAU 27th October, 2026

FINANCIAL AND CORPORATE SERVICE PROVIDERS (ANTI-MONEY LAUNDERING, COUNTERING THE FINANCING OF TERRORISM AND COUNTERING FINANCING OF PROLIFERATION) RULES, 2026

Arrangement of Rules

Rule

PART I - PRELIMINARY **3**

1. Citation....3
2. Interpretation....3

PART II – RISK RATING **5**

3. Duty of licensee to implement risk rating framework....5
4. Duty of licensee concerning internal controls....7
5. Group-wide programmes....7
6. Appointment of Compliance Officer....8
7. Money Laundering Reporting Officer....8
8. Outsourcing MLRO function....9
9. Suspicious transaction reporting....9

PART III – VERIFICATION OF CUSTOMER IDENTITY **10**

10. Due diligence measures....10
11. Verification of customer identity....10
12. Use of a business relationship prior to completion of verification....11
13. Simplified due diligence measures....12
14. Enhanced due diligence measures....13
15. Required information....13
16. Politically exposed persons....14
17. Reliance on third party verification procedures....16
18. Eligible introducer....16
19. Suspension or termination of activity or business....17
20. Ongoing monitoring....17

PART IV – TARGETED FINANCIAL SANCTIONS **18**

21. Targeted financial sanctions....18

PART V – RECORD KEEPING **18**
22. Maintenance of records....18
23. Verification records....19
24. Transaction records....19
25. Other records....20

PART VI – MISCELLANEOUS **20**
26. Education and training....20
27. Revocation of S.I. No. 11 of 2019....21

S.I. No. 107 of 2026

FINANCIAL AND CORPORATE SERVICE PROVIDERS ACT, 2020 (NO. 27 OF 2020)

FINANCIAL AND CORPORATE SERVICE PROVIDERS (ANTI-MONEY LAUNDERING, COUNTERING THE FINANCING OF TERRORISM AND COUNTERING FINANCING OF PROLIFERATION) RULES, 2026

The Securities Commission of The Bahamas, in exercise of the powers conferred by section 27 of the Financial and Corporate Service Providers Act, 2020, makes the following rules —

PART I - PRELIMINARY

1. Citation.

These Rules may be cited as the Financial and Corporate Service Providers (Anti-Money Laundering, Countering the Financing of Terrorism and Countering Financing of Proliferation) Rules, 2026.

2. Interpretation.

(1) In these Rules —

"Act" means the Financial and Corporate Service Providers Act, 2020 *(No. 27 of 2020)*;

"AML/CFT/CPF" means anti-money laundering, countering the financing of terrorism and countering financing of proliferation;

"Anti-Terrorism Act" means the Anti-Terrorism Act, 2018 *(No. 27 of 2018)*;

"Commission" means the Securities Commission of The Bahamas as continued under section 10 of the Securities Industry Act, 2024 *(No. 39 of 2024)*;

"customer" has the meaning assigned to it under section 2 of the Financial Transactions and Reporting Act, and where the context requires includes client or facility holder;

"designated person or entity" means a designated entity as defined under section 2 of the Anti-Terrorism Act;

"facility holder" has the meaning assigned to it under section 2 of the Financial Transactions and Reporting Act;

"financial group" means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group, together with the branches and subsidiaries of the group that are subject to AML/CFT/CPF policies and procedures at the group level;

"Financial Intelligence Unit" means the body continued under section 3 of the Financial Intelligence Unit Act, 2023 *(No. 54 of 2023)*;

"Financial Transactions Reporting Act" means the Financial Transactions Reporting Act, 2018 *(No. 5 of 2018)*;

"identified risk" has the meaning assigned to it under section 2 of the Financial Transactions Reporting Act;

"International Obligations (Economic and Ancillary Measures) Act" means the International Obligations (Economic and Ancillary Measures) Act *(Ch. 16)*;

"IRF Steering Committee" means the Identified Risk Framework Steering Committee established under section 6 of the Proceeds of Crime Act;

"licensee" means a person holding a licence under the Act;

"legal person" means a corporate or incorporate body;

"Money Laundering Reporting Officer" or **"MLRO"** means a person appointed pursuant to regulation 5 of the Financial Intelligence (Transactions Reporting) Regulations, 2001 *(S.I. No. 7 of 2001)*;

"Proceeds of Crime Act" means the Proceeds of Crime Act, 2018 *(No. 4 of 2018)*;

"suspicious transaction report" means a report made pursuant to section 25 of the Financial Transactions Reporting Act; and

"**targeted financial sanctions"** means sanctions imposed against a person or entity pursuant to section 3A of the International Obligations (Economic and Ancillary Measures) Act, to freeze or restrain

money, assets or property and any prohibition on making money, assets or property available, directly or indirectly, to or for the benefit of that person or entity.

(2) In these Rules, references to "money laundering, financing of terrorism and financing of proliferation" or "AML/CFT/CPF", where used in relation to the assessment, management or mitigation of risk, shall be construed as including all identified risks as defined in the Financial Transactions Reporting Act.

(3) These Rules are in addition to, and do not derogate from, any obligation of a licensee or of any other person under the Financial Transactions Reporting Act, the Anti-Terrorism Act, the International Obligations (Economic and Ancillary Measures) Act or any other enactment concerning money laundering, financing of terrorism and financing of proliferation.

PART II – RISK RATING

3. Duty of licensee to implement risk rating framework.

(1) A licensee shall implement a risk rating framework which assesses —

(a) the risk profile of each customer;

(b) the licensee's risk profile in relation to the countries or jurisdictions in which it operates; and

(c) the risk profile associated with the licensee's products, services, transactions and delivery channels.

(2) The risk rating framework shall be approved by the licensee's senior management based on the scope of the licensee's activities, and shall be designed to —

(a) take appropriate measures to manage and mitigate identified risks;

(b) take account of any risk assessment carried out at a national level and any regulatory guidance issued by the Commission;

(c) categorise customer relationships and products to identify the risk associated with each customer relationship or product;

(d) categorise customer relationships and products to take account of risk factors related to the particular customer relationship or product, including —

(i) customer type or profession;

(ii) country of domicile;

(iii) complexity of ownership;

(iv) complexity of legal structure;

(v) source of business;

(vi) type of assets;

(vii) type, size and volume of transactions;

(viii) level of cash transactions; and

(ix) adherence to customer activity profile;

(e) address which level of management can approve a decision for the licensee to enter into customer relationships at the various levels of risk rating categories;

(f) establish Know Your Customer and due diligence information requirements appropriate for the risk profile of the customer relationship or product including simplified due diligence and enhanced due diligence procedures;

(g) require the periodic review of the customer relationship or product to —

(i) ensure that the categorisations are current and appropriate; and

(ii) enable the licensee to determine whether any adjustment should be made to the risk rating;

(h) require the re-categorisation of a customer relationship or product offered by the licensee in the event of a change in the risk profile of a customer relationship or product; and

(i) require the documentation of the basis for the risk rating applied to a customer relationship or product and of any changes in the risk rating of a particular customer relationship or product.

(3) A licensee shall assess the risk profile of each new customer and carry out a risk assessment of each new product, business practice or technology prior to establishing a business relationship with such customer or introducing the product, business practice or technology.

(4) A licensee's risk rating framework shall be subject to review by the Commission and the outcome of each customer or product risk assessment conducted shall be documented and retained in accordance with these Rules.

4. Duty of licensee concerning internal controls.

A licensee shall implement internal control policies, procedures and systems for the prevention of identified risks associated with money laundering, the financing of terrorism and the financing of proliferation, and shall —

(a) engage a compliance officer;

(b) engage a Money Laundering Reporting Officer; and

(c) verify, on a regular basis, compliance with its internal policies, procedures and controls relating to money laundering, financing of terrorism and financing of proliferation.

5. Group-wide programmes.

(1) A licensee that is a member of a financial group shall implement group-wide programmes against money laundering, the financing of terrorism and the financing of proliferation which are applicable and appropriate to all branches and majority-owned subsidiaries of the financial group, and shall include —

(a) the internal control policies and procedures required under rule 4;

(b) policies and procedures for sharing information within the financial group where required for the purposes of customer due diligence and the management of money laundering, financing of terrorism and financing of proliferation risk;

(c) the provision, to group-level compliance, audit and anti-money laundering functions —

(i) of customer, account and transaction information from branches and subsidiaries where necessary for those purposes, including information and analysis of transactions or activities which appear unusual; and

(ii) where relevant to the management of risk, the fact that a suspicious transaction report or its underlying information has been submitted;

(d) the provision by the group-level functions referred to under subparagraph (c), to branches and subsidiaries, of the information referred to under that paragraph where relevant and appropriate to the management of risk; and

(e) adequate safeguards on the confidentiality and use of information exchanged within the financial group, including safeguards to prevent tipping-off.

(2) Where a licensee has a branch or majority-owned subsidiary in another country, the licensee shall ensure that the branch or subsidiary applies—

(a) measures consistent with these Rules and the Financial Transactions Reporting Act to the extent that the laws of that country permit; and

(b) where the laws of that country prevent the application of those measures, apply appropriate additional measures to manage the risks and inform the Commission of the same.

6. Appointment of Compliance Officer.

A Compliance Officer appointed by a licensee shall —

(a) be a person of a senior level; and

(b) have responsibility for establishing, implementing and maintaining policies, procedures and controls —

(i) to deter the use of a facility for money laundering, the financing of terrorism or the financing of proliferation;

(ii) to ensure the timely detection and reporting of suspicious activity; and

(iii) for the prompt investigation of suspicious activity.

7. Money Laundering Reporting Officer.

(1) A Money Laundering Reporting Officer shall —

(a) if an individual, be sufficiently senior in the organisational structure of the licensee's business operations to exercise the necessary authority to carry out the functions and duties of the office;

(b) if a legal person, be licensed under the Act to provide outsourced services as a MLRO;

(c) have responsibility for making suspicious transactions reports to the Financial Intelligence Unit regarding money laundering, terrorist financing and proliferation financing.

(2) A licensee shall submit the name of the person proposed to be the MLRO to the Commission, and where the person is appointed as the MLRO, the licensee shall —

(a) register the name of the person with the Financial Intelligence Unit;

(b) ensure that the MLRO or any person appointed to assist the MLRO has timely access to systems, customer records and relevant information required to perform the employee's, or the licensee's duties;

(c) notify the Commission before any change in such appointment and include in the notification a statement that the MLRO is a fit and proper person.

8. Outsourcing MLRO function.

(1) A licensee may outsource the role of the MLRO.

(2) Notwithstanding paragraph (1), a licensee shall retain ultimate responsibility for ensuring compliance with these Rules and the Financial Intelligence (Transactions Reporting) Regulations, 2001 *(S.I. No. 7 of 2001)*.

9. Suspicious transaction reporting.

(1) A licensee shall implement policies and procedures to facilitate an employee exercising that employee's duty to report their knowledge or suspicion that a customer is, may be, or is attempting or proposing to be engaged in money laundering, financing of terrorism and financing of proliferation to the MLRO.

(2) It shall be the responsibility of the MLRO to assess the sufficiency of the information contained in a report referred to under paragraph (1).

(3) Where, upon an assessment under paragraph (2), the MLRO knows, suspects or has reasonable grounds to suspect that a transaction, attempted transaction or proposed transaction involves the proceeds of criminal conduct, money laundering, the financing of terrorism or the financing of proliferation, the MLRO shall ensure that a suspicious transaction report is filed with the Financial Intelligence Unit in accordance with the Financial Transactions Reporting Act.

(4) In establishing and operating its systems for the detection of suspicious transactions and suspicious activity, a licensee shall have regard to —

(a) indicators of suspicious activity;

(b) the financial crime typologies relevant to its business; and

(c) any guidance concerning the detection or reporting of suspicious transactions issued by the Commission or the Financial Intelligence Unit,

and shall incorporate the relevant indicators into its monitoring systems and into the education and training provided under rule 26.

PART III – VERIFICATION OF CUSTOMER IDENTITY

10. Due diligence measures.

(1) Except where these Rules provide otherwise, the customer due diligence measures implemented by the licensee shall use reliable and independent source documents, data or information, whether or not electronically sourced.

(2) The risk rating framework of a customer shall be applied by a licensee to its due diligence measures.

(3) Once a business relationship has been established with a customer, the licensee shall take reasonable steps to ensure that due diligence measures are periodically reviewed and kept up to date.

(4) A licensee shall —

(a) apply customer due diligence measures to customers with which it has an existing business relationship on the basis of materiality and risk; and

(b) conduct due diligence on such existing relationships at appropriate times,

taking into account —

(i) whether and when customer due diligence measures were previously undertaken; and

(ii) the adequacy of the documents, data and information previously obtained.

11. Verification of customer identity.

(1) A licensee shall not enter into a business relationship with a person without applying customer due diligence measures to verify that person's identity.

(2) When verifying the identity of a person referred to under paragraph (1), the licensee shall —

(a) satisfy itself that the prospective customer is who the customer claims to be, and that any person acting on behalf of the customer is who that person claims to be and is properly authorised to act;

(b) ensure that sufficient information is obtained —

(i) on the nature of the business that the customer expects to undertake; and

(ii) concerning any expected or predictable pattern of transactions; and

(c) satisfy itself that any document produced by a prospective customer in support of identification verification is authenticated.

(3) Where a prospective customer fails or is unable to provide adequate evidence of identity, or a licensee is not satisfied that a new transaction with an existing customer is legitimate, the licensee shall determine if —

(a) other steps should be taken to verify the customer's identity;

(b) it is appropriate to proceed or continue with the business relationship.

(4) When verifying the identity of a customer, a licensee shall only accept certified copies of documents from a prospective customer where submission of original documents is impractical or impossible.

(5) A licensee shall apply enhanced customer due diligence measures where it is determined that a category of customer, business relationship, or transactions presents a higher risk for money laundering, the financing of terrorism, or the financing of proliferation.

(6) Notwithstanding any provision of these Rules, a licensee shall in each case, verify the identity of a customer, prospective or existing, where the licensee knows or suspects money laundering, the financing of terrorism, or the financing of proliferation and where such knowledge or suspicion arises, make a report to the Financial Intelligence Unit.

12. Use of a business relationship prior to completion of verification.

(1) For the purposes of section 8(3) of the Financial Transactions Reporting Act, a licensee may complete the verification of the identity of a customer or beneficial owner after the establishment of the business relationship only where —

(a) deferral of the verification is essential in order not to interrupt the normal conduct of business;

(b) the verification is completed as soon as reasonably practicable after the establishment of the business relationship; and

(c) the risks of money laundering, the financing of terrorism and the financing of proliferation are effectively managed in accordance with paragraph (2).

(2) A licensee that permits a customer to utilise a business relationship before the completion of verification shall adopt risk management procedures specifying the conditions under which the customer may do so, which shall include —

(a) limits on the number, types or amount of transactions that may be performed before the completion of verification; and

(b) the monitoring of large or complex transactions carried out outside the expected norms for that type of relationship.

(3) Where the verification is not completed within a reasonable period, the licensee shall —

(a) suspend activity on the account in accordance with rule 19(a);

(b) determine whether it is appropriate to continue the business relationship; and

(c) consider whether a suspicious transaction report should be filed with the Financial Intelligence Unit.

13. Simplified due diligence measures.

(1) A licensee may apply simplified due diligence measures to a customer, business relationship or transaction only where —

(a) the licensee has assessed the risk of money laundering, the financing of terrorism and the financing of proliferation associated with the customer, business relationship or transaction as low in accordance with its risk rating framework under rule 3, consistent with any risk assessment carried out at the national level and any regulatory guidance issued by the Commission;

(b) there is no suspicion of money laundering, the financing of terrorism or the financing of proliferation; and

(c) no higher risk circumstance of the kind referred to under rule 14 or under section 13 of the Financial Transactions Reporting Act applies.

(2) A licensee shall —

(a) document the basis for determining that a customer, business relationship or transaction presents a lower risk, together with the simplified due diligence measures applied;

(b) comply with any direction issued by the Commission not to apply, or to cease in applying, simplified due diligence measures.

(3) A licensee shall cease to apply simplified due diligence measures, and shall apply the due diligence measures otherwise required under these Rules, where the licensee knows or suspects money laundering, the financing of terrorism or the financing of proliferation, or where the risk associated with the customer, business relationship or transaction is no longer low.

14. Enhanced due diligence measures.

(1) A licensee shall apply enhanced customer due diligence measures for categories of customers, business relationships or transactions that present a higher risk for money laundering, the financing of terrorism or the financing of proliferation, based on the risk profile developed relative to the customer, business relationship or transaction.

(2) Without limitation, a higher risk may be presented where a customer or beneficial owner —

(a) is a politically exposed person within the meaning of rule 16;

(b) is from or established in, or is a party to a transaction connected with, a country which is identified by the IRF Steering Committee;

(c) presents complexity of ownership or legal structure with no apparent commercial justification;

(d) conducts transactions inconsistent in size, frequency or pattern with the customer's profile or known source of funds or wealth; or

(e) persistently avoids Know Your Customer thresholds through smaller transactions.

(3) A licensee when conducting enhanced due diligence measures shall —

(a) obtain additional information on the customer and the beneficial owner;

(b) establish the source of funds and source of wealth;

(c) obtain the approval of senior management before establishing or continuing the business relationship; and

(d) conduct enhanced ongoing monitoring.

15. Required information.

(1) A licensee shall obtain independent information and documentation appropriate to the nature and structure of the proposed customer when verifying the proposed customer's identity, which shall include, in the case of —

(a) a natural person —

(i) full and correct name or names;

(ii) at least two current means of contact, which may include a personal or business email address, a personal mobile or landline number, a business landline number, a personal, business or residential mailing address (including where applicable the street, post office box number, city, state or province, postal or zip code, landline telephone contact and

country), or any other means of contact which the Commission may specify;

(iii) date and place of birth; and

(iv) the purpose of the account and the nature of the business relationship;

(b) a legal person —

(i) the original or a certified copy of the certificate of incorporation or registration or the equivalent, and confirmation that the legal person has not been and is not in the process of being dissolved, struck off, wound up or terminated;

(ii) the resolution or mandate authorising the establishment of the facility and the persons authorised to act;

(iii) satisfactory evidence of the identity of all account signatories and of each natural person with a beneficial interest of ten per cent or more, with principal control over the legal person's assets, or who otherwise exercises control over the management of the legal person; and

(iv) the purpose of the account and the nature of the business relationship;

(c) a partnership or unincorporated business, a copy of the partnership agreement or constitutive document, the mandate authorising the facility, and satisfactory evidence of the identity of all partners, controllers and authorised signatories; and

(d) a trust, foundation or other legal arrangement, appropriate enquiries into the general nature and purpose of the arrangement and its source of funds, and satisfactory evidence of the identity of the settlor or founder, the trustees or council members, the protector (if any), all identifiable or known beneficiaries, and all persons exercising effective control over the arrangement.

(2) A licensee shall —

(a) review its records if a signatory, partner, controller, trustee or equivalent person is changed; and

(b) verify the identity of the new person before that person exercises control over the facility or funds.

16. Politically exposed persons.

(1) For the purposes of this rule —

"foreign politically exposed person" means an individual who is or has been entrusted with a prominent public function by a foreign country, including a head of state or of government, a senior politician, a senior government, judicial or military official, a senior executive of a state-owned corporation, or an important political party official;

"domestic politically exposed person" means an individual who is or has been entrusted with a prominent public function within The Bahamas, including a head of state or of government, a senior politician, a senior government, judicial or military official, a senior executive of a state-owned corporation, or an important political party official;

"international organisation politically exposed person" means an individual who is or has been entrusted with a prominent function by an international organisation, including a director, deputy director, member of the board or of senior management, or an individual entrusted with an equivalent function;

"family member" means an individual related to a politically exposed person directly or through marriage or a similar form of partnership, including a spouse or partner, parent, child or sibling; and

"close associate" means an individual who is closely connected to a politically exposed person, whether socially or professionally, and includes an individual who is in a position to conduct substantial domestic or international financial transactions on behalf of the politically exposed person.

(2) A licensee shall implement appropriate risk management systems to determine whether a customer or beneficial owner is a politically exposed person, a family member or a close associate.

(3) In relation to a foreign politically exposed person, whether as customer or beneficial owner, a licensee shall —

(a) obtain the approval of senior management before establishing the business relationship or, where the customer or beneficial owner becomes such a person after the establishment of the business relationship, before continuing the business relationship;

(b) take reasonable measures to establish the source of wealth and the source of funds of the customer or beneficial owner; and

(c) conduct enhanced ongoing monitoring of the business relationship.

(4) In relation to a domestic politically exposed person or an international organisation politically exposed person, a licensee shall take reasonable measures to determine whether a customer or beneficial owner is such a

person and, where the business relationship with such a person presents a higher risk, shall apply the measures set out under paragraph (3).

(5) Paragraphs (2), (3) and (4) apply, with the necessary changes, to a family member and close associate, and to any corporation, business or other entity formed by or for the benefit of a politically exposed person.

17. Reliance on third party verification procedures.

(1) A licensee may rely on the customer due diligence procedures implemented by another financial institution, provided that the financial institution is a regulated entity subject to AML/CFT/CPF obligations or is an entity located in a country which is not the subject of any list issued by an international organisation relative to the issues of money laundering, the financing of terrorism or the financing of proliferation and is able to —

(a) provide written confirmation that it has verified the identity of the relevant customer; and

(b) confirm the existence of the facility provided to the customer by the financial institution.

(2) Notwithstanding paragraph (1), a licensee shall only rely on the due diligence measures implemented by another financial institution with respect to those transactions, facilities or products which that other financial institution provides to the customer, and in any other circumstances, must undertake its own verification procedures.

18. Eligible introducer.

(1) A licensee's duty to verify the identity of prospective customers applies to any customer introduced by another financial institution, except where the financial institution is an eligible introducer.

(2) Where a licensee relies on the verification procedures of an eligible introducer, it shall obtain from that introducer —

(a) written confirmation that the eligible introducer has verified the customer's identity in accordance with the national laws applicable to the eligible introducer;

(b) certification that any photocopies provided are identical to the corresponding originals; and

(c) clear and legible copies of documentation, including where appropriate certified translations, within thirty days of receipt of the written confirmation referred to under subparagraph (a).

(3) For the purposes of this rule, an eligible introducer is —

(a) in relation to a domestic financial institution, a person —

(i) registered under Part VII of the Securities Industry Act;

(ii) licensed as an investment fund administrator under the Investment Funds Act;

(iii) licensed as a bank or trust company by the Central Bank of The Bahamas under the Banks and Trust Companies Regulation Act; or

(iv) carrying on life assurance business pursuant to the Insurance Act (*Ch. 347*); and

(b) in relation to a foreign financial institution, an institution which exercises functions similar to those of a domestic financial institution referred to under subparagraph (a), is located in a country which is not listed by the IRF Steering Committee, and has no obstacles, administrative or otherwise, which would prevent the licensee from accessing the original documentation.

19. Suspension or termination of activity or business.

A licensee shall —

(a) suspend activity on the account of a prospective customer, if reasonable efforts have been made to directly verify the prospective customer's identity without success; and

(b) terminate the business relationship with a prospective customer where it is unable to obtain the relevant information and documentation from the eligible introducer within thirty days of receiving the eligible introducer's confirmation.

20. Ongoing monitoring.

A licensee shall, after the verification procedures have been concluded and a business relationship has been established —

(a) monitor the conduct of the relationship on an ongoing basis, including scrutiny of transactions undertaken throughout the relationship, to ensure that the transactions are consistent with the licensee's knowledge of the customer and the customer's business and risk profile, including where necessary the customer's source of funds; and

(b) ensure that the conduct of the relationship remains consistent with the nature of the business stated when the relationship was established.

PART IV – TARGETED FINANCIAL SANCTIONS

21. Targeted financial sanctions.

(1) A licensee shall establish and maintain policies, procedures, systems and controls to ensure its compliance with targeted financial sanctions, which shall include the implementation of sanctions against a designated person or entity, pursuant to section 3A of the International Obligations (Economic and Ancillary Measures) Act and section 44 of the Anti-Terrorism Act to —

(a) freeze, without delay or notice to the designated person or entity, funds or other assets —

(i) of designated persons and entities that are owned or controlled, by designated persons or entities;

(ii) derived or generated from funds or other assets owned or controlled by designated persons or entities;

(iii) of persons and entities acting on behalf of or at the direction of a designated person or entity;

(b) inform the Attorney-General and the Financial Intelligence Unit that it holds funds and other assets owned or controlled by a designated person or entity; and

(c) inform the designated person or entity that the funds held by the licensee have been frozen.

(2) A licensee shall cooperate with any legal action for the forfeiture or confiscation of any money, asset or property frozen in accordance with the implementation of targeted financial sanctions.

(3) For the purposes of paragraph (1) —

(a) funds or other assets owned or controlled by a designated entity includes money, property, tangible or intangible assets;

(b) owned or controlled includes whole or joint ownership or direct or indirect control.

PART V – RECORD KEEPING

22. Maintenance of records.

(1) A licensee shall, in compliance with relevant laws, prepare and maintain records of its business relationships and transactions that enable —

(a) competent third parties to assess the licensee's compliance with AML/CFT/CPF policies and procedures;

(b) transactions effected through the licensee to be reconstructed;

(c) the licensee to satisfy court orders or enquiries from the Commission or appropriate authorities; and

(d) the identification of the customer.

(2) A licensee shall keep records required to be maintained by these Rules, for a period of seven years from the date that the customer ceases to be a customer.

(3) For the purpose of paragraph (2), a person ceases to be a customer from the date of —

(a) the carrying out of a one-off transaction or the last transaction in a series of transactions;

(b) the closing of the account or accounts or the ending otherwise of the business relationship; or

(c) the commencement of proceedings to recover debts payable on insolvency.

(4) The seven-year period referred to under paragraph (2) commences on the date of the completion of the last transaction where formalities to end a business relationship have not been undertaken but a period of seven years has elapsed since the date of the last transaction.

(5) Where the licensee is a company that is being liquidated, the liquidator shall retain the relevant records of the licensee for the balance of the prescribed period remaining at the date of dissolution.

(6) The records may be maintained in the form of original documents or electronic media, in a form which enables the relevant customer to be identified, and the customer's identity as verified, to be established.

23. Verification records.

A licensee shall maintain the records generated by the verification of the identity of a facility holder and of any non-facility holder in relation to a facility, in accordance with rule 22.

24. Transaction records.

A licensee shall maintain transaction records containing —

(a) a description of the nature of the transaction;

(b) details of the transaction, including the amount of the transaction and the denomination of the currency;

(c) the date on which the transaction was conducted;

(d) the identification verification details of the parties to the transaction;

(e) where applicable, information on the facility through which the transaction was conducted and any other facility directly involved in the transaction; and

(f) the files, business correspondence and records connected to the facility.

25. Other records.

A licensee shall maintain records of —

(a) suspicions raised internally by or with the Money Laundering Reporting Officer, but not disclosed to the relevant authorities;

(b) suspicions which the Financial Intelligence Unit or the Commission have advised are of no interest;

(c) findings of inquiries conducted by the licensee~~;~~ into unusual activity.

PART VI – MISCELLANEOUS

26. Education and training.

(1) A licensee shall take appropriate measures to ensure that every employee is aware of —

(a) policies and procedures put in place to detect and prevent money laundering and to counter the financing of terrorism and to counter the financing of proliferation, including those for the identification, record keeping, detection of unusual and suspicious transactions and internal reporting; and

(b) the AML/CFT/CPF legislative framework.

(2) A licensee shall provide every employee with the relevant training in the recognition and handling of suspicious transactions.

27. Revocation of S.I. No. 11 of 2019.

The Financial and Corporate Service Providers (Anti-Money Laundering and Countering the Financing of Terrorism) Rules, 2019 are hereby revoked.

Made this 27th day of October, 2026.

Signed
PETER T. CAREY
DEPUTY CHAIRMAN
SECURITIES COMMISSION OF THE BAHAMAS