For Public Consultation:
DRAFT DIGITAL ASSETS AND REGISTERED EXCHANGES (ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM) RULES, 2022

The Securities Commission of The Bahamas ("the Commission"), in exercise of its powers conferred by section 50 of the Digital Assets and Registered Exchanges Act, 2020 (No.28 of 2020), has issued draft Digital Assets and Registered Exchanges (Anti-Money Laundering and Countering the Financing of Terrorism) Rules, 2022 for public consultation. The draft Rules may be found on the Commission's website: https://bit.ly/3JSMJUL .

Summary
The draft Digital Assets and Registered Exchanges (Anti-Money Laundering and Countering the Financing of Terrorism) Rules, 2022 ("the Rules") will establish a legislative anti-money laundering (AML) and countering the financing of terrorism (CFT) framework applicable to Digital Asset Businesses registered under the Digital Assets and Registered Exchanges Act, 2020.

These draft Rules are aligned with international standards and developments with respect to AML/CFT requirements for virtual asset service providers. The draft Rules establish the mandatory standards with which applicable registrants under DARE must comply in order to implement the requirements of AML/CFT legislation, including the Financial Transactions Reporting Act, 2018, the Proceeds of Crime Act, 2018 and the Anti-Terrorism Act, 2018.
The draft Rules principally address:

- Implementation of risk rating framework;
- Internal control procedures including suspicious transaction reporting;
- Customer identity verification, including third party verification and eligible introducers; and
- Record keeping.

In addition to these core AML/CFT standards, the draft Rules include requirements that take into account some particular characteristics of virtual assets.

Scope
Once promulgated, the Rules will apply to Digital Asset Businesses registered under the Digital Assets and Registered Exchanges Act, 2020.

Consultation Period
The consultation period commences on **30 March 2022** and ends on **29 April 2022**, during which time the Commission invites the public to share comments with regard to the draft Digital Assets and Registered Exchanges (Anti-Money Laundering and Countering the Financing of Terrorism) Rules, 2022. Comments may be submitted via email to DAREconsultation@scb.gov.bs.

Alternatively, comments may be submitted by hand to:

Christina Rolle
Executive Director
Securities Commission of The Bahamas
Poinciana House
31A East Bay Street
Nassau, Bahamas

Issued: 30 March 2022

DIGITAL ASSETS AND REGISTERED EXCHANGES (ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM) RULES, 2022

Arrangement of Rules

Rule

DIGITAL ASSETS AND REGISTERED EXCHANGES ACT 2020

(CHAPTER___)

DIGITAL ASSETS AND REGISTERED EXCHANGES (ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM) RULES, 2022

The Securities Commission of The Bahamas, in exercise of the powers conferred by section 50 of the Digital Assets and Registered Exchanges Act 2020 (No. 28 of 2020) makes the following Rules –

PART I - PRELIMINARY

1. Citation

These Rules may be cited as the Digital Assets and Registered Exchanges (Anti-Money Laundering and Countering the Financing of Terrorism) Rules, 2022.

2. Interpretation

In these Rules -

"Act" means the Digital Assets and Registered Exchanges Act 2020;
"beneficial owner" has the meaning specified in the Register of Beneficial Ownership Act 2018;
"digital assets" has the meaning specified in section 2 of the Act;
"financial institution" has the meaning specified in the Financial Transaction Reporting Act 2018;
"identified risks" has the meaning specified in the Proceeds of Crime Act, 2018;
"key personnel" means senior management or other key employees who effectively manage the business of a registrant;
"Money Laundering Reporting Officer" or "MLRO" means the person appointed pursuant to regulation 5 of the Financial Intelligence (Transactions Reporting) Regulations;
"occasional transactions" has the meaning specified in the Financial Transactions Reporting Regulations, 2018 regarding digital assets;
"registrant" means a person registered under the Act;
"senior management" means an officer or employee of a registrant with sufficient knowledge and seniority to make decisions affecting the registrant's risk exposure and need not involve a member of the board or directors and includes a person responsible for compliance or duly authorised to bind the registrant;
"The Commission" means the Securities Commission of The Bahamas as continued under Part II of the Securities Industry Act, 2011.

PART II – RISK RATING

3. Duty of registrant to implement risk rating framework

(1) Every registrant shall implement a risk rating framework which assesses and identifies –

(a) the risk profile of each customer;
(b) its own risk profile in relation to the countries or jurisdictions in which it operates;
(c) the risk profile associated with its own business practices, products, services, transactions and delivery channels;
(d) the nature and extent of risks related to the registrant's non-face-to-face business relationships; and

(e) the nature and extent of risks related to the registrant's business activities that permit customers to receive payments from unknown or unassociated third parties.

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

(a) take appropriate measures to continuously identify, measure, manage, and mitigate identified current and emerging risks;
(b) take account of any risk assessment carried out at the national level and any regulatory guidance issued by the Commission;
(c) categorize customer relationships and products to identify the level of risk associated with each customer relationship or product;
(d) categorize 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;
    ix. non-face-to-face KYC document submission; and
    x. adherence to customer activity profile;
(e) address which level of management can approve a decision for the registrant 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;
(g) require the periodic review of the customer relationship or product to –
    i. ensure that the categorizations are current and appropriate; and
    ii. enable the registrant to determine whether any adjustment should be made to the risk rating;
(h) require the re-categorization of a customer relationship or product offered by the registrant in the event of a change in the risk profile of a customer relationship or product;
(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 particular customer relationship or product;
(j) mitigate any additional risks due to the cross-border nature of a transaction, particularly where the transaction takes place in a jurisdiction which could reduce the registrant's ability of oversight and the application of effective AML/CFT controls;
(k) identify and mitigate potential risks arising from products, services or activities, provided to or by anonymous or private sources including, but not limited to, unhosted wallets, the darknet and blacklisted addresses, particularly where the risk rating is high or where the type, size and volume of transactions is substantial.

(3) A registrant 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 such product, business practice or technology.

(4) The outcome of each customer or product risk assessment conducted shall be documented and retained as part of the registrant's document keeping requirements.

(5) A registrant's risk rating framework shall be subject to review by the Commission.

PART III – INTERNAL CONTROLS

4. Duty of registrant concerning internal controls

(1) A registrant shall implement internal control policies and procedures for the prevention, detection, and disclosure of identified risks associated with money laundering and the financing of terrorism and proliferation, in accordance with the Financial Transactions Reporting Act, 2018[1] and –

(a) document and track financial crime typologies specific to digital assets;
(b) have a MLRO approved by the Commission; and
(c) verify, on a regular basis, compliance with internal policies, procedures, and controls relating to money laundering and terrorism and proliferation financing activities.

(2) A registrant shall comply with the provisions of the Financial Transactions Reporting (Wire Transfers) Regulations, 2018 and ensure proper internal controls are in place.

(3) A registrant shall ensure it understands its operating processes and procedures, regularly verifies their integrity, and accounts for identified money laundering and terrorist and proliferation financing risks.

5. MONEY LAUNDERING REPORTING OFFICER

(1) A Money Laundering Reporting Officer shall –

(a) if an individual, be sufficiently senior in the organizational structure of the registrant's business operations to exercise the necessary authority to carry out their functions and duties;
(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, and terrorism and proliferation financing.

(2) A registrant 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 registrant shall –

[1] *(S.I. No. 5 of 2018).*

(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 all relevant information required to perform their duties; and
(c) notify the Commission prior to any change in such appointment and include in the notification a statement that the MLRO is a fit and proper person.

6. Outsourcing

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

(2) Notwithstanding paragraph (1), a registrant shall retain ultimate responsibility for ensuring compliance with the provisions of the Financial Intelligence (Transactions Reporting) Regulations.

7. Suspicious transaction reporting

(1) A registrant shall implement policies and procedures to facilitate an employee exercising their duty to report their knowledge or suspicions that a customer is or may be engaged in money laundering or the financing of terrorism and 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 in paragraph (1).

PART IV – VERIFICATION OF CUSTOMER IDENTITY

8. Due diligence measures

(1) Except where specifically exempted by any Rules issued by the Commission, the customer due diligence measures implemented by the registrant shall use independent and reliable source documents, data or information (whether or not electronically sourced).

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

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

9. Simplified due diligence

(1) If a transaction or a business relationship with a customer presents a low degree of risk for money laundering, or terrorism or proliferation financing, a registrant may apply simplified due diligence measures.

(2) Simplified due diligence measures shall only be applied in limited circumstances.

(3) Where simplified due diligence measures are applied, a registrant shall clearly document the risk assessment undertaken to justify the use of simplified due diligence measures.

(4) Simplified due diligence measures should be commensurate with the lower risk factors and may vary depending on the risk.

(5) Simplified due diligence measures may include, but are not limited to, postponing verification of a customer's identity until the risk is no longer deemed to be low or where a transaction exceeds a particular threshold set by the registrant.

(6) A business relationship or transaction may present a lower risk for money laundering, or terrorism or proliferation financing if, without limitation:

(a) the product, service or activity is considered to be low risk which may include cases where there are limitations on use, on the transaction volumes or amounts;
(b) digital assets are funded through a bank in a jurisdiction determined as low risk or with equivalent AML/CFT legal requirements;
(c) the source or destination address of digital asset has been whitelisted or otherwise determined as low risk; and
(d) the results of blockchain or similar analysis indicate a lower risk.

10. Enhanced due diligence measures

(1) Enhanced due diligence measures shall be applied by a registrant for categories of customers, business relationships, or transactions that may present a higher risk for money laundering, or terrorism or proliferation financing based on the risk profile developed relative to the customer, business relationship or transaction, which measures shall include taking additional verification measures.

(2) A customer may present a higher risk for money laundering, or terrorism or proliferation financing if, without limitation, a customer:

(a) is involved in digital asset mining operations (either directly or indirectly through relationships with third parties) that take place in a high-risk jurisdiction, relate to higher-risk digital assets including, without limitation, those with anonymity enhancing features, or where its organisation gives rise to higher risk;
(b) is unable to produce the required Know Your Customer information and documentation;
(c) uses anonymous or randomly generated email addresses or a temporary email service;
(d) requests an exchange to or from cash or other digital assets with anonymity enhancing features;
(e) persistently avoids Know Your Customer thresholds through smaller transactions;
(f) requests an exchange to or from state-sponsored digital assets that are suspected of being used to avoid sanctions;
(g) is a politically exposed person as defined in Rule 13.

(3) A transaction may present a higher risk for money laundering, or terrorism or proliferation financing if, without limitation:

(a) it is a peer-to-peer transaction;

(b) a significant proportion of the digital assets held or used in a transaction is associated with anonymity enhancing features or products and services that potentially obfuscate transactions or undermine a registrant's ability to know its customers and implement effective AML/CFT controls;

(c) the digital asset comes from, or is associated with, the darknet or other illegal/high-risk sources, such as an unregulated exchange, or is associated with market abuse, ransomware, hacking, fraud, Ponzi schemes or sanctioned digital asset addresses or accounts;

(d) the results of blockchain or similar analysis indicate a higher risk.

(4) Enhanced due diligence measures may include –

(a) corroborating the identity information received from the customer with information in third-party databases or other reliable sources;

(b) for non-face to face Know Your Customer verification:

i. video conferencing with the proposed customer;

ii. requiring identification documentation to be certified by a notary public or the equivalent;

iii. verifying with the customer, additional aspects of their identity (or biometric data) which is held electronically;

(c) tracing the customer's IP address;

(d) corroborating activity information consistent with the customer's transaction profile;

(e) obtaining additional information on the source of funds and source of wealth of the customer;

(f) obtaining information on the reasons for the intended or performed transaction;

(g) enhanced monitoring of the business relationship and transactions;

(h) requesting data relating to transaction and trading history.

11. Verification of customer identity

(1) Subject to Rule 9(5) above, a registrant shall not enter into a business relationship or execute an occasional transaction with any person without applying customer due diligence measures to verify the identity of the person,including any beneficial owner(s).

(2) When verifying the identity of a person referred to in paragraph (1), the registrant shall –

(a) satisfy itself that the prospective customer is who the customer claims to be by applying the customer due diligence measures referred to in Rules 8 to 10;

(b) ensure that sufficient information is obtained and documented –

i. on the nature and purpose of the business that the customer intends to undertake; and

ii. concerning any expected or predictable volume and pattern of transactions and activities; and

(c) satisfy itself that any independent and reliable source documents, data or information (whether or not electronically sourced) sufficiently verifies a customer's identity.

(3) Where a prospective customer fails or is unable to provide adequate evidence of identity, or a

registrant is not satisfied that a new transaction with an existing customer is legitimate, the registrant shall –

(a) determine whether –
    i. other steps should be taken to verify the customer's identity;
    ii. it is appropriate to proceed or continue with the business relationship; and
(b) file a suspicious transaction report with the Financial Intelligence Unit.

(4) Registrants shall have a clear policy regarding the escalation of decisions to senior management concerning the acceptance or continuation of high-risk business relationships.

(5) When verifying the identity of a customer, a registrant shall only accept either:
(a) original documents;
(b) certified copies of documents from a prospective customer where submission of original documents is impractical or impossible; or
(c) independent and reliable source documents, data or other information (whether or not electronically sourced) which sufficiently verifies a customer's identity.

(6) Notwithstanding any provision of these Rules, a registrant shall in all cases verify the identity of a customer, prospective or existing, where the registrant knows or suspects money laundering, or terrorist or proliferation financing, and where such suspicion or knowledge is confirmed, shall make a report to the Financial Intelligence Unit.

12. Required information

(1) Every registrant shall obtain independent and reliable source documents, data or other information (whether or not electronically sourced) appropriate to the nature and structure of the proposed customer when verifying the proposed customer's identity, which shall include, but is not limited to the following, in the case of –

(a) a natural person –
    i. full and correct name(s);
    ii. at least two current means of contact which may include:
        aa. personal email address;
        bb. business email address;
        cc. personal mobile telephone number;
        dd. personal landline number;
        ee. business landline number;
        ff. personal mailing address, which must include where applicable, the street, post office box number, city, state or province, postal or zip code, landline telephone contact, and country;
        gg. business mailing address, which must include where applicable, the street, post office box number, city, state or province, postal or zip code, landline telephone contact, and country;
        hh. residential mailing address, which must include where applicable the street, post office box number, city, state or province, postal or zip code, landline

telephone contact, and country; or

ii. any specific means of contact which the Commission may specify;

iii. date of birth;

iv. country of domicile; and

v. the purpose of the account and nature of the business relationship;

(b) a corporate customer –

i. the original or a certified copy of the certificate of Incorporation, Registration or the equivalent;

ii. certificate of good standing or the equivalent evidence that the company has not been or is not about to be struck off the register or wound up;

iii. a copy of the relevant board resolution authorizing the establishment of the business relationship, or authorizing the opening of an account and conferring permission on any person authorized to undertake transactions;

iv. satisfactory evidence of the identity of all persons authorized to undertake transactions and details of their relationship with the company; and

v. satisfactory evidence of identification of each natural person having a beneficial interest of ten percent or more of the company, or having principal control over the company's assets or otherwise exercising control over the management of the company;

(c) a partnership or unincorporated business –

i. a copy of the partnership agreement or document establishing the partnership agreement, or document establishing the partnership or unincorporated business;

ii. a mandate authorizing the establishment of the business relationship or the opening of an account, and conferring permission on any person authorized to undertake transactions;

iii. satisfactory evidence of the identity of all partners and controllers of the firm or business; and

iv. satisfactory evidence of the identity of all persons authorized to undertake transactions;

(d) other legal structures and fiduciary arrangements, such as trusts, fiduciary or nominee structures –

i. the applicable documents establishing the legal structure or fiduciary or nominee arrangement;

ii. all applicable documents, identifying persons exercising effective control over the legal structure or fiduciary or nominee arrangement, including the power to direct, withhold, consent to or veto the exercise of any power related to the legal structure or fiduciary or nominee arrangement;

iii. satisfactory identification evidence of all persons providing funds or assets to the structure;

iv. all applicable documents, identifying the known beneficiaries of the trust;

v. all applicable documents, identifying all beneficiaries of a fiduciary or nominee structure;

vi. all applicable documents, appointing and identifying any signatory powers in relation to the legal structure or fiduciary or nominee arrangement; and

vii. satisfactory evidence of the identity of all persons authorized to undertake transactions;

(e) a foundation –

i. the foundation Charter;
ii. the foundation's certificate of registration issued by the Registrar General, or the foreign equivalent;
iii. the source of funds, and where a person other than the founder provides funds for the foundation, verification of the identity of the third party providing the funds or for whom the founder may be acting;
iv. identification evidence of each founder, officer, and council member of the foundation as may be signatories for the accounts of the foundation;
v. identification evidence of beneficiaries that hold a vested interest in the foundation; and
vi. satisfactory evidence of the identity of all persons authorized to undertake transactions;

(f) a non-profit association or charity –
i. identification evidence of at least two signatories, and anyone authorized to give instructions on behalf of the entity;
ii. the nature of the proposed association's or charity's purpose and operations;
iii. the source of funds; and
iv. satisfactory evidence of the identity of all persons authorized to undertake transactions;

(g) powers of attorney –
i. identification of each donee;
ii. identification evidence of the donor;
iii. proof of any third party mandates; and
iv. satisfactory evidence of the identity of all persons authorized to undertake transactions.

(2) A registrant shall, in the case of services being provided to the estate of a deceased person, obtain identification evidence of each personal representative of the said estate.

(3) A registrant shall review its records periodically to ensure that the identification and other information kept by it is current and reflects the existing facts related to a customer, and in all cases when there have been changes to –
(a) persons authorized to undertake transactions;
(b) board resolutions or mandates authorizing the opening of an account and authorizing any person to undertake transactions;
(c) partners, controllers, trustees, fiduciaries or nominees; and
(d) the corporate structure of a customer.

(4) Where there has been a change to any of the items specified in paragraph (3), the registrant shall undertake the verification process in compliance with the provisions of this paragraph.

(5) For the purpose of the verification process, a registrant shall exercise additional care in relation to the provision of trading services with respect to digital assets with anonymity enhancing features or that obscure a user's identity or other transactional information.

(6) Where a registrant offers the service specified in paragraph (5), the registrant shall independently verify the identity of the proposed facility holder and any beneficial owner(s)

through reliable and independent source documents, data, or information.

(7) In all cases, a registrant shall maintain adequate documentation to evidence the implementation of due diligence measures and shall ensure that the verification of identification procedures implemented, are appropriate to the nature and structure of the proposed customer being verified.

(8) A registrant shall, as part of due diligence measures, implement procedures for the periodic re-verification of customers, which at the minimum, shall require re-verification to occur where –

(a) during the course of the business relationship, the registrant has reason to doubt the identity of the customer;
(b) there is a material change in the way transactions are undertaken; or
(c) there is a reasonable suspicion that any transaction carried out by the customer might have breached the law concerning money laundering, or the financing of terrorism or proliferation.

13. Politically Exposed Persons

(1) A registrant shall, in addition to applying enhanced due diligence measures, develop clear procedures and controls for the identification and verification of a politically exposed person when -

(a) establishing a business relationship with that politically exposed person, or a legal person in which the politically exposed person –
i. is a director, officer, founder or council member;
ii. is a partner or trustee;
iii. is a signatory or person authorized to undertake transactions;
iv. has a beneficial interest of ten per cent or more in the legal person;
v. has principal control over the legal person's assets;
vi. exercises control over the management of the legal person; or
(b) the registrant is continuing a business relationship with a customer who has become a politically exposed person, after the establishment of the business relationship.

(2) For the purposes of this Rule the terms set out below are defined as follows:

"**international organization**" means an entity established by a formal political agreement equivalent in status to an international treaty, made between, and recognized by law, in member countries, and which is not treated as a resident institutional unit of the countryin which it is located.

"politically exposed person" means:
(a) an individual who is or has been entrusted with:
i. a prominent public function within The Bahamas, inclusive of a head of state or government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation, or an important political party official;
ii. a prominent public function by a foreign jurisdiction, inclusive of, a head of state or government, senior politician, senior government, judicial or military official, senior

executive of a state-owned corporation, or senior political party official; or

iii. a prominent function within an international organization, including directors, deputy directors, members of the board, members of senior management, or individuals who have been entrusted with equivalent functions;

(b) an individual who is related to a politically exposed person, including a parent, child, spouse or sibling;

(c) an individual who is closely associated to a politically exposed person either socially, or professionally and includes a person who can conduct substantial domestic or international financial transactions on behalf of the politically exposed person;

(d) any corporation, business or other entity formed by or for the benefit of a head of state, head of government or individuals referred to in paragraph (a) above.

14. Reliance on third party verification procedures

(1) A registrant may rely on the customer due diligence procedures implemented by another virtual asset service provider or financial institution, provided that the virtual asset service provider or financial institution is a regulated entity subject to AML/CFT obligations and is an entity located in a country which is not the subject of any list issued by an international organization relative to the issues of money laundering, or terrorism or proliferation activities, 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 account or facility provided to the customer by the virtual asset service provider or financial institution.

(2) Notwithstanding paragraph (1), a registrant shall only rely on the due diligence measures implemented by another virtual asset service provider or financial institution with respect to those categories of transactions, services, or products which that other virtual asset service provider or financial institution provides to the customer, and in all other circumstances, must undertake its own verification procedures.

15. Eligible introducer

(1) In all cases, a registrant's duty to verify the identity of all prospective customers shall apply to any customer introduced by another virtual asset service provider or financial institution, except where a virtual asset service provider or financial institution is an eligible introducer.

(2) Where a registrant 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 of the eligible introducer;

(b) certification from the eligible introducer that any photocopies provided to the registrant are identical to the original document; and

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

(3) For the purposes of this paragraph, an eligible introducer shall be –

(a) in relation to a domestic financial institution –
   i. a person registered under Part VI of the Securities Industry Act, 2011 (No. 10 of 2011);
   ii. an investment fund administrator licensed under section 34 of the Investment Funds Act 2019;
   iii. a bank or trust company licensed by the Central Bank of The Bahamas under the Banks and Trust Companies Regulation Act 2020;
   iv. a digital asset business registered under the Act; or

(b) in relation to a foreign virtual asset service provider or financial institution, a service provider or institution –
   i. exercising functions similar to a domestic digital asset business or financial institution to which subparagraph (a)(i) through (iv) applies;
   ii. registered or functioning pursuant to Part VI of the Securities Industry Act, 2011 (No. 10 of 2011);
   iii. located in a country which is not the subject of any list issued by an international organization relative to the issues of money laundering or terrorism or proliferation activities; and
   iv. having no obstacles administrative or otherwise which would prevent the registrant from accessing the original documentation.

16. Suspension or termination of activity or business

A registrant 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.

17. Exemption from verification of identity

A registrant shall not be required to verify the identity of a prospective customer where that customer is –

a. a digital asset business or financial institution licensed or registered by the Central Bank of The Bahamas, the Securities Commission of The Bahamas, The Insurance Commission of The Bahamas, or the Gaming Boardfor The Bahamas;
b. a virtual asset service provider or financial institution which –
   i. is subject to anti-money laundering and countering the financing of terrorism obligations;
   ii. is under supervision for compliance with the obligations referred to subparagraph (i) and;
   iii. has adequate procedures for compliance with customer due diligence and record keeping requirements;
c. any central or local government agency or statutory body;
d. a publicly traded company listed on The Bahamas International Stock Exchange or any other

marketplace registered by the Commission and specified in the Schedule to the Financial Transactions Reporting Regulations, 2018[2].

18. Ongoing monitoring

(1) A registrant shall, after the verification procedures have been concluded and a business relationship has been established –

(a) monitor the conduct of the business relationship periodically; and
(b) ensure, on an ongoing basis, that the business relationship is consistent with the risk profile and nature of the business stated when the relationship was established.

(2) Ongoing monitoring of business relationships includes, without limitation:

(a) scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the registrant's knowledge of the customer, their business and risk profile;
(b) ensuring that the source documents, data or other information obtained for the purposes of applying due diligence are kept up to date;
(c) analysing blockchain and similar transactions in line with a risk-based approach including, without limitation, taking into account the nature of the registrant's business and whether it is appropriate to use such analysis for all transactions;
(d) where large volumes of transactions occur on a regular basis, using automated systems to monitor transactions provided that flagged transactions are subject to human expert analysis to determine whether such transactions are suspicious.

PART V – RECORD KEEPING

19. Maintenance of records

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

(a) competent third parties to assess the registrant's compliance with AML or CFT policies and procedures;
(b) transactions effected through the registrant to be reconstructed;
(c) the registrant to satisfy court orders or enquiries from the Commission or appropriate authorities; and
(d) the identification of customers.

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

(3) For the purpose of paragraph (2), a person ceases to be a facility holder from the date of –

[2] *(S.I. No 35 of 2018).*

(a) the carrying out of a one-off transaction or the last transaction in a series of transactions;
(b) the closing of the account(s) 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 in 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 registrant is a company that is being liquidated, the liquidator shall retain the relevant records of the regulated person for the balance of the prescribed period remaining at the date of dissolution.

(6) A registrant may maintain records in the form of original documents or other electronic media.

20. Transaction records

A registrant 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. the public keys (or equivalent identifiers) of relevant parties;
f. where applicable, information on the facility through which the transaction was conducted and any other facility directly involved in the transaction; and
g. the files, business correspondence, and records connected to the facility.

21. Other records

A registrant shall maintain records of –

a. suspicions raised internally by the Money Laundering Reporting Officer, but not disclosed to the relevant authorities;
b. suspicions which the Financial Intelligence Unit, the Commissioner of Police, or the relevant supervisory authority have advised are of no interest; and
c. findings of inquiries conducted by the regulated person into unusual activity.

PART VI – MISCELLANEOUS

22. Education and training

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

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

(2) A registrant shall ensure that:

(a) the relevant staff members and key personnel are trained on an ongoing basis to:
   i. identify, prevent, detect and disclose financial crime risks;
   ii. recognise and handle suspicious transactions;
(b) its key personnel possess the adequate knowledge, skills, experience and capability to understand the registrants' business and customer needs;
(c) key personnel and staff are aware of their obligations to comply with policies and procedures.

Made this_____day of_____, 2022.

Signed
Chairman
Securities Commission of The Bahamas