INTERNAL USE ONLY

24 Exchange

Anti-Money Laundering, Anti-Terrorist Financing (AMLATF) & Sanctions

Policies and Procedures

Updated June 2022

This set of AMLATF & Sanctions Policies and Procedures is the sole property of 24 Exchange Bermuda Limited, including its Parent, 24X Bermuda Holdings LLC and its Bermuda based operating affiliates and subsidiaries[1] (collectively, **24 Exchange** or the **Company**) and must be returned to the Company should an employee's association with the Company terminate for any reason or no reason. The contents of these policies are procedures are confidential and proprietary. Employees and consultants may not reproduce, duplicate, copy, or make extracts from or abstracts of these policies and procedures or otherwise make it available in any form to non- employees or consultants without prior written approval.

A declaration by all Employees must be executed acknowledging awareness and review of these AMLATF & Sanctions Policies and Procedures.

[1] Affiliates include 24 Exchange Broker Limited

Contents

1 OVERVIEW

1.1 Introduction

24 Exchange is a group of Bermuda-domiciled entities that operate a multi-asset electronic trading platform (**Platform**)[2] and offer counterparty execution. It does not maintain any premises or offices in Bermuda. 24 Exchange is carrying on digital asset business (**DAB**) within the meaning of the Digital Asset Business Act 2018 (**DABA**) and is a regulated financial institution (**RFI**) for the purposes of the Proceeds of Crime Act 1997 (**POCA**) and the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 (**AMLATF Regulations**). The Company is enabling the 24 hours matching trades of fiat or cryptocurrencies (both convertible and non-convertible) in deliverable and non-deliverable (Fiat-only settlement) contracts between a pre-approved set of institutional clients (counterparties or Participants) through its licensed proprietary multi-asset trading technology platform, the 24 Exchange Platform (**Platform**). In some instances, 24 Exchange Broker Limited will act as a counterparty to the trades.

The Company is committed to participating in efforts to identify, prevent, and combat money laundering activities and the financing of terrorist activities. The Company does not provide clearing or settlement services,nor does it maintain depository accounts for anyone admitted to trade on the Company's trading platform (**Participants**).

Additionally, in connection with offering a DAB Platform, the Company will periodically contract with one or more custodians or agents (hereinafter, an **Agent**) to facilitate the storage of digital assets, on and off-chain settlement, and provide verifiable proof of assets for transactions. All Agents will undergo screening and due diligence prior to engagement.[3]

The Company has adopted these Anti-Money Laundering[4] (**AML**) Policies and Procedures (**AML Plan**) to ensurethat the Company is not exploited or manipulated by money launderers, prevent the Company from being associated with money laundering (**ML**) or terrorist financing (**TF**), and assure Participants or Agents that engaging with in transactions with counterparty-Participantswill not result in facilitating money laundering or funding of terrorists and/or other criminal activities including the breach of international financial or trade sanctions. This AML Plan sets out the framework by which the Company will manage the ML/TF and Sanctions and extends out to any active subsidiaries of the Company.

This AML Plan is intended solely for the use of, and is binding upon, all Company employees and consultants. Willful or grossly negligent failure of an employee to follow this AML Plan may be grounds for discipline, including and up to termination, and may in certain circumstances, expose the employee to criminal prosecution, fine, and/or imprisonment. Adherence to this AML Plan is critical, and all employees and consultants, particularly those involved with Participant or Agent onboarding, areexpected to be familiar with it.

1.2 Risk-Based Approach

This AML Plan was developed considering the size, complexity, and regulatory oversight of the Company's business and business activities. As the Company's Participant base grows, both in size and/or diversity of Participant types and locations,the Company will review and update this AML Plan as needed.

In order to adopt a risk-based approach, ML/TF and Sanctions risk (**Risks**) must be identified in order to enable the development of strategies to manage and mitigate those identified risk. The risk from any particular combination of, including but not limited to customer, product, service, and transaction, the more onerous the mitigation measures must be.

The Bermuda National Risk Assessment (**NRA**) of 2018[5] has been taken under consideration in considering the Risks posed to the business of the Company. While it does not cover the digital asset sector, it does rank the Securities sector

[2] The Company does not have any branches.

[3] See Appendix D2: Agent Due Diligence

[4] In this set of policies and procedures, unless otherwise indicated, references to AML include references to ATF.

[5] https://www.gov.bm/sites/default/files/9171_Public%20NRA%20Report_Final_3.pdf

(Chapter 8) as having a high inherent risk for ML primarily due to the diverse international client base and high dollar values generally managed in the sector. The overall threat for ML to Bermuda was placed at medium-high with financial crimes, such as fraud, corruption, market manipulation/insider trading, international tax crimes and foreign bribery and corruption to have the highest ML threat; within the domestic landscape, drug trafficking had the highest threat. The NRA further noted that there was no evidence of terrorist financing having taken place in Bermuda, however the potential risk for TF was rated as medium-low.

The Company intends to apply the General and Sector Specific GNs for implementing the appropriate mitigants and controls in their licensed proprietary technology match trading exchange platform of which is limited to approved Participants. Details of the 24 Exchange Platform and its operations are provided for tin the Operating Procedures Manual (**OPM**). The OPM should be read in conjunction with this AML Plan with particular focus on:

- Chapter 18 Market Conduct (e.g. Prohibited Trading Practices)
- Chapter 19 Suspension/Termination
- Chapter 20.1 Regulatory Co-operation

The overall risk appetite and tolerance of the Company is Medium risk. Pursuant to pursuant to Reg 16(1)(e) and 1(ea) the Company will maintain an up-to-date business risk assessment (review at least annually) and ensure to carry out a documented risk assessment of any product or service prior to launch[6].

1.3 Bermuda Legal & Regulatory Framework

Regulated financial institutions of Bermuda must adhere to the long-established regulatory regime to prevent the country and the financial sector from criminal abuse. The following are the key elements of the AML framework of Bermuda:

- Anti-Terrorism (Financial and Other Measures) Act 2004 (ATFA 2004)
- Criminal Justice (International Cooperation)(Bermuda)Act 1994
- Criminal Code Act 1907
- Financial Intelligence Agency Act 2007 (FIA 2007)
- Proceeds of Crime Act 1997 (POCA 1997)
- Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 (AML Regulations 2008);
- Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008 (SEA 2008)
- Extradition (Overseas Territories) Order 2002
- International Sanctions Act 2003
- International Sanctions Regulations 2013 (Regulations 2013)

In addition to the following key acts, policy and guidance documents as relevant to digital asset businesses issued by the BMA[7]:

- Digital Asset Issuance Statement of Principles 2020
- Digital Asset Custody Codes of Practice 2019
- DAB Statement of Principles 2018
- DAB Code of Practice 2018
- Digital Asset Business Act 2018 (DABA)
- Digital Asset Business Regulations 2018 (DABA Regs)
- General Guidance Notes for AML-ATF Regulated Financial Institutions on AML and ATF 2016 (General GNs)
- Sector specific: Annex VIII AML-ATF Specific Guidance Notes for Digital Assets 2018 (DABA or Sector Specific GNs)

[6] A business risk assessment is provided for in Appendix C.

[7] Please follow the link for up-to-date BMA issued DABA policy and guidance: https://www.bma.bm/document-centre/policy-and-guidance-digital-asset-business

Failure to comply with the requirements of specified AML Regulations is a criminal offence and carries with it significant and serious penalties. Further, the above codes, principles and regulatory requirements are relied upon to ensure the Company's business is conducted in a prudent manner and drive the basis for the internal control processes, and material departures from them will be supported accordingly. Such internal controls are risk based and commensurate with the risk of the product being managed and the local environment.

It is to be noted that under Bermuda law, money laundering involves the proceeds from any criminal conduct or any terrorist property. Criminal conduct includes all offences triable on indictment before the Supreme Court. Criminal conduct also includes all offences outside Bermuda that, had they occurred in Bermuda, would be triable on indictment before the Supreme Court.

1.4 Money Laundering

Money laundering is broadly defined as an attempt to conceal or disguise the illegal source and nature of funds so that they appear to be assets derived from legitimate activities or sources, which may be more readily used for other purposes. Money laundering is typically motivated by illegal or criminal activity, including tax evasion (among other corrupt and illegal activities) and often involves careful orchestration between several entities to effect complex transactions to conceal the fund's illegal nature. Generally, money laundering occurs inthree phases:

- **Placement** – the illegally derived funds are placed into the banking system;
- **Layering** – layers of complex transactions are created to conceal the illegal origin of the funds; and
- **Integration** – the funds have been laundered and now appear legitimate, ready for use in the financial system.

The specific money laundering offences under Bermuda law pursuant to Sections 43-45 POCA 1997[8] and Section 8 ATFA 2004 include:

- Concealing or transferring proceeds of criminal conduct;
- Assisting another to retain proceeds of criminal conduct; and
- Acquisition, possession or use of proceeds of criminal conduct.

In addition, Sections 46–47 of POCA 1997 criminalize the following acts:

- Failure to disclose to the Financial Intelligence Agency (**FIA**) knowledge or suspicion of money laundering; and
- Tipping off a person other than the FIA by disclosing information likely to prejudice an investigation into money laundering.

A person found guilty of a money laundering offense under Sections 43-45 of POCA (namely concealing, assisting, acquisition) shall be liable on summary conviction to imprisonment for 5 years or a fine of $50,000 or both and on conviction on indictment to imprisonment for 20 years or an unlimited fine or both. The sanctions for failing to comply with section 46 or 47 POCA 1997 (namely failure to disclose knowledge or suspicion; tipping off) shall be liable on summary conviction, to imprisonment for 3 years or a fine of $15,000 or both and on conviction on indictment, to imprisonment for 10 years or an unlimited fine or both.

The maximum civil penalty for failure to comply with AML/ATF obligations, pursuant to Section 20(1) read with Section 20(1A)(a) of the Proceeds of Crime (AML and ATF Supervision and Enforcement) Act 2008, is up to $10,000,000 as the Authority considers appropriate.

1.5 Terrorist Financing

Terrorist financing may not involve the proceeds of criminal conduct but involves an attempt to conceal or disguise either the origin of the funds, or their intended use, which may be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the

[8] Sections 32, 33 and 230 of the Criminal Code also criminalize any attempt, conspiracy or incitement to commit any such offense

motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Specific terrorism financing offences under Bermuda law pursuant to Sections 5-8 ATFA 2004[9] include:

- Fund raising for the purposes of terrorism;
- Soliciting, collecting or providing money or other property for the purposes of financing terrorist organizations or financing persons participating in terrorism;
- Using or possessing money or other property that is intended to be used for the purposes of terrorism; and
- Participating in arrangements to make money or property available for the purpose of terrorism.

In addition, ATFA 2004 criminalizes the following acts:

- Failure to disclose to the FIA knowledge or suspicion of terrorist financing; and
- Tipping off a person other than the FIA by disclosing information likely to prejudice an investigation into terrorist financing.

A person found guilty of a TF offense under Sections 5-8 of ATFA (fundraising, use and possession, funding arrangements or money laundering) shall be liable on summary conviction to a fine of $20,000 or to imprisonment for 12 months or both and on conviction on indictment to a fine of $200,000 or to imprisonment for 14 years or to both. The sanction for failing to comply with Section 9 or 10A of the ATFA 2004 (the offence of failing to disclose information) on summary conviction, is a fine of $15,000 or imprisonment for 3 years or both and on conviction on indictment, to an unlimited fine or imprisonment for 10 years or both.

The maximum civil penalty for failure to comply with AML/ATF obligations, pursuant to Section 20(1) read with Section 20(1A)(a) of the Proceeds of Crime (AML and ATF Supervision and Enforcement) Act 2008, is up to $10,000,000 as the Authority considers appropriate.

1.6 AML Compliance Officer Designation and Duties

The Company has appointed[10] David Sassoon[11] as its AML Program Compliance Officer (**AMLCO**) and Mazars Limited (**Mazars**) as its Money Laundering Reporting Officer (**MLRO**). The AMLCO is ultimately responsible for the Company's AML Plan but may delegate certain tasks or functions to a designee. The AMLCO or his designee is responsible for, among other things, monitoring the Company's compliance with this AML Plan and applicable AML legal framework, maintaining current knowledge of applicable AML laws, supervising the maintenance of AML-related records, and conducting AML training when necessary. The AMLCO must ensure that this AML Plan is reviewed, and updated if needed, at least annually. For afuller explanation of the AMLCO's duties and obligations, please see Section 3.

1.7 Staff Hiring and Training

The Board, senior management and employees (including temporary and contract workers) must have the requisite understanding of MLTF and Sanctions and the internal reporting procedures, including the identity of the AMLCO at all times. On an annual basis, the Company ensures that the employees in view of their roles are trained on:

- the Acts and Regulations relating to MLTF, Sanctions
- How to identify transactions which may be related to MLTF
- Know how to properly report suspicions regarding transactions that may be related to financial crimes
- Customer due diligence (**CDD**) measures
- On-going monitoring
- Record-keeping
- Internal controls; and

[9] Ibid
[10] Pursuant to Regulations 17 and 18A of the AML Regulations 2008
[11] Who is of managerial position

- Risk assessment and management

It is to be noted that the hiring process carries out reference and background checks to ensure integrity and a high standard of hiring practices.

1.8 Suspicious Activities Reporting – Duty to Report

All Company employees and consultants are expected to be familiar with this policy and to immediately report any suspiciousactivities to the MLRO. In addition, employees and consultants must immediately forward any inquiry from a regulatoryor law agency to the MLRO. Any such inquiries must be referred to and handled by the MLRO.

If the MLRO determines that a Suspicious Activities Report (**SAR**) should be filed, the MLRO will submit it to the most relevant regulatory authority. In Bermuda, the Financial Intelligence Agency (**FIA**[12]) is the relevant authority for receiving and analyzing suspicious activity reports (**SARs**). Where the MLRO knows or suspects or has reasonable grounds to suspect that a person is engaged in money laundering or terrorist financing, a SAR must be filed with the FIA, along with any other appropriate authorities such as a Participant's homelocality, if required.

In any such case, the filing of external SARs is primarily the responsibility of the MLRO or his designee. Employees and consultantshave the obligation to report suspicious activity via an **internal** SAR to the MLRO where during the course of business or their employment, he knows, suspects or has reasonable grounds to suspect that another person is engaged in money laundering which relates to any proceeds of criminal conduct[13]. The MLRO is responsible for investigating and determining whether an external SARs is necessary and the reasoning for that decision (either for or against) be documented in a SAR log, see Appendix C Logs/Registers. Where an external SARs is deemed necessary, the MLRO is responsible for ensuring that the information submitted in a SAR is accurate and filed by the relevant locality's filing deadline, if any. Fora template SAR, see Appendix A.

The Company is aware that under Section 16 FIA 2007 enables the Financial Intelligence Agency, in the course of inquiring into a suspicious transaction or activity relating to ML/TF, serve a notice in writing on any person, requiring the person to provide the FIA with such information as it may reasonably require for the purpose of its enquiry.

Further guidance on suspicious activity reporting is provided for in the General GNs, Chapter 9. It includes a description of **knowledge** and **suspicion** for the purposes of interpreting the obligations that arise under AMLATF framework.

1.9 Red Flags for Suspicious Activities

During the course of conducting due diligence on a Participant or a prospective Participant (**Applicant**), and during the course of the Company's business relationship with a Participant, the AMLCO and other employees and consultants or designees involved in the Company's AML process should be aware of certain red-flags that could suggest suspicious activities, including, but not limited to, as applicable, an Applicant's and/or Participant's :

- Transaction activities that are inconsistent with the business or financial background of such person;
- Unwarranted delay or refusal to provide requested due diligence documentation;
- Lack of concern regarding commissions or other transaction costs;
- Being the subject of significant regulatory or governmental inquiries;
- Source of funds information is false, misleading, or substantially incorrect;
- Appearance of acting as an agent for an undisclosed principal, while refusing to provide information regarding such principal's identity;
- Frequent large purchases or movement of funds, especially to or from custodians located in suspect countries;
- Conducting transactions with the goal of moving funds or securities rather than obtaining a favorable return; or
- Engaging in transactions involving cash and/or cash equivalents that appear structured to avoid regulatory reporting requirements.

[12] www.fia.bm
[13] Section 46 POCA 1997

To further support the AML Plan in view of the digital assets, please refer to Appendix E for a direct excerpt from the BMA issued Sector Specific GNs for digital assets which includes a non-exhaustive list of sector-specific risk factors addressing customers, products, services, transactions, delivery channels, agents and other third parties, geographical connections

Additionally, to ensure maintaining up-to-date on the Risks and corresponding controls and mitigants, the AMLCO will maintain awareness and consideration of current reports and guidance from the Financial Action Task Force[14] (**FATF**)[15] on virtual assets (**VA**)[16], virtual asset service providers (**VASPs**), digital assets generally and the Fintech sector.

Sample cryptocurrency exchange red flag indicators per the September 2020 FATF report[17] often occur in instances when depositing cryptocurrencies at an exchange and immediately thereafter the customer –

- withdraws the cryptocurrencies without additional exchange activity to other cryptocurrencies, which is an unnecessary step and incurs transaction fees;
- converts the cryptocurrencies to multiple types of cryptocurrencies, again incurring additional transaction fees, but without logical business explanation (e.g. portfolio diversification); or
- withdraws the cryptocurrencies from a VASP immediately to a private wallet. This effectively turns the exchange/VASP into an mixer.

Further industry specific reports will be considered as needed such as those from Chainalysis[18] (quarterly newsletters and e.g. 2020 Geography of Cryptocurrency Report); and the International Organization of Securities Commissions (**IOSCO**) papers on Crypto-Asset Trading Platforms.

1.10 Transaction Screening for Digital Assets

For tracking illicit crypto transactions, the adage of "follow the money" applies. In order to mitigate the AML risks of transacting in cryptocurrencies, build confidence in the transaction monitoring process, and more effectively track and trace transaction activity, 24 Exchange primarily utilizes Chainalysis software which provides a blockchain explorer (a piece of software that uses API and blockchain node to draw various data from a blockchain and then uses a database to arrange the searched data and to present the data to the user in a searchable format), analytics, and transaction monitoring.

Each wallet which is party to a crypto transaction is vetted by 24 Exchange through Chainalysis (or a similar service) using the following process:

- Prior to trading, client provides 24X with wallet addresses;
- 24X vets new wallet addresses through Chainalysis and reviews for red flags;
- All submitted wallet addresses are then saved for ongoing monitoring;
- 24X continues to monitor for any potential new flags for known wallets on a daily basis;

Chainalysis will flag a transaction based on indicators of risky behavior. For example, a transaction will be flagged if the counterparty wallet is identified as an illicit service, such as a darknet market or terrorist financing organization.

24 Exchange would reject any transaction flagged as illicit by Chainalysis.

1.11 Financial Crime

Financial Crime in Bermuda is a general concept which covers ML and TF but extends to any activity which involves fraudulent or dishonest behaviour for the purposes of financial gain. Tax evasion has a financial cost and thus falls within this concept.

[14] Inter-governmental global standard setting body, note the FATF Recommendations and supporting Methodology for their implementation
[15] https://www.fatf-gafi.org
[16] FATF Report, Virtual Assets Red Flag Indicators, September 2020
[17] Ibid 16
[18] www.chainalysis.com

The Company's financial crime policy is set out in the 24 Exchange's ABC Policy (i.e. Anti-Bribery, Anti-Corruption and Anti-Financial Crime)

Tax evasion is the illegal attempt to reduce or evade tax liability by circumventing or frustrating tax laws, such as deliberate misrepresentation or omission of taxable income or wilful non-payment of due taxes. Tax evasion is different from tax avoidance, which is the use of legal methods to reduce or minimize tax liabilities.

24 Exchange mitigates tax evasion risk using the same AML/ATF control, customer risk assessments, screening, collection of CDD/KYC documentation, ongoing monitoring and employee training. Employees also understand that one of their core obligations, in line with the Company's ABC Policy and internal procedures, is that they must bring any suspicion of criminal activity or financial crime, promptly to the attention of the Compliance Officer for investigation, who then determines whether to report the activity to the MLRO for the purposes of SARs reporting.

2 CUSTOMER IDENTIFICATION PROGRAM

2.1 Customer Identification Program and Know Your Client

The Company's primary method of detecting and preventing money laundering is carried out during onboarding as the Company executes its Customer Identification Program (**CIP**), a process also frequently referred to as Know Your Client (**KYC**). CIP/KYC refers to the process in which the Company collects identifying information about Applicants that have selected for participation in the crypto market for the purposes of conducting due diligence prior to accepting them as Participants.

CIP and KYC serve as the Company's first and primary lines of defense against misuse of the Platform for money laundering or terrorist financing by preventing such actors from accessing the Platform at the outset. All Applicants that seek access to the crypto asset market on the 24 Exchange Platform are subject to CIP/KYC either via the pre-approved institution or directly via the Company; and no such Applicant may be accepted as a Participant without undergoing CIP/KYC. Any Applicant identified as, associated with, or suspected of money laundering or terrorist financing during CIP/KYC will not be accepted as a Participant. Any Applicant who fails to provide adequate information for the Company to conduct CIP/KYC will not be permitted to access the Platform as a Participant.

It is to be noted that all Applicants must already be customers of the Company's pre-approved institution[19] through which the Platform is made available or directly with the Company. The Applicants must have a standing and active account that is AML compliant in order to trade on the Company Platform. The Company does not have any direct access to the funds and are merely providing the systems and technological systems through the 24 Exchange Platform to enable FX trades through a non-manual matching engine between counterparties that are known institutional clients. While the trade itself my occur in an anonymous manner to prevent such things as market skewing or influence by the large institutional client trades, the trades are only permitted by the approved Applicants, known as Participants, and details are disclosed subsequent to the trade.

By preventing malicious actors from accessing the Platform at the outset, the Company better assures Participants that their transactional counterparties have undergone similar CIP/KYC procedures and have not been identified as, suspected of, or associated with, money laundering or terrorist financing, reducing the risk of Participants inadvertently transacting withmalicious actors in contravention of their local AML laws or becoming associated with criminal activities outright. In addition, the Company's business depends the integrity, legality, and public perception of not only the Platform itself, but theParticipants that we accept. CIP/KYC assists the Company in mitigating the likelihood of the Platform or its Participants from becoming associated with or used for criminal activities or terrorist financing. Accordingly, it is critical that the Company appliesformal, documented CIP/KYC consistently and without exception to each Applicant prior to their acceptance as Participants on the Company's Platform.

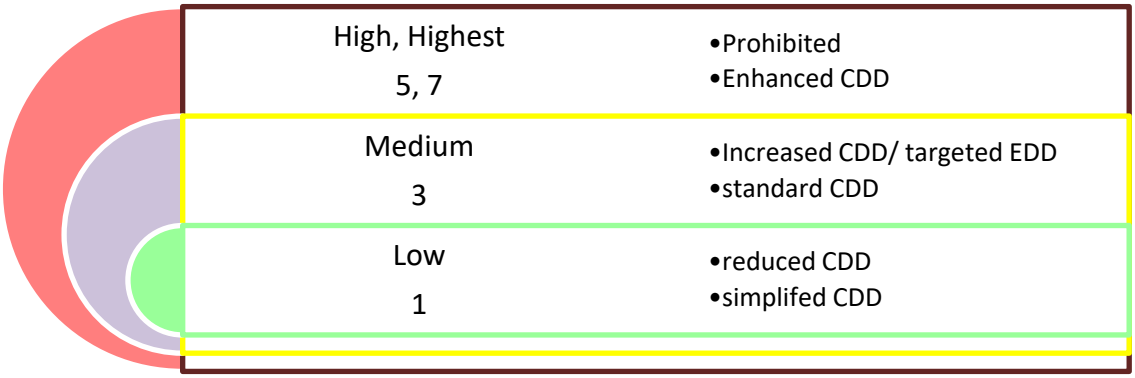
[19] Pre-approved institutions are banks or other financial institutions with which the Company has or will have a dedicated agreement to provide Participants access to the 24 Exchange Platform; which may or may not include the exchange of cryptocurrencies.

2.2 Applicant and Participant Risk

The 24 Exchange Platform is available predominantly to the Company's pre-approved institutions such as banks or other institutions that are regulated for AMLATF purposes in an equivalent jurisdiction to Bermuda. As such all Applicants must have completed the pre-approved institutions' AML onboarding program or that of the Company, and have a line of credit extended to them prior to be permitted to become Participants. As all Applicants must be of a particular client type (sample list of existing customers of the exempt business of the Company are provided for in Appendix D), the driving risk factors will be the product/cryptocurrency traded in, the geographical connection of the Applicant's trades and related PEP status or negative news media that may be deemed relevant by the AMLCO affecting its Risks. For the purposes of this AML Plan, those Participants that elect to enable cryptocurrency trading on the Platform, CIP/KYC under the Company will apply to the extent it will obtain the identification information and verify information via public and private reliable resources as the Participants are large, well known institutional clients seeking to find solution into safe and reliable cryptocurrency trading on the 24 Exchange Platform.

The employees should understand that the Company remains liable for its AML obligations. While onboarding due diligence may be carried out by the pre-approved institution, ongoing monitoring and scrutiny of transactions obligations are carried out internally.

Depending on the risk score, High/Medium/Low associated with a particular Applicant, the Company applies either Standard Customer Due Diligence (**CDD**) or varying levels of EnhancedDue Diligence (**EDD**). The risk associated with a particular Applicant depends on a variety of facts and circumstances, including an Applicant's country of domicile, an Applicant's regulatory status in their country of domicile, an Applicant's association with or status as a Politically Exposed Person (**PEP**)[20], an Applicant's lack of physical presence for identification purposes, where the Applicant is identified as being actually or potentially associated with criminal activities, and other factors that the AMLCO or his designee deems relevant.



The client scoring is based on a four-tiered system as supported by the Wolfsberg Principles. provided the AMLCO is ultimately responsible for determining either an Applicant must undergo Standard Due Diligence or Enhanced Due Diligence and may delegate the conduct of due diligence to a designee.

While the Wolfsberg principles and FATF guidance are utilized to support the risk score evaluation, a general summary of the risk evaluation is derived from the following:

- Low: factors of the profile demonstrate nominal risks, no "red flags" or suspicious activities and may be accepted by simplified or reduced due diligence
- Medium: factors of the profile present an inherent risk to MLTF and as such requires standard due diligence or an increased level due diligence and or a targeted level of enhanced due diligence where circumstances warrant.
- High: factors of the profile present inordinate risks, or appear to demonstrate any number of "red flags" and or suspicious activity that requires the AMLCO to review. The review process includes any combination of the

[20] Foreign PEPs are automatically undergo EDD

following actions (all of which will be documented and added to the AMLATF records.

- AMLCO approval, which may require implementing additional controls to lower or mitigate the identified risks
- Additional review by Senior Management or the Board depending on the seriousness of the identified risk
- Application of additional measures or resources necessary to reduce the identified risk to one within the risk appetite of the Company;
- Rejections/Terminations of the business relationship with the Applicant/Participant/Agents;
- Considering filing a SAR with the FIA or other appropriate regulatory authority.

2.3 Customer Due Diligence

Customer Due Diligence (**CDD)** as defined by Reg 5 of the AML Regulations is applied to applicants to ensure the Company knows who the customer, or Applicant, is and can establish an expected profile on the relationship for onboarding and monitoring purposes. CDD is applied when the Company:

- establishes a business relationship;
- carries out an occasional transaction;
- suspects ML or TF and
- doubts the veracity and adequacy of documents, data or information previously obtained for the purposes of identification or verification.

EXCEPT where performing CDD will result in tipping-off the Applicant that an Employee suspects that the transaction related to ML or TF – a disclosure or SAR must be submitted to the FIA instead of performing CDD.

A standard level of CDD is applied in situations where the risk associated with an Applicant is considered low to medium and does not require Enhanced Due Diligence. Under CDD, Applicants are required to provide certain supporting KYC information and at times documentation, summarized below. All Applicants are screened for negative news, sanctions and PEP status (if relevant) for AML purposes, such as the UK Consolidated List[21], US Office of Foreign Assets Control (**OFAC**) List, the European Union Sanctions List, and/or the United Nations Sanctions List.

Simplified Due Diligence (**SDD**) involves the application of reduced or simplified CDD measures where the risk assessment process results in the finding of lower than standard risk. Reg 10 of the AML Regulations 2008 provides for the instance where the Company may vary from the standard CDD measures if it has reasonable grounds for believing that the Applicant falls within one of the selected paragraphs with an overall risk that has been determined to be low:

The Applicant is:

- An AMLATF regulated institution of Bermuda or equivalent jurisdiction (note it may not be listed on the FATF high risk countries lies);
- Is a company (or parent thereof) whose securities are listed on an appointed stock exchange; or
- Is a public authority in Bermuda.

Further SDD guidance as applied to the DAB sector is provided for the Sector Specific GNs paragraphs VIII.117-VIII.123 and VIII.139-VIII.143.

The following table provides guidance as to the CDD on the typical Applicant and/or Participant and/or Agent seeking to extend its Platform services to the cryptocurrency market:

[21] https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets

Full name of Applicant or Participant or Agent (and any former and or trade names):	
Date and Place of Incorporation (or registration or establishment):	
Location of Business (full operating address):	
Domicile Country (Country of Incorporation):	
Type of Entity (public, private, trust, etc.)	
Official Identification Number (where applicable):	
Relevant Company Registry, Regulator:	
Named Stock Exchange and Ticker:	
Where not publicly listed, a register of the Directors and Shareholders:	

2.4 Enhanced Due Diligence

Enhanced Due Diligence (**EDD**) pursuant to Regulation 11 AML Regulations 2008 applies to Applicants identified as high risk. As noted in Reg 11, EDD must be applied in any of the following instances:

- The customer has not been physically present for identification purposes (see Appendix D Customer Due Diligence Documentation, in particular the paragraphs on document certification and the alternatives for mitigating against impersonation fraud);
- The business involves a correspondent banking relationship;
- The business relationship or occasional transaction involves a politically exposed person (see Section 2.5 Politically Exposed Persons); or
- The business relationship or occasional transaction has a connection with a country or territory listed as high risk by the FATF or Caribbean FATF, or that represents a higher risk of money laundering, corruption, terrorist financing or being subject to international sanctions.

In addition to CDD requirements, when applying EDD, the Company may require Applicants to provide copies of CIP/KYC documentation certified by a qualified, suitable person in their locality, such as an attorney, accountant, or notary, as applicable, who is expected to adhere to ethical or professional standards and exercises their vocation in a jurisdiction with an adequate AML regime. The AMLCO or his designee may also conduct further inquiry into an Applicant's information prior to making a determination on whether the Company should accept the Applicant as a Participant, including correspondence with the Applicant's most relevant regulator in their country of domicile, request for reference letters, or other inquiries that the AMLCO or his designee deems appropriate.

2.5 Politically Exposed Persons

Politically Exposed Persons[22], or **PEPs**, are:

- Current or former senior officials in the executive, legislative, administrative, military, or judicial branches of a foreign government;
- Senior officials of major foreign political parties, or senior executives of foreign government-owned commercial enterprises; and
- Corporations, businesses, or other entities formed by or for the benefit of such individuals; immediate family members of such individuals, or any individuals publicly known (or actually known by the Company) to be a

[22] See the Schedule, paragraphs 2 of the AML Regulations 2008; and Appendix G PEPs

close personal or professional associate of such individuals.

There are three categories of PEP of which carry different levels of risk: (1) Foreign PEPs, or FPEP carry the obligation for automatic EDD; (2) International Organizational PEPS, or IO PEPS; (3) Domestic (Bermuda) PEPs or DPEPs. The latter two categories' risk level may require EDD if other factors of the profile are high risk. It is to be noted that DPEPs would not be applicable to the Company as the Platform is not made available to Bermuda natural persons.

AMLCO or senior management approval is necessary prior to establishing and continuing to have a business relationship or carry out an occasional transaction with a PEP.

As part of the Company's onboarding documentation, Applicants may be asked whether they are a PEP or associated with a PEP. If the Applicant responds in the affirmative, or if the Company discovers in the course of CIP/KYC that the Applicant is oris associated with a PEP, such application may only be accepted by senior management of the Company in consultation with the AMLCO. Furthermore, the Company may inquire as to the Applicant's source of funds and conduct EDD and enhanced monitoring of the relationship if deemed necessary. The level of scrutiny an Applicant or Participant who is, or is associated with, a PEP is subject to will depend on a variety of factors, which may include, among others:

- Proof that the Applicant's funds do not emanate from criminal activities;
- Whether the home jurisdiction of such Applicant is one in which political figures have been implicated in corruption; and/or
- The length of time that a former political figure has been in office.

In situations where CIP/KYC cannot be satisfactorily completed, the Company should not accept the Applicant, suspend the Participant's access to the Company's Platform until CIP/KYC can be conducted, terminate the relationship with such Participant, or file a report with the AMLCO, as applicable.

2.6 Required Documentation

As part of CIP/KYC, the Company strives to collect certain information and documentation concerning an Applicant to verify the identity of the Applicant and to conduct due diligence on the Applicant prior to their acceptance as a Participant. Depending on the type of Applicant, the Company may request different types of documents in connection with CIP/KYC. Thetypes of required information and documentation required for different Applicant types are detailed below in Section 2.10.

2.7 Formal Report and Responsibilities

The Company's AMLCO or designee is responsible for conducting CIP/KYC, including review of any information and documentation received from an Applicant. Any determination made by a designee is subject to the AMLCO's final approval, including among others, an Applicant's risk rating (and thus the level of due diligence applicable to such Applicant) or whether the Applicant should be admitted as a Participant at all.

For each instance that CIP/KYC is conducted, the Company will perform a Customer Risk Assessment using the documents and information received in connection with an Applicant. The Customer Risk Assessment will confirm the risk-level assigned to the Applicant,the level of due diligence applied, the factors contributing to the Applicant's risk rating, and any findings discovered during the course of CIP/KYC.

2.8 Ongoing Due Diligence

All Applicants are subject to CIP/KYC prior to their acceptance to the Platform as Participants and are subject to ongoing monitoring pursuant to Regulation 7 of the AML Regulations 2008 throughout their business relationship with the Company to ensure their profile matched the expected Participant profile, the KYC is up-to-date and investigation into any unusually large or complex transactions (outside what is expected for the industry or Participant profile). The AMLCO or his designee will conduct ongoing CIP/KYCon the Participant at frequency corresponding to their risk score or at a triggering event: **High risk** (every 6 months), **Medium risk** (annually), **Low risk** (18 months). The depth of scrutiny and reexamination may vary at the discretion of theAMLCO, depending on factors including the level of risk or the types of

risks associated with such Participant.

Further ongoing monitoring guidance as applied to the DAB sector is provided for in the Sector Specific GNs paragraphs VIII.179-VIII.193.

2.9 Prohibitions

In accordance with Reg 13 of the AML Regulations, the Company will not permit or maintain anonymous accounts, or accounts in fictitious names, such that the true beneficial owner is not known. In the instance that an Applicant requests an account be set up anonymously, in a fictious name and/or to obscure beneficial ownership; the matter will be escalated and reported to the AMLCO to investigate and action immediately with an appropriate measure such as freezing access to the Platform, freezing potential transactions, consideration of filing an external report to the FIA and/or termination of the business relationship. Where a business relationship is terminated on the basis of suspicion, then a report must be filed with the FIA.

Further, the Company is prohibited from knowingly entering, or continuing, a relationship with:

- a shell bank or a bank which is known to permit its accounts to be used by shell bank; and
- retail traders/investors
- persons/organizations/entities organized, based, operating, or with a beneficiary owner
    - in a sanctioned country, or
    - supporting MLTF or related criminal activity.

2.10 Required Documentation by Applicant Type

The Company requests different types of information from different types of Applicants, or Counterparties, that choose to trade in the crypto market for CIP/KYC purposes. If an Applicant fits into one of the Company's broad categories, they must generally submit all required, enumerated documentation associated with their Applicant type[23]. The following requirements are not necessarily a complete list of all information required for CIP/KYC purposes, and the requested documents detailed are both supplemented and superseded by any requirements that the AMLCO or his designee deems relevant; a detailing of the required documentation and review is provided for in Appendix D: Customer Due Diligence Documentation. The following serves as a baseline summary of the types of documentation that the Company anticipates requesting.

Applicants/Counterparties:

- KYC identification (verify the name and address of the Counterparty and ultimate beneficial owner as applicable, note: most of the institutional clients are listed either directly or via parent on a stock exchange)
- Verification of the Counterparty and beneficial owners as applicable is applied either:
    - during the establishment of the business relationship if it necessary not to interrupt the normal conduct of business, there is little risk of ML/TF if it is done shortly thereafter and any ML/TF that do arise during due diligence are managed effectively [including prevention of closing out the account or payment out of the account prior to completion of verification]; OR
    - PRIOR to establishment of the business relationship or occasional transaction where the above is not possible
- Verification is executed on the basis of documents, data or information obtained from reliable independent source(s)
- Nature and purpose of the business of the Counterparty and the business relationship (note: limited to the use of the Platform for access to the cryptocurrency market)
- Determine anticipated level of activity in the cryptocurrency market
- Determine whether they are regulated and by whom
- Determine if they are targets of international sanctions
- Screen for negative news media that would be relevant to MLTF and for PEP status

[23] Refer to the Principal Trading Participating Agreement (which is part of the Participant application process)

The due diligence process will be executed, on a risk-sensitive basis, prior to enabling any Participant that elects to trade in the cryptocurrency market. It is to be noted that an established business relationship may already exist with the Company through the exempt business of the current FX exchange business.

3 RESPONSIBILITIES OF THE ANTI-MONEY LAUNDERING COMPLIANCE OFFICER

3.1 General Supervision

The Company's AMLCO's primary duty is to generally oversee the Company's AML Plan, including initial and ongoing CIP/KYC processes. The AMLCO may assign a designee to assist in fulfilling some of the AMLCO's responsibilities, which broadlyinclude, but are not necessarily limited to:

- Developing the Company's AML policies, procedures, and controls;
- Providing a writing annual Compliance report[24] to the Board of the Company in view of the crypto asset trading.
- Conducting staff AML training[25] on an annual basis and maintain their own level of AML training adequate to their role;
- Implementing and monitoring day-to-day operations and internal controls of the Company's AML Plan;
- Staying educated of critical developments or changes in relevant laws, rules, regulations, or best practices;
- Investigating, reviewing and reporting on suspicious activity;
- Maintaining corresponding logs (see appendix) and
- Handling and responding to inquiries received from the FIA and competent authorities such as the BMA.

The AMLCO is also responsible for various other critical AML functions, as detailed below.[26]

3.2 Annual Review of the Broader AML Program

The AMLCO is responsible for annually reviewing the efficacy of the Company's broader AML Plan, ensuring that the AML Planremains current, up-to-date, and adequately designed to detect and prevent misuse of the Company and/or its Platform for illicit purposes in the context of the Company's business and its needs. In conjunction with the AMLCO's duty to maintain current knowledge of updates to laws, rules, regulations, or industry practices, the AMLCO should update the AML Plan to reflect any such changes during the course of such annual review. Such review is to be formally documented and memorialized in the form of a brief memoranda, describing at a minimum, the methodology in which such review was conducted, any findings or deficiencies discovered in the course of review, and remedial actions taken to address such issues. The AMLCO may designate another person or a third-party to conduct such review. In such a case, the AMLCO holds final responsibility for ensure that such annual review was conducted properly, adequately, and formally documented.

3.3 Annual Review of AML Documentation

The AMLCO is responsible for either conducting or arranging for the review of Participant CIP/KYC documentation, shouldthe Participant's activities warrant such review or if the AMLCO deems it necessary or desirable. At least annually, the AMLCO should examine the Company's roster of Participants and determine whether any Participants require additional or renewed CIP/KYC. The AMLCO may deem a Participant worthy of further review after considering factors such as the Participant's trading activities, any issues encountered in connection with such Participant over the course of the relationship, any other facts and/or circumstances which the AMLCO believes tends to suggest that CIP/KYC is warranted,or no reason at all. If a Participant is selected for CIP/KYC, the AMLCO will document the reason why, if any.

Similar documentation required for an ordinary CIP/KYC process will be required and maintained, including a report detailing the findings of such additional and/or renewed CIP/KYC.

[24] General GNs paragraphs 1.50-1.53

[25] Internally or by a reliable third party qualified in AML training

[26] General GNs, Chapter 1

3.4 Independent Review

The AMLCO may utilize the services of designees or other third parties to assist in fulfilling his obligations pursuant to this AML Plan. All work product created by a designee or third-party is subject to independent review by the AMLCO, who may not rely on such third-party or designee to review any work product that they created. The AMLCO should at least annually conduct independent review of such work products, such as AML findings reports or reviews, if facts and circumstances suggest that such review is warranted. The AMLCO is responsible for determining if such review is necessary, and if so, the frequency and depth of review.

At minimum, the AMLCO will ensure that annual audit of the Company's AML policies, procedures, systems and controls are reviewed pursuant to Regulation 17A AML Regulations 2008; must be separate to the Company's general or financial audit(s).

3.5 Accuracy and Filing of Suspicious Activities Reports

The AMLCO holds authority to determine if and when a SAR needs to be filed, and to whom. Employees and consultants are responsible for reporting suspicious activities to the AMLCO, who will make the determination either by himself or inconsultation with senior management, outside consultants, and/or outside counsel, as he deems appropriate. Once the determination has been made that a SAR needs to be filed, the AMLCO is responsible for supervising the completion and filing of the SAR with the relevant regulatory authorities and ensuring the accuracy of the information contained in anySAR. The AMLCO or his designee is also responsible for determining which authority the SAR must be filed with.

3.6 Maintaining Books and Records

The AMLCO supervises the proper maintenance of books and records in connection with the Company's AML Plan, such asCIP/KYC findings reports, copies of CIP/KYC documentation, annual reviews, and others. The AMLCO may utilize a designee or third-party to assist with such recordkeeping. Generally, all AML-related records must be retained for a minimum of five years.

It is to be noted that the Company is not relied upon by another entity or person for CDD or other related AMLATF record keeping purposes.

3.7 Records to be Maintained for at Least Five Years from the Date of Creation:

- Documentation of the Company's annual review of the AML plan;
- Documentation of the further CIP/KYC conducted at the AMLCO's request;
- Documentation of the AMLCO's independent review of work done by designees or third-parties; and
- Documents created in connection with an Applicant's application, where the Applicant is ultimately not accepted as a Participant on the Company's Platform.

Records to be Maintained for at Least Five Years Following the Termination of a Participant's Business Relationship with the Company:

- All AML, CIP, KYC documentation created in connection with a specific Participant, including their initialCIP/KYC findings reports, the results of any subsequent due diligence conducted, and information and documents received in connection with their initial application.

Exception to the 5 year rule is in the case where a police officer has notified the Company in writing that particular records are or may be relevant to an investigation which is being carried out, the Company must keep the records pending the outcome of the investigation.

3.8 Outsourcing & Reliance

The Company will not rely upon or enter into any outsourcing arrangement with a third party where access to data without delay is likely to be impeded by confidentiality, secrecy, privacy or data protection restrictions. No

confidentiality, secrecy, privacy or data protection restrictions are currently seen to prevent access to the records either by the Bermuda office freely upon request or by Bermuda law enforcement agencies under court order. If it is found that such restrictions exist, the Company will notify the BMA, and copies of the records will be obtained and retained in Bermuda.

Reliance

The Company is permitted to rely on third parties to apply customer due diligence measures in accordance with Regulation 14[27]. Regulation 14 provides that the Company may rely on a Third Party (as defined below) provided that:

a. the Third Party consents to being relied on; and
b. Notwithstanding the Company's reliance on the Third Party, the Company:
    i. must immediately obtain information sufficient to identify customers;
    ii. must ensure that requested information on customers and beneficiaries is made available as soon as reasonably practicable following a request;
    iii. must satisfy itself that reliance is appropriate given the level of risk for the jurisdiction in which the third party is usually resident; and
c. will remain liable for any failure to apply such measures.

The Company relies upon Mazars, to carry out screening for the Participants and CIP process. The AMLCO will maintain oversight of those screening functions through periodic meetings with Mazars: quarterly meetings, or more frequent where concerns or issued need to be addressed.

Additionally, 24 Exchange receives a Customer Risk Assessment (**CRA**) for each new client submitted to Mazar's for AML/KYC screening, as well a detailed report containing the results of the client screening against multiple international databases, which include sanctions screening at on boarding and on an on-going basis. Applicants are screened for sanctions against lists that include, but are not limited to, the UK Consolidated List, US Office of Foreign Assets Control (**OFAC**) List, the European Union Sanctions List, and the United Nations Sanctions List.

Upon receipt of these reports, 24 Exchange makes a decision as to whether the client meets the Company's risk profile for opening an account. 24 Exchange reserves the right not to proceed with any client in its sole and absolute discretion.

Outsourcing Arrangements[28] [29]

- Screening - Mazars: For the purposes of the Company, the screening of Applicants and subsequent Participants that have elected to extend trading to cryptocurrencies on the Platform, is intended to be outsourced to Mazars. Mazars intends to utilize an internationally recognized screening platform such as eSpear, Namescan or RDC for screening purposes in conjunction with publicly available reliable resources.
- Technology - Cobalt[30]: The Company has a service agreement with Cobalt to provide their Participants credit management on the Platform via Cobalt's technology to access the Digital Asset (**DA**) market. Cobalt implements the best practices per the FX Global Code[31].

[27] Additional guidance is provided for in the General GNs paragraphs 5.118 through 5.148
[28] An "outsourcing arrangement" occurs where the Company uses a service provider to perform an AML activity, such as applying CDD measures, that would normally be carried out by the Company. Irrespective of whether the service provider is in Bermuda or overseas, and irrespective of whether the service provider is within or independent of any financial sector group of which the Company is a member, any outsourcing arrangement is subject to the Regulations and the Guidance Notes.
[29] See also Outsourcing Policy
[30] Copa Fin Limited, England and Wales – is trading as Cobalt
[31] https://www.bis.org/about/factmktc/fx_global_code.htm

- Cybersecurity - BreachLock Inc: The Company has a service agreement with BreachLock to maintain the cybersecurity of Platform which includes penetration testing.
- Agent – only pre-approved agents permitted. See Appendix D2: Agent Due Diligence.

Each of the functions carried out by the above entities are fully visible, monitored and managed by via periodic updates to review with any deficiencies or issues identified and how addressed included. Please refer to the Continuity Policy and each agreements' provisions addresses such issues.

In any outsourcing arrangement, the Company understands that it cannot contract out of its statutory and regulatory responsibilities to prevent and detect ML/TF. The risks identified should be factored into the decision whether or not to enter into the relationship, and into the risk ratings for any customers, products, services and transactions affected by the relationship.

In any outsourcing relationship, the Company will take care to avoid:

- Impeding the effective ability of the Company's senior management to monitor and manage its compliance functions, including the application of non-standard measures, such as enhanced due diligence;
- Impeding the effective ability of the Board to provide oversight;
- Impeding the effective ability of the appropriate regulator to monitor the Company's compliance with all obligations under the regulatory system;
- Reducing the responsibility of the Company and/or its managers and officers;
- Removing or modifying any conditions subject to which the Company's authorization was granted; and
- Increasing ML/TF risk in any way that is not adequately addressed through appropriate risk assessment and mitigation.

The Company will implement a policy to maintain the continuity of its business in the event that the provision of services by a service provider fails or deteriorates to an unacceptable degree. The policy will include contingency planning and a clearly defined strategy for exiting the outsourcing arrangement.

Prior to entering into any further AMLATF outsourcing arrangements or modification of the ones in place, the Company will carry out due diligence as to the service provider under consideration to ensure that the relevant service provider has the ability, capacity, and any required authorization to perform the outsourced activities reliably, professionally, and in accordance with the Regulations.

4 INTERNATIONAL SANCTIONS

Financial sanctions are economic and trade restrictions or prohibition enforcement measures imposed by the international community to achieve, maintain or restore international peace and security that is specific to jurisdiction, sector, group, entity or even individual natural person. Although they are primarily

Such measure prohibit you from carrying out certain activities; including making any funds or other assets, economic resources, or financial or other related services, available, directly or indirectly, wholly or jointly, for the benefit of designated persons or entities; or behaving in a certain way if financial sanctions apply.

The Company's policy is to at all times in accordance with the highest professional and ethical standards and we expect client to act in a like manner in all dealing with us and their counterparties. If the Company believes that any activities or funds are held in breach applicable laws or our policies in respect of the following sanctions regimes, we reserve the fight to apply the required actions such as account freezing, reporting and terminating the client with immediate effect or as directed by competent or legal investigatory authorities:

- Bermuda (via the UK)
- United States of America OFAC[32]

The Company has measures in place to ensure it is not transacting or harboring any funds, property or assets of a sanctioned person or entity whereby it would be in breach of the Bermuda Internal Sanctions Regime.

4.1 Legal Framework

The Bermuda International Sanctions Regime[33] is made up of the International Sanctions Act 2003 (Sanctions 2003) and the International Sanctions Regulations 2013 (Regulations 2013). As a British Overseas Territory, Bermuda bases it regime predominantly on the UK which is demonstrated in that the Sanctions 2003 empowers the Minister responsible for Legal Affairs (**Minister**) to make such provisions as appear to be necessary or expedient to give effect in Bermuda to the international sanctions obligations of the UK. Bermuda's primary legislation, the Regulations 2013 gives effect to the international sanctions of the UK legislation on which Bermuda basis its regime.

The Governor of Bermuda has delegated its Sanctions Regime functions to the Minister of Legal Affairs which is now the competent authority to which sanctions-related license applications, notifications and authorizations should be made to:

The Minister of Legal Affairs
Financial Sanctions Implementation Unit
Global House
43 Church Street
Hamilton HM 12

Email: fsiu@gov.bm; utilizing the following form: Bermuda Asset Freeze License Application

Notifications and guidance on the Bermuda Sanctions Regime are provided by the BMA[34] and the Financial Sanctions Implementations Unit (**FSIU**).[35]

---

[32] Where OFAC is not selected, it is to be noted that unwittingly the Company may be drawn in via an employee working on the matter that is a US Citizen, dealing in US currency, or transacting through a correspondent bank or office in the US. If any of these occur, then a potential breach of the OFAC US Sanctions regime could occur.

[33] https://www.gov.bm/international-sanctions-measures

[34] Found at either https://www.bma.bm/international-sanctions ; OR https://www.bma.bm/document-centre/policy-and-guidance-aml-atf

[35] Financial Sanctions Guidance 2018 (https://www.gov.bm/sites/default/files/Financial-Sanctions-Guidancev4.pdf) and the

Breaches of financial sanctions are considered to be a serious criminal offence. Upon conviction on indictment, offences under the OT Orders in regards to UN / EU financial sanctions provide for a term of imprisonment of up to seven years or a fine or both; and on summary conviction, imprisonment for a maximum of 6 months or to a fine not exceeding £5,000.00 or its Bermuda dollar equivalent or both[36].

The maximum civil penalty for failure to comply with international sanctions obligations, pursuant to Section 20(1) read with Section 20(1A)(a) of the Proceeds of Crime (AML and ATF Supervision and Enforcement) Act 2008, is up to $10,000,000 or as the Authority considers appropriate.

4.2 Screening

Clients and identified related parties will be screened and negative news media searches performed to identify potential sanction links and matches against sanctions lists[37].

The AMLCO (or its delegate) will:

- Check whether the Company maintain any accounts or otherwise hold any funds or economic resources for designated or listed persons;
- Freezing such accounts or other funds and, unless the Minister has granted a license, refraining from dealing with or making available such funds or economic resources to the designated or listed persons or any third party; and
- Notifying the Minister of the above.

As sanctions measures are subject to change, it is essential that ongoing screening is carried out.

4.3 Actions

If the Company knows or have reasonable cause to suspect that the Company is in possession or control of, or are otherwise dealing with funds or economic resources owned, held or controlled by a designated person, the AMLCO (or delegate) must:

- freeze the funds or economic resources that it has control of (e.g. freezing the Platform at various enabled points for preventing completion of a transaction)
- not deal with them or make them available to, or for the benefit of, the designated persons, unless: there is an exemption in the legislation that the Company can rely on (e.g. blocking the Participant)
- apply for a license from the FSIU
- report them to the FSIU.

Records of any potential matches to names and sanctions lists, whether the match turns out to be a true match or a false positive must be kept. At minimum, the following information about any match will be held on record:

- the information or other grounds which triggered the match (i.e. a 'hit' provided by screening software);
- any further checks or enquiries undertaken;
- the relevant Sanctions Regime;
- the person(s) involved, including any members of compliance or senior management who authorized

Financial Sanctions Frequently Asked Questions (FAQs) 2018 (https://www.gov.bm/sites/default/files/Financial-Sanctions-FAQsv3.pdf)

[36] Bermuda Financial Sanctions Guidance 2018

[37] The 'Bermuda current list of designated persons' list is manually monitored.

treatment of the match as a false positive;

- the nature of the relationship with the person or entity involved, included attempted or refused transactions; subsequent action taken (i.e. freezing accounts);
- if you consulted with, or filed, a report with the FSIU and other relevant authority (i.e. BMA).

APPENDIX A: SUSPICIOUS ACTIVITIES REPORT

Date of This Internal Report:

Date of Last Report (if any):

UPON SUBMISSION: **Do NOT** in any way inform the subject (directly or indirectly) of the report that the report has been submitted or you incur personal liability for a Tipping Off Offense. Follow instructions of the AMLCO accordingly.

Complete SECTION A if Natural Person

Complete SECTION B: if Legal Entity or Arrangement

Reason for Suspicion (Attach Additional Sheets as Necessary)

Include relevant details (noting Section A, B and or C as applicable), including the date the business relationship was established or declined, source of funds, value of assets held, if any, and nature of suspicion.

Signature of Anti-Money Laundering Compliance Officer:

AMLCO use only (actions take)

Tick as applicable:

- **Filed externally**
- **Cleared, not suspicious**
- **Continued monitoring**

SECTION A: Subject(s) of Report (Natural Persons) (Attach Additional Sheets as Necessary)

Last: **First:** **Gender:**

Date of Birth: **Place of Birth:** **Nationality:**

Nature of Services Provided to Subject Individual/Entity of this Report:

Occupation/Profession:

Address(es):

PO Box: **Street Address:** **City:**

State/Province: **Country:** **ZIP/Postal Code:**

Telephone: **Fax:** **Email:**

Identification Document Type (passport, driver's license, etc.):

Identification Document Number:

Date of Issue: **Place of Issue:**

Other signatories on account:

Other Information:

SECTION B: Subject(s) of Report (Legal Entities) (Attach Additional Sheets as Necessary)

Entity Type (company, trust, partnership, charity, etc.):

Name of Entity: **Jurisdiction of Incorporation:**

Purpose of Entity: **Date of Incorporation/Registration**

Registered Address:

Business Address:
(if different)

Shareholder Names:

Director Names:

Beneficial Owners, if different:

Other Signatories (if any):

Other Information:

APPENDIX B: Logs/Registers

MLRO log of PEP and high-risk clients

Name	Related entity/client	Nationality	Reason for potential PEP	Country of residence	Political connections	Key issues considered	Senior management approval	Ongoing monitoring: review date

SAR Log

Date	Client	Description	MLRO review	MLRO assessment	External date	FIA ref#

Declined Business Log

Name	Date	Reason (e.g. not within Business risk appetite)	Any suspicion	If Yes, see SAR Log

Training Log

Date of training	Staff	Title of training	Type of training (e.g. online)	Materials used (e.g. handouts)	Trainer	Summary of test results (pass/fail)

Sanction Log

Date	Client/matter	Description	MLRO/CO review	MLRO assessment	FSIU date and ref#	BMA date	Regime	License	Comment

APPENDIX C: Business Risk Assessment

24 Exchange must identify, assess, and present how the business will mitigate the ML/TF/Sanctions risks the Company faces amongst its customers, products, services, transactions, delivery channels, outsourcing arrangements and geographic connections. The AML Plan seeks to provide corresponding moderate to strong levels of mitigants and controls via the Company's policies, procedures and systems in view of the following identified Risks:

1. Clients – Low to Medium Risk: The client targets are large well-known international institutional clients seeking to enter the cryptocurrency market; predominantly from the USA, UK and Europe. Of the existing clients, the likelihood is that about 50 Participants of existing customers will request to enable access to the crypto market on the 24 Exchange Platform. All new customers, as noted in the AML Plan, must first go through the AML onboarding program of one of the pre-approved banks with which the Company will have an established business relationship for providing the Platform.
2. Geographical: Low to Medium Risk: the Company's operations are in US and Bermuda but the clientele are global with prohibitions on Iran and DPKR, and on other countries subject to financial or trade sanctions of Bermuda, UK and the USA; limitations (or prohibitions) and EDD on those with connections (either through operations, ownership, domicile) to high risk countries listed by the FATF[38] (or the Caribbean FATF), the Transparency International Index and the Basel AML Index.
3. Delivery channel – Medium: while the delivery channel is non-face to face, the business of the Company is providing a technology driven trading platform utilizing trade matching engines to select clients, Participants, from pre-approved institution, that are known to the pre-approved institution of the Company, or directly with the Company.
4. Product/Service - Medium: The Company is enabling the 24 hours matching trades of fiat or cryptocurrencies (both convertible and non-convertible) in deliverable and non-deliverable (Fiat-only settlement) contracts between a pre-approved set of institutional clients (counterparties or Participants) through its licensed proprietary multi-asset trading technology platform, the 24 Exchange Platform (**Platform**). Should the Company introduce a new product, practice, technology or service, the Company will document a risk assessment prior to launch of that product/service/practice/technology.
5. Outsourcing: Medium: The risk is high from the perspective that it is driven by technology and network connectivity in relation to the service agreements held with an pre-approved Agent, 11B[39], Cobalt and BreachLock. If a system on which the Platform relies fails to carry out its service, then then system failures (dependent upon the issue and severity) may enable weakness or gaps in the trading system. From the perspective of AMLATF functions such as screening and assistive CIP/KYC processes, the risk is Medium given that only a portion of the due diligence portion (screening) is outsourced to Mazars (screening services) and access to screening outputs and reviews are accessible at all times by the AMLCO via a shared secure data room. Note the 24 Exchange polices on Outsourcing and Business Continuity are to be read in conjunction with the AML Plan and assist in reducing the risk posed by the outsourcing arrangements.
6. Transactions: multi-asset trading technology platform enabling cryptocurrency FX exchange; although anonymous within the transactional trade to prevent such actions as market manipulation, all 24 Exchange Participants are known prior to participation and disclosed post settlement.

   The business risk assessment utilizes the Wolfsberg Principles in a four-tiered system: Low, Medium, High, and Highest (scores in the client risk assessment methodology have the corresponding scores of Low/1, Medium/3,

[38] http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-february-2021.htm

[39] Parties have signed a Letter of Intent to acquire the assets of 11B, which will be the current outsourcing executing element in-house

High/5 and Highest/7).

Entities /Client Risk – The following are permitted client profiles	
Publicly Held Companies	
• - Recognised Stock Exchange (most)	Low
• - Not Recognised Stock Exchange (rare)	Medium
Privately Held Companies	
• - Operating Company	Low
Financial Institutions/Banks and Regulated Brokers	
• - Recognised Stock Exchange plus Compliant Country	Low – Medium
• - Partially Compliant and not Compliant Country (rare)	Medium

Standard Inherent Risk Ratings	
FI Type / Business Unit / Business Line	**Inherent ML risk Rating (3 tier)**
Asset Management	Low to Medium
Brokerage	Medium to High
Commercial Banking	Medium to High
International Correspondent Banking	High
Credit & Other Card Banking	Low to Medium
Investment Banking	Low to Medium
Retail Banking	Medium to High
Wealth Management / Private Banking	Medium to High

Special Categories with Increased Risk Attributes – where applicable	**Rating**
Politically Exposed Person	
- Domestic (and IO PEP)	Medium
- International	High
Industry	
- Intermediaries/Commission agents (not likely)	Medium/High
- Digital Currency Providers or similar	Medium/High

Examples of Increased Risk Transactions	**Rating**
Rapid In/Out (High Velocity Turnover)	High
Other Unusual/Suspicious	High

Geography/Country Risk (e.g. Basel AML Index)	**Rating**
Institutional Client connections	
• - Higher Risk Countries	Higher
• - High Risk Countries	High
• - Medium Risk Countries	Medium
• - Low Risk Countries	Low

Other Qualitative Risk Factors	**Rating**
Client Base Stability	Low/Medium/High
Integration of IT Systems	Low/Medium/High
Expected Account/Client Growth	Low/Medium/High
Expected Revenue Growth	Low/Medium/High
Recent AML Compliance Employee Turnover	Low/Medium/High
Reliance on Third Party Providers	Low/Medium/High
Recent/Planned Introduction of New Products and/or Services	Low/Medium/High
Recent/Planned Acquisitions	Low/Medium/High
Recent Social Projects and Initiatives Related to AML Compliance Matters (e.g. Remediations, Eliminations of Back-logs, Offshoring)	Low/Medium/High
Recent Internal Audit or Other Material Findings	Low/Medium/High

APPENDIX D: Customer & Agent Due Diligence

D1: Customer Due Diligence

Standard CDD

Part 1: Natural Persons/Private Individuals

Obtain the following identification information for all private individuals, clients or select private individuals of a legal entity or legal arrangements as identified in Part 2:

- Full name, any former names (such as maiden name) and any other names used;
- Residential address[40]; and
- Date of birth.

Additional information for increased risk:

- Place of birth;
- Nationality;
- Sex;
- Source of funds;
- Occupation;
- Employer's name;
- Government issued personal identification number or other government issued unique identifier;
- Additional information or research through public databases surrounding any of the above gathered pieces of information;
- Approvals of Senior Management.

And in the case of a person purporting to act on behalf of a client, verifying that the person is in fact so authorised and identifying and verifying the identity of that person.

The following documents should be obtained to verify the information recorded pursuant to items noted:

- A certified copy of the pages of the individual's valid passport, national identity document
- Certified documentary evidence of the individual's permanent residential address.

Part 2: Legal Persons or Legal Arrangements

Customer due diligence legal requirements for legal persons or legal arrangements shall include documentation and information to support the following list:

- full name and trade name;
- date and place of incorporation, registration or establishment;
- registered office address and, if different, mailing address;
- address of the principal place of business;
- whether and where listed on a stock exchange;
- official identification number (where applicable);
- name of regulator (where applicable);
- legal form, nature and purpose (e.g. discretionary, testamentary, bare); and
- control and ownership.

In the case of a person purporting to act on behalf of a client, verifying that the person is in fact so authorised and

[40] Post Office Box numbers are not acceptable

identifying and verifying the identity of that person.

Additional information for increased risk include:

- Satisfactory evidence of the identity for more than 2 of the directors, partners as it applies to the legal entity/arrangement; dependent of level of high risk, then it may require all the identification and verification of all directors/partners;
- Certified copies of additional documentation;
- Additional independent research into the background and news surrounding the legal entity or arrangement and the natural person exerting control;
- Approvals of Senior Management.

Specifically:

Obtain the following standard evidence for corporate clients:

- Full name and former names;
- Country of incorporation;
- Registered number (if applicable);
- Registered office in country of incorporation (if applicable);
- Business address;
- Names and addresses of all directors (for private or unlisted companies); and
- Names and addresses of individuals who own or control over 10%
- The existence of the corporate client should be verified from:

  Confirmation of the company's listing (if applicable);

  - A search of the relevant company registry;
  - Identification documents per Part 1 for at least 2 directors (preference are those exerting control e.g. President, CEO) and
  - A certified copy of the company's certificate of incorporation and where necessary of other constitutional documentation.

The existence of the corporate client should be verified from:

- Confirmation of the company's listing (if applicable);
- A search of the relevant company registry;
- Identification documents per Part 1 for at least 2 directors (preference are those exerting control e.g. President, CEO) and
- A certified copy of the company's certificate of incorporation and where necessary of other constitutional documentation.

Carry out the following for client that are private and unlisted Companies

- Searches of the appropriate company registry should be carried out.
- Documents from certain countries may require further verification.
- Verification of one or more Directors should take place based upon its risk assessment of the company. Such verification is likely to be appropriate for those directors who can give instructions on the use or transfer of funds/assets.
- Individual beneficial owners should be verified even where those interests are held indirectly.
- Identities of signatories need only be verified on a risk-based approach.
- Higher risk clients should undergo EDD.

Obtain the following standard evidence for clients that are a Trust:

- Full name of trust;
- Nature and purpose of trust;

- Country of establishment;
- Name and address of the settlor of the trust assets;
- Names of all trustees;
- Depending on the terms of the trust, any named beneficiaries (primary or non-discretionary);
- Names of any Beneficial Owners (as defined); and
- Name and address of any instructing party to the trust, such as the enforcer, protector or controller;
- The identity of trustees should be verified as they exercise control. If the Trustee is a Regulated Institution, identification and verification procedures should reflect the standard risk-based approach for such an entity.

Less transparent and more complex structures will require EDD. Additional information may include:

- Donor/settler/grantor of the funds;
- Domicile of business activity;
- Nature of business activity; and
- Location of business activity.

Obtain the following Standard evidence for clients that are Partnerships/ Unincorporated associations includes:

- Full name;
- Business address;
- Names and addresses of all partners/principals who exercise control over management; and
- Names and addresses of individuals who own or control over 10% of capital, profits or voting rights;
- Identification documents for all partners as detailed above in Part 1.

Certification of Documentation

The person certifying the document as a true copy should only certify if both the original and photocopy are in front of him/her at the time of certification. The wording should state that it is a true copy of the original, that the photograph is a true likeness of the individual concerned.

The person certifying the document must be either:

- A member of the judiciary, a senior civil servant, or a serving police or customs officer: or
- An officer of an embassy, consulate or high commission of the country of issue of documentary evidence of identity; or
- A lawyer or notary public who is a member of a recognised professional body; or
- An accountant who is a member of a recognised professional body; or
- A company secretary who is a member of recognised professional body; or
- A compliance officer who is a member of a recognised professional body.

In addition to the signature, he/she should also print his/her name clearly in capitals and state his/ her qualification. His/her certification should be dated and include his/her contact details.

The Company will not accept a copy of identification documentation certified by the individual to which it relates, (including family members) nor a photocopy, facsimile or certified copy of a certified copy.

Certification is a recommendation in place of being able to mitigate impersonation fraud via verifying documentation against the customer in a face-to-face setting however it is not a requirement. Other options are available such as verification through reliable electronic databases or as referred to in the General Guidance Notes paragraph 4.42. Paragraph 4.42 provides for additional measures that may include one or a combination of the following:

  - Requiring the first payment to be carried out through an account in the customer's name with a regulated financial institution in Bermuda or a jurisdiction that imposes equivalent AML/ATF requirements;
  - Verifying additional aspects of the customer's identity, or of his electronic 'footprint';

- Requiring copy documents to be certified by an appropriate person;
- Telephone contact with the customer prior to opening the account on a home or business number which has been verified (electronically or otherwise), or a "welcome call" to the customer before transactions are permitted, using it to verify additional aspects of personal identity information that have been previously provided during the setting up of the account;
- Communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him, which, in full or in part, is required to be returned completed or acknowledged without alteration);
- Internet sign-on following verification procedures where the customer uses security codes, tokens or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address; and
- Other reasonable card or account activation procedures.

D2: Agent Due Diligence

As noted, the Company will periodically contract with one or more crypto asset custodian wallet provider or agents (hereinafter, an **Agent**) to facilitate the storage of digital assets, on and off-chain settlement, and provide verifiable proof of assets for transactions. Prior to contracting with a potential Agent, the following due diligence process must occur prior to engagement with periodic testing administered to the approved Agent to ensure appropriate measures to counter the facilitation of ML/TF through our Platform and associated service providers.

- **Step 1:** Due diligence on the potential Agent will be undertaken on a risk-sensitive basis mirroring the onboarding process of Customer Due Diligence for an Applicant of the Company.
- **Step 2**: Once the CDD is completed on the potential Agent, if the potential Agent is regulated and supervised for AMLATF purposes in an equivalent jurisdiction to Bermuda, OR provides evidence of an implemented AMLATF program of equivalent robustness, then upon senior management approval and or approval by the MLCO, the Agent may be engaged to facilitate the storage of digital assets, on and off-chain settlement, and provide verifiable proof of assets for transactions.
- **Step 3**: At least on an annual basis, and similar to the outsourcing obligations provided for in section 3.8, the Agent will be reviewed and tested for compliance.
- **Step 4**: Agents are obligated to report suspicious activity to the MLCO of the Company in the instances that the activity is connected to any Company or Company's customer matter and in view of Section 1.8 of this AML Policy.

All potential Agents must complete the Agent Due Diligence process and have the appropriate approval prior to engagement.

APPENDIX E: DAB Sector Red Flags

The following Appendix is a direct excerpt of the sectoral red flags of the Digital Asset Business sector as published by the BMA's Sector Specific DABA Guidance Notes (Annex VIII)

VIII.225 In addition to the non-exhaustive list of risk factors set forth above and in paragraph 2.35 of the main guidance notes, RFIs conducting DAB should consider sector-specific risk factors, including those in paragraphs VIII.57 and VIII.226 to VIII.231, in order to fully assess the ML/TF risks associated with a particular business relationship. The non-exhaustive list of sector-specific risk factors addresses customers, products, services, transactions, delivery channels, agents and other third parties, and geographic connections.

VIII.226 ***Customer risk factors include, but are not limited to:*** • A customer who offers false, fraudulent, or fictitious identification information or documents;

- Unjustified delays in the production of identity documents or other requested information;
- A non-face-to-face customer, where doubt exists about the identity of the customer;
- A customer who knows little or is reluctant to disclose basic details about the payee;
- A customer who has only vague knowledge about the amount of money involved in the transaction;
- A customer who gives inconsistent information;
- A customer transacting with a jurisdiction with which the customer has no apparent ties;
- A customer who appears to be acting on behalf of a third party but does not disclose that information;
- One or more persons other than the customer watching over the customer or waiting just outside of the RFI;
- A customer reading from a note or mobile phone while providing details of the transaction;
- A customer travelling unexplained distances to different locations of the RFI and/or its agents to conduct transactions;
- A customer who frequently deposits and withdraws funds from its account for no apparent reason and/or the activity does not appear commensurate with its established risk profile;
- A customer who owns or operates a cash-based business;
- The involvement of any PEPs as a person owning, controlling or representing the customer, or as a person otherwise connected with the customer;
- A customer who is known to the RFI to have been the subject of law enforcement sanctions in relation to crime generating proceeds;
- A customer who begins a transaction, but cancels the transaction after learning of a CDD requirement;
- A customer who threatens or tries to convince the RFI's personnel to avoid reporting;
- A customer who is a member of a class of persons considered higher risk for ML/TF;
- The unnecessary granting of a power of attorney;
- A customer who is unwilling or unable to provide satisfactory information to verify the source of wealth or source of funds;
- Levels of assets or transactions that exceed what a reasonable person would expect of a customer with a similar profile;
- A customer offering to pay extraordinary fees for unusual services, or for services that would not ordinarily warrant such a premium;
- Requests for payment to be made via the RFI's client money account, where such a payment would normally be made from a customer's own account;
- Requests for anonymity that go beyond a reasonable request for discretion;
- A customer or counterpart who is another DAB or financial institution which has been sanctioned by a respective national competent authority for non-compliance with applicable AML/ATF regulations and who is not engaging in remediation to improve its compliance;
- A customer who uses agents or associates such that it is difficult for the RFI to identify the beneficial owner of the funds;
- A transaction or business relationship that uses complex networks of legal arrangements where there is no

apparent rationale for the complexity, or where the complexity appears to be intended to conceal the true ownership or control arrangements from the RFI;

- A customer that is involved in online gambling; and
- A customer that transacts with mixing/tumbler services or the dark web.

VIII.227 ***Products and services risk factors include, but are not limited to:*** • Products or services that may inherently favour anonymity;

- Products that can readily cross international borders, such as cash, online money transfers, stored value cards, money orders and international money transfers by mobile phone;
- Products or services that have a very high or no transaction limit; and
- Products or services that permit the exchange of cash for a negotiable instrument, such as a stored value card or a money order.

VIII.228 ***Transaction risk factors include, but are not limited to:*** • Transactions that are just below the RFI's thresholds for due diligence checks;

- Transactions that appear to have no obvious economic or financial basis;
- Unusual, complex or uncharacteristically large transactions;
- Transactions that route through third countries or third parties, including mixers;
- Transactions that can be traced to or from the dark web or mixing /tumbler services;
- Transactions accompanied by information that appears false or contradictory;
- A wire transfer or money transmission that is not accompanied by all required information;
- A transaction to a country or region that is outside of the RFI's normal business;
- Large cash or bearer instrument transactions in circumstances where such a transaction would normally be made by cheque, banker's draft or wire transfer;
- Transfers to the same person from different individuals or to different persons from the same individual with no reasonable explanation;
- Transfers of funds that are not in line with the stated business activities of the customer;
- Customers requesting transfers to or from overseas locations with instructions for payment to be made in cash;
- Transactions from another DAB that is not acting as the RFI's agent;
- Transactions of a size or volume that exceeds what a reasonable person would expect of a customer with a similar profile, or given the nature and stated purpose of the transaction or business relationship;
- One-off transactions giving rise to suspicion; and
- Requests for funds, shares or other assets to be transferred to PEPs or higher-risk charities or other not-for-profit organizations not subject to effective supervision and monitoring.

VIII.229 ***Delivery channel risk factors include, but are not limited to:*** • A lack of face-to-face contact with the customer and any persons associated with them;

- Any request to carry out significant transactions using cash, or using any payment or value transfer method that obscures the identity of any of the parties to the transaction; and
- The use of third-party intermediaries, agents or brokers.

VIII.230 ***Agent and other third party risk factors include, but are not limited to:*** • Agents for which the RFI is unable to satisfactorily complete the steps set forth in paragraph VIII.168;

- Agents that refuse to provide information requested for inclusion in the RFI's agent list;
- Agents representing more than one RFI;
- An agent that has its own agents for which it provides inadequate supervision;
- Agents located in a higher-risk jurisdiction or serving higher-risk customers or transactions;
- Agents that are, or involve, PEPs;
- Agents conducting an unusually high number of transactions with another agent location, particularly with an

agent in a high risk geographic area or corridor;

- Agents that have transaction volume that is inconsistent with either overall transaction volume or relative to typical past transaction volume;
- Agents that have been the subject of negative attention from credible media or law enforcement sanctions;
- Agents that have failed to attend or satisfactorily complete the RFI's training programs;
- Agents that do not effectively manage compliance with the RFI's AML/ATF policies, procedures and controls;
- Agents that fail to provide required originator information upon request;
- Agents that conduct inconsistent or substandard data collection or record keeping;
- Agents willing to accept false identification or identification records that contain false information, non-existent addresses that would be known to be non-existent to a person in that area, or phone numbers that are used as fillers;
- Agents with a send-to-receive ratio that is not balanced, as compared with other agents in the locale, or that engage in transactions or activities indicative of complicity in criminal activity;
- Agents whose ratio of questionable or anomalous customers to customers who are not questionable or anomalous is out of balance with the norm for comparable locations;
- Agents who move money through RFI accounts in amounts not corresponding with the agent's digital asset business on behalf of the RFI;
- Agents that are new businesses without an established operating history; and
- An agent that fails the RFI's transaction testing for compliance with the RFI's AML/ATF policies, procedures and controls.

VIII.231 ***Geographic risk factors include, but are not limited to:*** • A customer entity established with funds originating from banks in high-risk jurisdictions;

- A customer, person acting on behalf of the customer, person owning or controlling the customer or any agent or other third party associated with the customer who is a resident in, or citizen of, a high-risk jurisdiction;
- A DAB transaction to, though, or from a high-risk jurisdiction;
- A non-face-to-face transaction initiated from a high-risk jurisdiction;
- A DAB transaction linked to business in or through a high-risk jurisdiction;
- DAB involving persons or transactions with a material connection to a jurisdiction, entity, person, or activity that is a target of an applicable international sanction; and
- A DAB relationship or transaction for which an RFI's ability to conduct full CDD may be impeded by another jurisdiction's confidentiality, secrecy, privacy or data protection restrictions.

APPENDIX F: AMLATF & Sanctions Policy Declaration

24 Exchange

Anti-Money Laundering, Anti-Terrorist Financing (AMLATF) & Sanctions

Declaration

I have been provided a copy of the 24 Exchange's Anti-Money Laundering, Anti-Terrorist Financing (**AMLATF**) & Sanctions Policy and Procedures (**AML Plan**). I have been informed about its content, requirements, and expectations and hereby agree to abide by the AML Plan as a condition of my employment and my continuing employment at 24 Exchange.

I understand that the AML Plan applies equally to 24 Exchange Bermuda Limited, as well as its affiliate, 24 Exchange Broker Limited.

I understand that if I have questions, at any time, regarding the Company's or my own AMLATF & Sanctions obligations, I will consult with the Anti-Money Laundering Compliance Officer (**AMCLO**), who at this time is David Sassoon.

Employee Signature: _____

Employee Printed Name: _____

Date: _____

APPENDIX G: PEPs

Natural persons, who have or have had a high political profile or hold or have held public office or a prominent function in an international organisation, can pose a higher risk as their position may be abused for ML and related predicate offences such as corruption and bribery, as well as for the financing of terrorism and proliferation. This risk also extends to their family members and known close associates. PEP status itself does not, of course, incriminate natural persons or entities.

Definitions of PEPs: including foreign, domestic and international organisation PEPs

A PEP is defined in Regulation 11 of POCR as a natural person who, at any time in the preceding year, has been entrusted with a prominent public function by a government of a country or territory, or with a prominent function by an international organisation. The application of AML/ATF regulations concerning PEPs also extends to members of their immediate families and known close associates.

The application of AML/ATF regulations concerning PEPs extends to the following persons:

PEPs in or from any country or territory outside Bermuda:

a) Heads of state, heads of government, ministers and deputy or assistant ministers;

b) Members of parliament and senior political party officials;

c) Members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances;

d) Members of the courts of auditors or of the boards of central banks;

e) Ambassadors, charges d'affaires and high-ranking officers in the armed forces;

f) Members of the administration, management or supervisory bodies of state-owned enterprises; and

g) Natural persons entrusted with a prominent function by an international organisation, as defined in Regulation 2(1) of POCR, including senior management, directors and deputy directors and members of the board or equivalent function of an international organisation.

PEPs in or from Bermuda:

a) The Governor, Premier, Ministers and Junior Ministers;

b) Members of the Legislature;

c) Permanent Secretaries;

d) Judges of the Supreme Court and Court of Appeal and Magistrates;

e) Members of the Board or senior management of the Authority and the Regulatory Authority of Bermuda;

f) Commissioned officers in the Royal Bermuda Regiment and senior officers above the rank of Sergeant (which includes the Commissioner of Police) of the Bermuda Police Service;

g) Members of the Board of Directors and the Chief Executive Officer (by whatever name called) of the Bermuda Government owned or controlled enterprises or authorities, including but not limited to:

i. West End Development Corporation;

ii. Bermuda Land Development Corporation;

iii. Bermuda Development Agency;

iv. Bermuda Tourism Authority;

v. Bermuda Deposit Insurance Corporation;

vi. Bermuda Casino Gaming Commission; and

h) Natural persons entrusted with a prominent function by an international organisation, as defined in Regulation 2(1) of POCR, including senior management, directors and deputy directors and members of the board or equivalent function of an international organisation.

The above categories are not exhaustive but do not include middle-ranking or more junior officials. Functions exercised at levels lower than national should normally not be considered prominent.

However, when their political exposure is comparable to that of similar positions at national level, the Company should consider, on a risk-based approach, whether persons exercising those public functions should be considered as PEPs.

Family members of natural persons entrusted with the requisite public or prominent function:

a) Spouse;

b) Partner (including a person who is considered by national law as equivalent to a spouse);

c) Children and their spouses or partners;
d) Parents; and
e) Siblings.

Close associates of natural persons entrusted with the requisite public or prominent function:
a) Natural persons known to have joint beneficial ownership of a legal entity or legal arrangement with a PEP;
b) Natural persons who have sole beneficial ownership of a legal entity or legal arrangement that has been set up for the benefit of a PEP; and
c) Natural persons known to have any other close business relations with a PEP.

The following sources can be consulted to discover foreign, domestic and international organisation PEPs:

- Third party databases (e.g., eSpear)
- Open Source Searches (eg. Google)
- Royal Gazette[41];
- Bermuda Parliament Website[42] (and register of interests list[43]);
- Bermuda Government website such as that on Government boards and committees[44];
- Relevant Websites of Government Entities such as:
    - The Bermuda Hospitals Board[45],
    - Bermuda Housing Corporation[46],
    - West End Development Corporation[47],
- The list of current clients of the Bermuda Auditor General[48].

[41] www.royalgazette.com

[42] www.parliament.bm

[43] www.parliament.bm/about-parliament/house-of-assembly/register-of-interest.aspx

[44] https://www.gov.bm/government-boards-and-committees

[45] http://bermudahospitals.bm/about-us/our-team/board-members/

[46] http://www.bhc.bm/index.php/page/view/8

[47] http://www.choosewestend.org/board-of-directors

[48] http://www.oagbermuda.bm/our-clients.php