FSRA

ST HELENA, ASCENSION AND TRISTAN DA CUNHA

FSRA DIRECTIVES

Directive on Anti-Money Laundering, Counter-Terrorist Financing and Financial Sanctions Compliance

1 AUGUST 2025

www.fsra.sh

Section 1 – OVERVIEW

INTRODUCTION

1.1	This Directive is issued by the Financial Services Regulatory Authority (FSRA) under section 4 of the Financial Services Ordinance 2008 and its effective date is 1 August 2025.
1.2	Subject to 1.5, this Directive applies to any business that is licensed by the FSRA. It applies to a business that carries out regulated activities on any of St Helena, Ascension or Tristan da Cunha. Unless specified to the contrary, a reference in this Directive to "St Helena" is to be read as including all of St Helena, Ascension and Tristan da Cunha.
1.3	Terms used in this Directive should be interpreted by reference to the definitions set out in the Financial Services Ordinance 2008 and the Financial Services Regulations 2017, unless otherwise defined in this Directive.
1.4	In addition, this Directive also: (a) provides some general background on the subject of money laundering, terrorist financing and financial sanctions measures; and (b) practical guidance to assist a relevant business to devise and implement policies, procedures and controls, taking into consideration their own circumstances, so as to meet the FSRA's expectations in relation to anti-money laundering, counter-terrorist financing and sanctions compliance.
1.5	In relation to a general insurance intermediary, a general insurer or a general reinsurer, the only provisions of this Directive that are directly applicable relate to financial sanctions measures. However, a relevant business of that kind may wish to have regard to the contents of the Directive more generally when designing and implementing its controls to manage the financial crime risk to which it is exposed.
1.6	This Directive sets out the minimum steps that a relevant business must take to combat money laundering and to counter terrorist financing. Accordingly, where the Directive uses the word "should" in relation to an action, consideration or measure, it means that the provision is a mandatory requirement. This Directive is not intended to be exhaustive in relation to the measures that a relevant business may need to take, and other measures may be required, depending on the business's circumstances. At the same time, a relevant business should apply the contents of this Directive in a risk-based, proportionate way, taking into account such factors as the nature, size and complexity of its business.
1.7	Compliance with this Directive will be enforced through the Financial Services Ordinance 2008 or successor legislation. A relevant business which does not comply with this Directive may be subject to disciplinary or other actions under the Financial Services Ordinance 2008.
1.8	In assessing whether an applicant for a licence to carry out a regulated activity is a fit and proper person, the FSRA will have regard to the ability and willingness of that person to comply with this Directive. In addition, non-compliance with this Directive may also reflect adversely on the continuing fitness and properness of a relevant business and of its sole proprietor, ultimate beneficial owner, directors, managers or partners.

1.9	A relevant business should notify the FSRA without delay when it becomes aware that it has failed to comply with this Directive. There is no materiality threshold in this respect and a relevant business is therefore required to report every breach. The FSRA will treat a failure to report a breach by a relevant business as a disciplinary matter. Where the FSRA has evidence that an individual who has been approved as fit and proper by the FSRA deliberately withheld the fact of a breach or has communicated the circumstances of a breach with insufficient candour or in a way intended to mislead the FSRA, the FSRA will consider whether that behaviour constitutes grounds for revocation of that individual's approval.

WHAT ARE MONEY LAUNDERING AND TERRORIST FINANCING?

1.10	In broad terms, money laundering is an act which is intended to disguise the illegal origin of property that is or is derived from the proceeds of crime.
1.11	The Money Laundering Ordinance 2008 contains a detailed definition of "money laundering" as an act which constitutes: (a) in relation to criminal property, the offence of acquiring, concealing, converting, disguising, importing, possessing, removing, transferring or using that property; or (b) the offence of entering into or becoming concerned in an arrangement which a reasonable person would know or suspect facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person; or (c) the offence of attempting, conspiring or inciting to do any of the acts in (a) or (b); or (d) the offence of aiding, abetting, counselling or procuring the commission of any of the acts in (a) or (b).
1.12	Money laundering generally follows three stages, each frequently involving numerous transactions: (a) "Placement" - an initial stage in which the launderer introduces their illegal profits from criminal activity into the financial system (e.g., by depositing funds directly into an account at a bank, perhaps by breaking larger amounts into smaller sums, or by converting money into a financial instrument); (b) "Layering" - after the funds have entered the financial system, a second stage involves creating complex layers of financial transactions designed to disguise the illicit origins of the money, subvert the audit trail and provide anonymity (e.g., by buying and selling investments, or by perhaps wiring money through a series of accounts at various banks in multiple jurisdictions); and (c) "Integration" - once the funds are so far removed from their criminal source that it is not feasible for the authorities to trace their origins, the launderer effectively returns the laundered proceeds back into the legitimate economy as ostensibly "clean" money, the result of legitimate business activities (e.g., by the purchase of real estate).
1.13	Terrorists and terrorist organisations need finance in order to carry out their activities. They may seek to keep secret their sources of funding. This would typically involve obscuring or disguising where their funding is coming from. A terrorist group might have links with organised criminal activity, but it might also be funded using income that has been legitimately obtained. Regardless of whether their funds come from a legitimate or illegitimate source, terrorist groups can be expected to launder those funds, in order to be able to use them without bringing about the intervention of law enforcement authorities.

1.14	There are overlaps and similarities between terrorist financing and money laundering. Terrorism financing involves the raising and processing of funds to supply terrorists with resources. It may be further expressed as the provision or collection of funds with the intention of being used to carry out terrorist acts whether by terrorist organisations or by individuals acting alone or in small networks. The UK Terrorism Act 2000, which applies in St Helena, establishes a range of offences, including, in summary: (a) being involved in fundraising (including by making a contribution), knowing or having reasonable cause to suspect that the money or other property raised may be used for the purpose of terrorism; (b) using money or other property for terrorist purposes, or possessing it intending that it should be used, or having reasonable cause to suspect that it may used, for the purpose of terrorism; (c) becoming involved in a funding arrangement which makes, or is intended to make, money or other property available to another while knowing or having reasonable cause to suspect that it may be used for terrorist purposes; and (d) becoming involved in arrangements for laundering money or other property to facilitate the retention or control of terrorist property by, or on behalf of, another person including by concealment, removal from the jurisdiction or by transfer to nominees.
1.15	The following abbreviations are used in this document: AML anti-money laundering CFT countering the financing of terrorism ML money laundering TF terrorist financing

Section 2 – A RISK-BASED APPROACH

INTRODUCTION

2.1	A relevant business should take a risk-based approach to AML/CFT matters. This means that a relevant business should identify, assess and understand the ML/TF risks to which it is exposed and take measures commensurate with those risks in order to manage and mitigate them effectively. This approach enables a relevant business to make more efficient and effective use of its resources, proportionate to the risks faced by that business. A relevant business should therefore take a risk-based approach to the design and implementation of its AML/CFT policies, procedures and systems ("AML/CFT Controls") in order to manage and mitigate ML/TF risks.

INSTITUTIONAL ML/TF RISK ASSESSMENT

2.2	To implement an appropriate risk-based approach, a relevant business will need to identify, assess and understand the risks of ML and TF in its business. Accordingly, a relevant business should carry out an institutional ML/TF risk assessment which should cover: (a) its customers; (b) the countries or jurisdictions in which the business operates, and the countries or jurisdictions which its customers are in or from, or from which they derive their funds; (c) the products, services, and delivery channels of the business; and (d) the nature of the transactions that it carries out for its customers.

2.3	In relation to its institutional risk assessment, a relevant business should ensure that: (a) it is documented in writing; (b) it sets out the risk assessment process, including the identification and assessment of relevant risks supported by qualitative and quantitative analysis, using information obtained from appropriate sources; (c) it takes account of all relevant risks before determining what is the level of overall risk, and the appropriate type of mitigation to be applied; (d) it is approved by the Board of that business; and (e) there is a process in place to ensure that it is kept up-to-date.
2.3	The scale and scope of the institutional ML/TF risk assessment should be proportionate to the nature, size and complexity of the business of a relevant business.
2.4	Where a relevant business whose business operations are based in St Helena has a branch or subsidiary in another jurisdiction, the institutional ML/TF risk assessment of that business should take account of the ML/TF risks in any such branch or subsidiary.
2.5	A relevant business should ensure that it keeps its institutional ML/TF risk assessment up-to-date, by carrying out a new assessment at least once every two years and whenever events occur which have a material impact on its business and ML/TF risk exposure.
2.6	A relevant business should ensure that it is able to provide its completed institutional ML/TF risk assessment to the FSRA promptly on request.
CUSTOMER RISK ASSESSMENT	
2.7	In relation to a proposed business relationship, a relevant business should carry out a risk assessment to assess the ML/TF risks associated with that relationship. A customer risk assessment of this type that is carried out at the initial or onboarding stage of the CDD process will serve to determine the extent of the CDD measures that a relevant business should apply. The amount and type of information obtained, and the extent to which this information is verified, should be increased where the ML/TF risks associated with the business relationship are higher. A relevant business should take into account the result of the customer risk assessment when determining whether to enter into the business relationship. A relevant business should also carry out a customer risk assessment before carrying out an occasional transaction for a customer.
2.8	A relevant business should use the result of a customer risk assessment to determine the amount and nature of ongoing monitoring of each business relationship. As a customer's risk profile may change over time, a relevant business should periodically review and update that customer's risk assessment, particularly during ongoing monitoring. A relevant business should consider whether the result of any periodic review provides grounds for increasing the amount of CDD measures or the intensity of ongoing monitoring for the business relationship, or for terminating that relationship.

2.9	A relevant business should take a risk-based approach to the design and implementation of its customer risk assessment framework, and the complexity of the framework should be proportionate to the nature, scale and complexity of that business. It should also take close account of the results of the institutional ML/TF risk assessment. In general, the customer risk assessment framework will include customer risk factors, country risk factors, product, service or transaction risk factors, and delivery channel risk factors.
2.10	A relevant business should document its customer risk assessment methodology, and it should ensure that it leads to the classification of business relationships into a number of ML/TF risk categories, including a higher risk category. In relation to every business relationship, a relevant business should keep records and supporting documents so that it can demonstrate to the FSRA (a) how it has assessed a customer's ML/TF risks; and (b) that the extent of CDD measures and ongoing monitoring is appropriate based on that customer's ML/TF risks.

RISKS ASSOCIATED WITH NEW BUSINESS DEVELOPMENTS

2.11	A relevant business should identify and assess the ML/TF risks that may arise in relation to: (a) the development of new products and new business practices, including new delivery channels; and (b) the use of new or developing technologies for products. A relevant business should ensure that it undertakes the risk assessment prior to the launch of the new products, new business practices, or the use of new or developing technologies. The FSRA will expect that a relevant business will be able to demonstrate that it has taken adequate steps to manage and mitigate any risks identified.

LIMITS OF THE RISK-BASED APPROACH

2.12	The risk-based approach does not apply to the reporting of suspicious activities. Such reports should be made whenever the suspicion arises.

Section 3 – AML/CFT CONTROLS

AML/CFT CONTROLS

3.1	A relevant business should take all reasonable measures to ensure that there are proper controls to mitigate the risks of ML/TF and to ensure adherence to any anti-money laundering requirements to which it is subject. So that it may comply with this requirement, a relevant business should therefore put in place and maintain appropriate AML/CFT Controls.
3.2	A relevant business should ensure that it: (a) has AML/CFT Controls, which are approved by senior management, to enable the business to adequately manage and mitigate its ML/TF risks; (b) monitors the implementation of those AML/CFT Controls, and enhances them if needed; and (c) takes additional measures to manage and mitigate any identified higher ML/TF risks.

3.3	A relevant business should put in place AML/CFT Controls commensurate with the nature, scale and complexity of its business and the associated ML/TF risks. AML/CFT Controls should include: (a) customer due diligence measures and ongoing monitoring; (b) risk assessment and management; (c) compliance oversight arrangements; (d) an independent audit function; (e) employee screening; (f) employee training; (g) arrangements for disclosing suspicious transactions; and (h) record-keeping.

THE ROLE OF SENIOR MANAGEMENT

3.4	It is the responsibility of the senior management of a relevant business to ensure that the business's ML/TF risks are effectively managed. Senior management should ensure that adequate AML/CFT Controls are implemented for that purpose. So that senior management can properly discharge their responsibility to ensure that ML/TF risks are effectively managed, a relevant business should ensure that senior management receive sufficient information about those risks to enable them to make informed decisions. The FSRA expects that the senior management of a relevant business should be able to demonstrate to the FSRA the adequacy of the steps that they have taken to discharge their responsibilities.
3.5	As part of their responsibility to ensure that effective AML/CFT Controls are implemented, the senior management of a relevant business should appoint competent individuals to act as Compliance Officer (CO) and Money Laundering Reporting Officer (MLRO). Senior management should ensure that the CO and MLRO are: (a) normally based in St Helena; (b) technically competent, with a comprehensive understanding of the AML/CFT requirements that apply to the business and the ML/TF risks in the business; (c) adequately resourced, including having an adequate number of supporting staff; (d) independent of the business functions; (e) sufficiently senior; (f) able to access all information, including client files, that they require to discharge their responsibilities; and (g) able to communicate directly with the senior management where necessary.

COMPLIANCE OFFICER

3.6	The CO of a relevant business is responsible for oversight of all activities relating to AML/CFT in that business. In particular, the CO is responsible for: (a) designing and implementing AML/CFT Controls which satisfy statutory and regulatory requirements and which are effective for the purpose of managing that business's ML/TF risks; (b) monitoring the effectiveness of AML/CFT Controls; (c) designing and implementing appropriate training for staff on AML/CFT matter; and (d) reporting on AML/CFT matters to senior management, including bringing instances of non-compliance or risk events to the attention of senior management promptly.

MONEY LAUNDERING REPORTING OFFICER

3.7	The MLRO of a relevant business is responsible for: (a) reviewing all internal reports of suspicious transactions and exception reports and determining whether it is necessary to file a Suspicious Activity Report (SAR) with the Royal St Helena Police Service and the Money Laundering Regulatory Authority; (b) keeping records relating to the review of those reports; (c) providing guidance to staff on how to avoid "tipping-off" if any SAR is filed; and (d) acting ordinarily as the main point of contact with the Royal St Helena Police Service and the Money Laundering Regulatory Authority.
3.8	Depending on the nature, scale and complexity of a relevant business and its ML/TF risk profile, it may be acceptable to appoint the same person as the CO and MLRO. The larger and more complex and the higher the ML/TF risk exposure of the relevant business, the more likely it is that it will be appropriate to appoint separate people to the roles. Whether or not that is the case, it will be important to recognise where the roles differ. A sole trader with no employees will, by default, be the relevant business's CO and MLRO.

INTERNAL AUDIT

3.9	Where appropriate with regard to the nature, size and complexity of its business, a relevant business should establish an internal audit function with responsibility to: (a) examine and evaluate the adequacy and effectiveness of the AML/CFT Controls adopted and implemented by the business; (b) make recommendations in relation to those AML/CFT Controls, and monitor the relevant business's implementation of those recommendations where adopted; and (c) review the effectiveness of the risk management and compliance functions.
3.10	Where appropriate, a relevant business should also seek a review from an external party, such as a professional advisory firm, as to the adequacy and effectiveness of its AML/CFT Controls.

SCREENING

3.11	A relevant business should carry out screening of its staff, both before they are appointed, and at regular intervals during the course of their appointment. Screening of employees for these purposes means an assessment of the skills, knowledge and expertise of the individual to carry out their functions effectively, and as to the conduct and integrity of the individual.

Section 4 – CUSTOMER DUE DILIGENCE (CDD)

CDD MEASURES

4.1	A relevant business should carry out CDD measures according to this Directive and any applicable statutory or regulatory requirements. A relevant business should also establish and implement effective AML/CFT Controls to ensure that the necessary CDD measures are applied correctly.
4.2	A relevant business should take a risk-based approach to carrying out CDD and the measures it takes should be proportionate to the ML/TF risks associated with a business relationship. A relevant business will need to conduct additional measures (referred to as enhanced due diligence (EDD)) where higher ML/TF risks are present, but it may conduct simplified customer due diligence (SDD) in certain circumstances where those risks are assessed to be low.
4.3	A relevant business should ensure that its CDD measures include: (a) identifying the customer and verifying the identity of that customer on a timely basis, using documents, data or information from a reliable and independent source; (b) in a situation where there is a beneficial owner, identifying that beneficial owner and taking reasonable measures to verify their identity; (c) where a person purports to act on behalf of a customer, identifying that person and taking reasonable measures to verify their identity, and also verifying that person's authority to act on the customer's behalf; (d) where the purpose and intended nature of the intended business relationship or occasional transaction is not obvious, taking steps to understand, including obtaining information, about those matters; and (e) in the case of a company, body corporate, partnership trust or similar legal arrangement, taking steps to ascertain the ownership and control structure of the customer and the nature of the customer's business.
4.4	In this Directive, "customer" means the party with which a relevant business establishes a business relationship or on whose behalf that business carries out an occasional transaction.

WHEN TO APPLY CDD MEASURES

4.5	A relevant business should apply CDD measures: (a) before establishing a business relationship with a customer; (b) before carrying out for a customer any occasional transaction that involves an amount equal to or above SHP 500 (or equivalent value in a foreign currency) whether carried out in a single action or in several actions that appear to be linked; (c) if ever a relevant business suspects that the customer is involved in ML/TF, regardless of the monetary levels of transactions; (d) if ever the business has reason to question the adequacy or veracity of any documents, data or information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity; and (e) if it becomes aware that any circumstances of a customer that are material to its risk assessment for that customer have changed; or (f) on the occurrence of any other trigger event.
4.6	Where a relevant business is unable to apply CDD measures, it should not establish a business relationship or carry out any occasional transaction with that customer and should assess whether this failure provides grounds for knowledge or suspicion of ML/TF.
4.7	In this Directive, "business relationship" means a business, professional or commercial relationship between a relevant business and a person that has an element of duration, or the relevant business expected it to have at the time the person was a potential customer.
4.8	In this Directive, "occasional transaction" means a transaction between a relevant business and a customer who does not have a business relationship with the relevant business. A relevant business should be alert to the possibility that a series of linked occasional transactions could meet or exceed the CDD threshold of SHP 500. Where a relevant business becomes aware that the threshold is reached or exceeded, full CDD procedures should be applied.
HOW TO CARRY OUT IDENTIFICATION AND VERIFICATION OF IDENTITY - CUSTOMERS	
4.9	A relevant business should identity its customer and verify the identity of that customer by means of documents, data or information provided by: (a) a governmental body, regulator or other public body; (b) the St Helena Companies Registry or a similar body in another jurisdiction; or (c) any other reliable and independent source.
4.10	It may be possible for a relevant business to be reasonably satisfied as to a customer's identity based on, in appropriate circumstances, written assurances from professional firms that have dealt with the customer for some time.
FOR INDIVIDUALS	

4.11	To identify a customer that is an individual, a relevant business should collect at least: (a) the individual's full name; (b) their date of birth; (c) their nationality; (d) their unique identification number and the type of document to which it pertains (e.g., passport); and (e) their residential address.
4.12	To verify the identity of a customer that is an individual, a relevant business should verify the matters listed in 4.11 by reference to documents, data or information provided by a reliable and independent source, including for example: (a) a valid, unexpired passport or other travel document bearing the person's photograph, which states the nationality, domicile or place of permanent residence of the holder; (b) a valid, unexpired national driving licence bearing the person's photograph; (c) a document issued by a governmental body; or (d) in respect only of verification of residential address, an account statement issued by a bank, a utility bill, or correspondence received from a government department, in any case issued no more than three months before the relevant business carries out its CDD measures.
4.13	Where an individual does not have a passport, travel document or driving licence with a photograph, a business may, applying a risk-based approach, accept other documents as evidence of identity (wherever possible such documents should have a photograph of the individual). A relevant business should not reject an individual as a customer simply because that individual does not have a passport, travel document or driving licence with a photograph. The FSRA expects that a relevant business should take proactive steps to ensure that all individuals whose ML/TF risk is within the business's risk appetite are able to access services offered by that business. The FSRA further expects that a relevant business should apply identification and verification measures in an objective and even-handed manner to all individuals.
4.14	A relevant business may not rely on a document issued by that business, or by a branch or subsidiary of that business, to an individual by way of verification of that individual's identity.
FOR COMPANIES, OTHER BODIES CORPORATE, PARTNERSHIPS AND ASSOCIATIONS	
4.15	To identify a customer that is a company, other body corporate, partnership or an association, a relevant business should collect at least: (a) its full name (b) its date of incorporation, foundation or registration (c) its place of incorporation, foundation or registration; (d) its registered office address and, if different, the address from which business activities are conducted (a post office box address is not acceptable in either case); (e) its unique identification number (e.g., incorporation number) and the type of document to which it pertains; and (f) its tax identification number.

4.16	To verify the identity of a customer that is a company, body corporate, partnership or association, a relevant business should verify the matters listed in 4.15, together with its continued existence at the time of verification and the constitutional or other legal arrangements that govern its operation, by reference to documents, data or information provided by a reliable and independent source. Such documents, data and information include for example: (a) its certificate of incorporation, or other such business registration document; (b) its entry in a register maintained by a company registry; (c) a company search report from the registry in the place of incorporation or registration; (d) a certificate of incumbency or equivalent issued by a company's registered agent, confirming the identity and authority of individuals holding specific positions, including directors, officers, or key shareholders; (e) a certificate of good standing; (f) its record of registration with a regulator or professional body; (g) its constitutional documents, including its Articles of Association, byelaws or rules; (h) details of the ownership and control structure of the company (e.g., an ownership chart); (i) its partnership agreement or deed; or (j) other relevant documents issued by a governmental body, regulator or other public body.
4.17	It is likely that a relevant business will need to collect several of the documents referred to in 4.16 in order to satisfactorily verify the identity of the customer. In particular, a relevant business should ensure that the documents collected enable it to confirm not just that that the company, body corporate, partnership or association has been established, but that it still exists at the time that verification takes place. Where the customer is a company, a relevant business will need to obtain a very recent certificate of incumbency, certificate of good standing, company search report or equivalent document.
4.18	A relevant business should decide on the basis of the ML/TF risk whether there is a need for further verification or to obtain additional information in respect of the customer.
4.19	Some partnerships are bodies corporate and should be treated as such for the purpose of applying CDD measures. Other partnerships (including some law firms and accountants) are unincorporated bodies and may be long-established and well-known. The names of their partners may be in the public domain. Confirmation of the customer's membership of a relevant professional or trade association may be enough to provide reliable and independent verification of the identity of the customer. In the case of less well-known partnerships and other unincorporated bodies the relevant business should primarily have regard to the number of partners and controllers. Where there are relatively few, the customer should be treated as a collection of individuals so that each of them will be subject to identification and verification procedures. For a partnership or other body having a larger number of partners and controllers, the relevant business should make a judgment on whether it will rely on evidence of membership of a relevant professional or trade association.
4.20	For associations, clubs, societies, charities and religious bodies, a relevant business should establish that the organisation has a legitimate purpose, initially by obtaining its constitution, byelaws or rules.

FOR TRUSTS AND SIMILAR LEGAL ARRANGEMENTS	
4.21	In relation to trusts, a relevant business should identify and verify the trust as a customer. However, most trusts do not have a separate legal personality and cannot enter into business relationships or be a party to transactions themselves. In this case it is the trustee who enters into a business relationship or carries out transactions on behalf of the trust and the trustee should be regarded (in addition to the trust itself) as being a customer of the relevant business. The licensee should identify and verify the identity of the trustee according to the requirements for a customer that is an individual, company, body corporate or partnership, as applicable.
4.22	To identify a customer that is a trust or similar legal arrangement, a relevant business should collect at least: (a) the name of the trust or legal arrangement, if any; (b) the date of its settlement or establishment; (c) the jurisdiction whose laws govern the trust or legal arrangement; (d) its unique identification number issued by a governmental body, registrar of trusts or regulator; (e) its registered office address, if any; and (f) its tax identification number.
4.23	To verify the identity of a customer that is a trust or similar legal arrangement, a relevant business should verify the matters listed in 4.22, together with its continued existence at the time of verification, its legal form and the constitutional or other legal arrangements that govern its operation, by reference to documents, data or information provided by a reliable and independent source. Such documents, data and information may include for example: (a) the trust deed or similar instrument; (b) the entry in the register of the registrar of trusts or other register maintained by a governmental body; (c) written confirmation from a trustee acting in a professional capacity; or (d) written confirmation from a lawyer who has reviewed the relevant instrument.
4.24	A relevant business should in all cases endeavour to obtain a copy of the complete trust deed, which should be retained with the CDD records.
DOCUMENT AND INFORMATION INTEGRITY ISSUES	
4.25	A relevant business should be alert to the fact that some types of documents are more easily forged than others. If there is suspicion of forgery in relation to any document provided by a customer, the business should take appropriate steps to establish whether the document provided is genuine. This may include, for instance, making enquiries with authorities to ascertain whether a document (such as a passport) has been reported as lost or stolen, or checking the contents of a document (such as certificate of incorporation) against a publicly available record. If a relevant business is not convinced that the document is genuine it should not be accepted, and the business should consider whether this suspicion might in turn give rise to a suspicion of ML/TF.

4.26	An increasing amount of data on individuals is held electronically/digitally, in various forms, and by various organisations and a relevant business may choose to use electronic/digital means to establish evidence of identity where this is possible, either on their own or in conjunction with documentary evidence. Sources of electronic information about individuals can vary in integrity and in reliability and independence in terms of their technology and content, therefore a relevant business should be satisfied that any source from which such information is obtained is secure from fraud and misuse and capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact that person. A relevant business should document the steps taken in this regard.
4.27	For documents in a language other than English, a relevant business should take appropriate steps to satisfy itself that the documents in fact provide verification of the customer's identity (e.g., by ensuring that staff assessing such documents are proficient in the language or by obtaining a translation from a suitably qualified person).
4.28	Where appropriate, a relevant business should consider obtaining copies of documents that have been certified by a suitable professional who has seen the original documentation. Use of an independent certifier helps guard against the risk that the documentation provided does not correspond to the customer whose identity is being verified. However, a relevant business should exercise caution when accepting certified copy documents, where such documents originate from a country perceived to represent a higher ML/TF risk. If a relevant business is unsure of the authenticity of certified documents, or that the documents relate to the customer in question, the business should take additional measures to mitigate the ML/TF risk.
4.29	Suitable persons for certifying verification of identity documents may include a member of the judiciary, an officer of an embassy, consulate or high commission of the country or territory of issue of documentary verification of identity, a Justice of the Peace, or a professional person such as a lawyer, notary public, certified public accountant or professional company secretary. The certifier should sign and date the copy document (printing their name clearly in capitals underneath) and indicating their position or capacity on it. The certifier should state that it is a true copy of the original (or words to similar effect).
CONNECTED PARTIES	
4.30	In respect of a customer that is a company, body corporate, partnership, association, trust or other similar legal arrangement, a relevant business should identify all the connected parties of that customer by obtaining their names.
4.31	A person is a connected party of a customer if they are: (a) a director of a company that is a customer; (b) a partner of a partnership that is a customer; (c) a trustee (or equivalent) of a trust or similar legal arrangement that is a customer; and (d) an individual at a senior management level of any other body that is a customer.
4.32	If a connected party is also in its own right a customer, a beneficial owner of the customer or a person purporting to act on behalf of the customer, a relevant business should identify and verify (or take reasonable steps to verify, as appropriate) the identity of that person in that capacity (and not as a connected party) following the requirements elsewhere in this section.

HOW TO CARRY OUT IDENTIFICATION AND VERIFICATION OF IDENTITY – BENEFICIAL OWNERS	
4.33	A beneficial owner of a customer is an individual who ultimately owns or controls the customer or on whose behalf a transaction is being undertaken by a relevant business. A relevant business should identify any beneficial owner in relation to a customer, and it should take reasonable measures to verify the beneficial owner's identity. It should be emphasised that the requirement in relation to verification of the identity of the beneficial is that of taking "reasonable measures", and it is therefore not the same standard that applies in relation to verification of the identity of a customer.
4.34	When identifying a beneficial owner, a relevant business should endeavour to obtain the same identification information as set out in 4.11 as far as practicable.
4.35	In determining what constitutes reasonable measures to verify the identity of a beneficial owner of a customer, a relevant business should have regard to the ML/TF risks posed by the customer and the business relationship or occasional transaction. Reasonable measures are therefore measures that are commensurate with the ML/TF risks. It is therefore for a relevant business to decide whether it is appropriate to, for example, (a) make use of the records about a beneficial owner that are available publicly; or (b) request its customer to provide documents or information in relation to the beneficial owner's identity that is obtained from a reliable and independent source .
4.36	If the ownership structure of a customer involves different types of legal persons or legal arrangements, in determining the identity of the beneficial owner, a relevant business should seek to identify the individual who has ultimate ownership or control over the customer.
FOR INDIVIDUALS	
4.37	In respect of a customer who is an individual, that individual is normally the beneficial owner. A relevant business is not expected to take steps to identify any other person who might be a beneficial owner, unless there is a suspicion that the customer is not acting on their own behalf.
FOR COMPANIES, OTHER BODIES CORPORATE, PARTNERSHIPS AND ASSOCIATIONS	
4.38	In respect of a customer that is a company or other body corporate, the beneficial owner is: (a) any individual who: (i) directly or indirectly, including through a trust or bearer share holdings, owns or controls more than 25% of the issued share capital of the company; (ii) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights at a general meeting of the company; or (iii) exercises ultimate control over the management of the company; or (b) if the company is acting on behalf of another person, that other person.
4.39	4.38 does not apply to a company listed on a stock exchange and subject to disclosure requirements which impose requirements to ensure adequate transparency of beneficial ownership, and a relevant business is not under any obligation to take measures to identify the beneficial owners of such a company.

4.40	In respect of a customer that is a company or other body corporate, a relevant business should identify any individual who ultimately has a controlling ownership interest (i.e., more than 25%) in the customer and any individual exercising control of the customer or its management, and it should take reasonable measures to verify their identities. If a relevant business is unable to identify an individual who is the beneficial owner, or it it is not satisfied that the individual identified is the beneficial owner, the relevant business may treat the senior person in the organisation responsible for managing it as its beneficial owner. The relevant business should take reasonable measures to verify the identity of the senior person in the organisation responsible for managing it, and record all actions in doing so, as well as difficulties encountered, where applicable.
4.41	For some corporate customers, such as supranational organisations, wholly state-owned entities, certain multilateral financial institutions, government agencies and sovereign wealth funds, there may be no reasonable expectation of them having a beneficial owner. In such a case a relevant business does not need to verify the identity of the senior person but should still document the steps taken and record the reasons for their conclusions.
4.42	In respect of a customer that is a partnership, the beneficial owner is: (a) any individual who: (i) is entitled to or controls, directly or indirectly, more than a 25% share of the capital or profits of the partnership; (ii) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights in the partnership; or (iii) exercises ultimate control over the management of the partnership; or (b) if the partnership is acting on behalf of another person, that other person.
4.43	In respect of a customer that is any other type of unincorporated body, the beneficial owner is: (a) an individual who ultimately owns or controls the unincorporated body; or (b) if the unincorporated body is acting on behalf of another person, that other person.
FOR TRUSTS AND SIMILAR LEGAL ARRANGEMENTS	
4.44	In respect of a customer that is a trust, the beneficial owner is: (a) a beneficiary (or a class of beneficiaries, where the identity of some beneficiaries has not yet been determined) of the trust; (b) the settlor of the trust; (c) any protector or enforcer of the trust; (d) the trustee of the trust; or (e) an individual with ultimate control over the trust.
4.45	In respect of a customer that is a trust, a relevant business should identify the settlor, the trustee, the protector, the enforcer, the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate control over the trust (including through a chain of control or ownership), and it should take reasonable measures to verify their identities. For a customer that is a legal arrangement similar to a trust, a relevant business should identify any individual in equivalent or similar positions to a beneficial owner of a trust as stated above and take reasonable measures to verify their identities.

4.46	For an individual to have control over a trust means that they have a power (exercisable by that individual on their own or jointly with another), under the trust instrument or by law to: (a) dispose of trust property in some way (including by investing it, or advancing, lending or paying it); (b) vary or terminate the trust; (c) add or remove a person as a beneficiary (or to add or remove them from a class of beneficiaries); (d) appoint or remove trustees or give another individual control over the trust; or (e) direct, withhold consent to or veto the exercise of one of the above powers.
4.47	Where beneficiaries of a trust are yet to be determined, a relevant business should focus on verification of the identity of the settlor. However, a relevant business should obtain sufficient information concerning the class of beneficiaries of a trust to ensure that it will be able to establish the identity of a beneficiary at the time of distribution.
OWNERSHIP AND CONTROL	
4.48	In respect of a customer that is not an individual, a relevant business should ensure that it understands the customer's ownership and control structure, including identifying any intermediate layers. The aim is to follow the chain of ownerships to the beneficial owners of the customer. In respect of a customer that has a complex ownership or control structure, a relevant business should obtain enough information to enable it to be confident that there is a legitimate reason behind that structure.
NOMINEES	
4.49	In respect of a customer which has nominee shareholders in its ownership structure, a relevant business should obtain satisfactory evidence of the identities of the nominees, and the persons on whose behalf they are acting, as well as the details of arrangements in place, in order to determine the identity of the beneficial owner.
BEARER SHARES	
4.50	Where a company issues bearer shares, the ownership interest represented by those shares belongs to the person who possesses the physical bearer share certificate. Given the challenges associated with establishing the true beneficial ownership of a company with bearer shares, a relevant business should not establish a business relationship with or carry out an occasional transaction for a customer whose supposed beneficial ownership is evidenced by bearer shares.
HOW TO CARRY OUT IDENTIFICATION AND VERIFICATION OF IDENTITY IN RELATION TO A PPTA	
4.51	Where an individual, company, other body corporate or partnership purports to act on behalf of a customer (a "PPTA"), e.g., as an attorney or agent, a relevant business should identify that person and take reasonable measures to verify that person's identity. A relevant business should also verify the person's authority to act on behalf of the customer. A relevant business should identify and verify the identity of the PPTA in line with the identification and verification requirements for a customer that is an individual, company, other body corporate, or partnership as relevant. A relevant business should obtain evidence (e.g., a board resolution or power of attorney) to verify that the person purporting to act on behalf of the customer is authorised to do so.

4.52	A relevant business should establish a written policy to govern its interaction with a PPTA and the CDD measures that it will apply.

UNDERSTANDING THE PURPOSE AND INTENDED NATURE OF THE BUSINESS RELATIONSHIP OR OCCASIONAL TRANSACTION

4.53	A relevant business should understand the purpose and intended nature of the business relationship or occasional transaction. In some instances, this will be obvious, but in others the relevant business will need to obtain explanatory information from the customer.

TIMING OF VERIFICATION

4.54	Exceptionally, the identity of the customer and any beneficial owner may be verified after establishing the business relationship. A relevant business is not under any obligation to do so and may instead as a matter of policy require that, in every case, identity verification must be completed before the business relationship begins. A relevant business may permit verification of identity after the start of the business relationship only if: (a) any risk of ML/TF arising from the delayed verification of the customer's or beneficial owner's identity can be effectively managed; (b) it is necessary not to interrupt the normal conduct of business with the customer; (c) the verification is completed as soon as reasonably practicable; and (d) the business relationship will be terminated if verification cannot be completed, as soon as reasonably practicable.
4.55	This exception should not be applied where: (a) a relevant business has knowledge or a suspicion of ML/TF; (b) a relevant business becomes aware of anything which causes it to doubt the identity or intentions of the customer or beneficial owner; or (c) the business relationship is assessed to pose a higher risk.
4.56	Subject to 4.57, where a business relationship is entered into prior to identity verification, a relevant business should ensure that the AML/CFT Controls include: (a) establishing a reasonable timeframe for the completion of the identity verification measures and any further actions; (b) monitoring of transactions pending completion of the identity verification, and keeping senior management informed of any pending verification cases; (c) limiting the number of transactions and type of transactions that can be undertaken pending verification; and (d) ensuring that funds are not paid out to any third party.

4.57	The verification of the identity of a bank account holder may take place after the bank account has been opened provided that there are adequate controls in place to ensure that, before verification has been completed: (a) the account is not closed; and (b) transactions are not carried out by or on behalf of the account holder, including any payment from the account back to the account holder.
4.58	A relevant business should ensure that it adheres to the maximum permitted timeframes as follows (a business may choose to adopt shorter timeframes): (a) verification should be completed no later than 30 working days after the establishment of the business relationship; (b) if verification is not completed within 30 working days, a relevant business should suspend the business relationship with the customer and should not carry out further transactions; and (c) if verification remains incomplete 60 working days after the start of the business relationship, a relevant business should terminate the relationship with the customer.
4.59	Where verification cannot be completed within a reasonable time the relevant business should terminate the business relationship. A relevant business should consider whether this provides grounds for knowledge or suspicion of ML/TF, especially where the customer requests that money or other assets be transferred to third parties or back to the customer prior to identity verification, and a whether a suspicious activity report should be made.
SIMPLIFIED DUE DILIGENCE (SDD)	
4.60	A relevant business may apply SDD measures in relation to a business relationship or occasional transaction if it determines, having regard to its risk assessment, that the business relationship or transaction poses a low level of ML/TF risk. A relevant business must properly document its reasons for concluding that there is a low level of ML/TF risk and should be prepared to justify its conclusion to the FSRA.
4.61	SDD measures are the lowest permissible form of CDD and must not be applied, or continue to be applied, when a relevant business suspects ML or TF, when there are doubts about the veracity or adequacy of any information previously obtained from the customer for identification or verification purposes, or when a relevant business has any other reason to believe that the ML/TF risk is no longer low. In addition, a relevant business should not apply SDD measures to a PPTA or the beneficial owner of a PPTA. If a relevant business chooses to use SDD measures, it must still carry out ongoing monitoring of the business relationship in accordance with Section 5.
4.62	In this Section, where the provisions of this Directive refer to an "equivalent jurisdiction" that means a jurisdiction that is a member of the Financial Action Task Force (FATF) or which imposes AML/CFT requirements that are consistent with the standards published by the FATF.

4.63	Factors which potentially lower the level of ML/TF risk, include: (a) the type of customer, for example where it is: (i) a governmental or regulatory body, or a state-owned enterprise in St Helena, the United Kingdom or an equivalent jurisdiction; (ii) a financial institution in St Helena, the United Kingdom or an equivalent jurisdiction and is subject to and supervised for compliance with AML/CFT requirements consistent with standards published by the FATF; (iii) a company listed on a stock exchange and subject to disclosure requirements which impose requirements to ensure adequate transparency of beneficial ownership; or (iv) a pension scheme or collective investment scheme, approved by the FSRA for offering to the public in St Helena; (b) the nature of the transaction, product or service, for example where it is a pension, superannuation or similar scheme which provides retirement benefits to employees, where contributions are made by an employer or by way of deduction from an employee's pay and the scheme rules do not allow the transfer of a member's interest under the scheme; or (c) the country or jurisdiction in which the customer is established or does business, for example where it is: (i) a country or jurisdiction considered as having AML/CFT controls that are consistent with standards published by the FATF; or (ii) a country or jurisdiction with documented low levels of corruption or other criminal activity.
4.64	By way of possible SDD measures, a relevant business might consider: (a) adjusting the intensity, frequency and type of ongoing monitoring of a business relationship; (b) applying simplified due diligence in relation to the beneficial owners of the customer; or (c) reducing the frequency of updates of customer identification information.
SIMPLIFIED DUE DILIGENCE IN RELATION TO BENEFICIAL OWNERS	
4.65	Subject to 4.66, a relevant business may choose not to identify and take reasonable measures to verify the beneficial owner in relation to a customer that is: (a) a relevant business; (b) a bank, custodian, financial intermediary, insurer, investment manager, or trustee corporation that is: (i) incorporated or established in the United Kingdom or an equivalent jurisdiction; (ii) has measures in place to ensure compliance with AML/CFT requirements that are consistent with standards published by the FATF; and (iii) is supervised for compliance with those requirements by a statutory regulator; (c) a corporation listed on a stock exchange and which is subject to disclosure requirements (either by stock exchange rules, or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership of the customer;

	(d) an investment vehicle (including a pension fund) where the person responsible for carrying out measures that are similar to the CDD measures in this Directive in relation to all the investors of the investment vehicle is: (i) a relevant business; or (ii) a firm falling into paragraph (b); (e) the government of St Helena or any public body in St Helena; or (f) the government of or a public body in, the United Kingdom or an equivalent jurisdiction.
4.66	A relevant business which is licensed by the FSRA to carry on banking business may not apply SDD where it has or proposes to have a banking or similar relationship with an overseas financial institution.
4.67	Where a customer is an investment vehicle, a relevant business may choose not to identify and take reasonable measures to verify its beneficial owners (i.e., the investors), provided that the relevant business is able to ascertain that the person responsible for carrying out measures that are similar to the CDD measures in relation to all the investors of the investment vehicle falls within any of the categories of firms in paragraph (a) or (b) of 4.65. An investment vehicle includes a pension fund in which pension fund members are invested.
4.68	A relevant business may choose not to identify and take reasonable measures to verify the beneficial owners in relation to a customer if it reasonably believes that the customer's transaction relates to a pension, superannuation or similar scheme which provides retirement benefits to employees, where contributions are made by an employer or by way of deduction from an employee's pay and the scheme rules do not allow the transfer of a member's interest under the scheme.
ENHANCED DUE DILIGENCE (EDD)	
OVERVIEW	
4.69	A relevant business should apply EDD measures in any situation which by its nature may present a higher ML/TF risk. A relevant business should ensure that the EDD measures that it applies in each case are proportionate to the ML/TF risk, and it should be prepared to justify to the FSRA the basis for those EDD measures.
4.70	For the purpose of 4.69, a relevant business should treat the following as examples of a situation which may present a higher ML/TF risk and should therefore apply EDD measures to any business relationship or occasional transaction arising in that situation: (a) where a relevant business has or proposes to establish a business relationship with or carry out an occasional transaction for an Overseas PEP; (b) where a relevant business has or proposes to have a business relationship with a customer or carry out an occasional transaction for that customer and a beneficial owner or PPTA of that customer is an Overseas PEP; (c) where a customer has not been physically present for identification purposes; or (d) where a relevant business which is licensed by the FSRA to carry on banking business has or proposes to have a banking or similar relationship with an overseas financial institution.
4.71	The senior management of a relevant business should approve every business relationship that has been assessed as posing a higher ML/TF risk.

4.72	The following is a non-exhaustive list of higher-risk factors that a relevant business should take account of, while bearing in mind that the presence of one or more risk factors may not always indicate that there is a higher ML/TF risk in a particular situation: (a) the type of customer and whether it is: (i) a trust or similar legal arrangement that is used for holding assets beneficially owned by other persons; (ii) a company that has nominee shareholders, nominee directors or shares in bearer form; (iii) one whose corporate structure is unusual or excessively complex given the supposed nature of the business; (iv) one in relation to which a relevant business is not able to establish whether it has any ongoing, apparent or visible operation or business activity; (v) a third country national who is applying for residence rights or citizenship in exchange for transfers of capital, purchase of a property, government bonds or investment in corporate entities in a country or jurisdiction; (vi) a cash intensive business, e.g., bureaux de change, money transfer agents, casinos, betting and other gambling related activities; or (vii) is engaged in or facilitates business practices intended, whether in St Helena or elsewhere, to facilitate tax evasion, or the concealment of assets from government authorities or creditors, or otherwise to impede the tracing of assets for lawful purposes; (b) the nature of the product, service transaction and whether: (i) it involves private banking, trusts or cryptocurrency; (ii) the product or transaction is one which might favour anonymity; (iii) frequent payments are received from apparently unrelated third parties; (iv) the service involves the provision of nominee directors, nominee shareholders or shadow directors; or (v) there is a transaction related to armaments, precious metals, cultural artefacts, ivory or other items related to protected species, or other items of archaeological, historical, cultural or religious significance or of rare scientific value; and (c) the country or jurisdiction in which the customer is established or does business and whether: (i) the customer is not located in St Helena and the customer's reasons for wishing to establish a business relationship with a relevant business in St Helena are unexplained, unclear or dubious; (ii) it is a country or jurisdiction considered by credible sources as having significant levels of corruption or other criminal activity, such as terrorism, money laundering, and the production and supply of illicit drugs; (iii) it is a country or jurisdiction subject to sanctions, embargoes or similar measures issued by St Helena, the United Kingdom or the United Nations; (iv) it is a country or jurisdiction that provides funding or support for terrorism; (v) it is a country or jurisdiction that has an organisation within its territory which has been designated by St Helena or the United Kingdom as a proscribed organisation or a terrorist organisation; or (vi) it is a country or jurisdiction identified by credible sources as not implementing measures to counter ML/TF that are consistent with the standards published by the FATF, or one in relation to which the FATF has called for countermeasures.

POLITICALLY EXPOSED PERSONS (PEPS)	
4.73	A relevant business should have in place AML/CFT Controls to enable it to determine whether a customer, its beneficial owner or PPTA is a PEP. This Directive distinguishes between a St Helena PEP and an Overseas PEP, and whether a relevant business applies, and the extent to which it applies, EDD measures depends on the category into which a PEP customer falls. Unless a specific ML/TF high-risk indicator is present, a relevant business need not apply EDD measures in relation to a business relationship with or occasional transaction for a St Helena PEP or for a customer whose beneficial owner or PPTA is a St Helena PEP.
4.74	The provisions of this Directive dealing with EDD measures and enhanced ongoing monitoring for PEPs apply only where a relevant business is entering into a business relationship with or undertaking an occasional transaction for a customer that is PEP (or with or for a customer whose beneficial owner or PPTA is a PEP). Therefore, a relevant business should not apply EDD measures to an individual simply because they are an employee or senior executive of a government-owned company, statutory body or other public body with which a relevant business has or proposes to have a business relationship or carry out an occasional transaction.
ST HELENA PEPS	
4.75	A St Helena PEP is: (a) an individual who is, or has previously been, entrusted with a prominent public function in St Helena and: (i) includes a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and an important political party official (ii) does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph (i); (b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or (c) a close associate of an individual falling within paragraph (a).
4.76	A close associate of a PEP is an individual who has close business relations with a PEP and includes: (a) an individual who is known to have joint beneficial ownership of a legal entity, trust or similar legal arrangement, or any other close business relations, with a PEP; and (b) an individual who has sole beneficial ownership of a legal entity, trust or similar legal arrangement which is known to have been set up for the benefit of a PEP.
4.77	For the purpose of deciding whether a person is a close associate of a PEP, a relevant business need only have regard to information which is in its possession, or to credible information which is publicly available. This means that it is only expected to be able to identify a close associate where the information it already holds, or is publicly available, indicates that this is what they are. This includes relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations.

4.78	A relevant business should apply the measures set out in 4.82 and 4.83 in any of the following situations: (a) before establishing a high-risk business relationship with a customer who is or whose beneficial owner or PPTA is a St Helena PEP; (b) when continuing an existing business relationship with a customer who is or whose beneficial owner or PPTA is a St Helena PEP where the relationship subsequently becomes high-risk; or (c) when continuing an existing high-risk business relationship where a relevant business subsequently becomes aware that the customer or the beneficial owner or PPTA of the customer is a St Helena PEP.
4.79	Accordingly, a relevant business need only apply EDD measures to a St Helena PEP when the business relationship or occasional transaction presents a high-risk of ML/TF. A relevant business should not apply EDD measures to a St Helena PEP simply because that person falls into one of the paragraphs in 4.75, but it need instead only apply EDD measures where there is a specific high risk associated with the business relationship. As noted above, a business relationship between a St Helena PEP and a relevant business does not in any event arise by reason of that PEP's position as a senior executive of a government-owned company, statutory body or public body.
OVERSEAS PEPS	
4.80	An Overseas PEP is: (a) an individual who is, or has been, entrusted with a prominent public function in a place outside St Helena and: (i) includes a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and an important political party official; (ii) but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph (i); (b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or (c) a close associate (bearing the same meaning as in 4.76) of an individual falling within (a).
4.81	A relevant business should establish and maintain effective arrangements for determining whether a customer or a beneficial owner of a customer is an Overseas PEP. It should do so by referring to public domain information such as websites of parliaments and governments, reliable news sources and work by reputable pressure groups focused on corruption risk such as Transparency International, and/or commercially available databases that list PEPs, family members and known close associates. Where a relevant business is anything other than a very small business, the FSRA will expect that business to make use of commercially available databases as part of its screening. In any case, the FSRA expects that every relevant business will put in place a systematic and rigorous screening procedure for the identification of Overseas PEPs.

4.82	Where a relevant business establishes that a customer or a beneficial owner or PPTA of a customer is an Overseas PEP, it should, before (i) establishing a business relationship or (ii) continuing an existing business relationship, or (iii) carrying out an occasional transaction, with or for that customer apply EDD measures, namely: (a) it should ensure that senior management of the relevant business approve the establishment or continuation of the business relationship or the carrying out of the transaction; and (b) it should take reasonable measures to establish the customer's or the beneficial owner's or the PPTA's source of wealth and the source of the funds.
4.83	In addition to the EDD measures in 4.82, a relevant business should also conduct enhanced ongoing monitoring of the business relationship.
OTHER CONSIDERATIONS – ALL PEPS	
4.84	In relation to both a St Helena PEP and an Overseas PEP, a relevant business should adopt and implement a policy to govern the treatment of former PEPs and the circumstances in which it will cease to apply the EDD measures and enhanced ongoing monitoring set out in 4.82 and 4.83. A relevant business should conduct a customer risk assessment after the customer (or its beneficial owner or PPTA) ceases to occupy their public position to determine whether they continue to pose a higher risk of ML/TF. A relevant business should not cease to apply EDD measures and enhanced ongoing monitoring automatically once a specified period has elapsed since a PEP stepped down, but it should instead take a risk-based decision on a case-by-case basis. It should in particular consider the level of influence that the PEP is likely to continue to exercise after they have stepped down.
4.85	PEPs do not all present the same level of ML/TF risks, and a relevant business should therefore take a risk-based approach to determining the extent of EDD measures in paragraph 4.82 and enhanced ongoing monitoring in paragraph 4.83. In making that determination, a relevant business should consider such matters as: (a) the nature of the functions that a PEP holds; (b) the geographical risk associated with the jurisdiction where a PEP holds those functions; (c) whether the person currently holds those functions or did so formerly; and (d) the nature of the business relationship, such as the product or service offered (e.g., transactions or structures which may help obscure the ownership or transfer of assets).
4.86	Source of wealth refers to the origin of an individual's total assets. This information will usually give an indication as to the size of wealth the customer would be expected to have, and a picture of how the individual acquired such wealth. Although a relevant business may not have specific information about assets that are not deposited with, or handled by it, it may be possible to gather information from the individual, commercial databases or other open sources. This information can be expected to give an indication as to what amount of wealth the customer would be reasonably expected to have as well as a picture of how the person acquired such wealth. A relevant business will need to be satisfied that they understand where the customer's overall wealth has come from and also, so far as it can be ascertained, that it comes from a legitimate origin.

4.87	Source of funds refers to the origin of the money or other assets which are the subject of the business relationship between an individual and the relevant business (e.g., the amounts being deposited or transferred as part of the business relationship). Source of funds information should not be limited to knowing from which source the funds have been transferred, but also the activity that generates the funds. Examples of documents, data and information that a relevant business may find useful for the verification of the source of funds include payslips, bank statements, audited financial accounts, sales/purchase agreements, or income from share capital, business activities, a bequest or a gift.
4.88	A relevant business should determine the measures that it considers appropriate, in accordance with its assessment of the risks, to establish the source of funds and source of wealth. In practical terms, this will often amount to obtaining information from the PEP and verifying it against publicly available information sources.
4.89	Where a relevant business cannot successfully establish the customer's source of wealth in higher risk situations, the relevant business should consider ceasing to act for the customer and whether it needs to submit a suspicious activity report.
CUSTOMER NOT PHYSICALLY PRESENT FOR IDENTIFICATION PURPOSES	
4.90	A relevant business can establish a business relationship either on a face-to-face basis, or a non-face-to-face basis (e.g., through the internet). However, where a relevant business chooses to accept customers on a non-face-to-face basis, it should apply EDD measures to mitigate the associated risks (e.g., impersonation risk). Where a customer was not physically present for identification purposes at account opening stage, a relevant business should take at least one of the following further steps to mitigate the risks: (a) further verifying a customer's identity using documents, data or information referred to in 4.12 but not previously used for the purposes of verification of the customer's identity under that provision; (b) taking supplementary measures to verify information relating to the customer; or (c) ensuring that the payment or, if there is more than one payment, the first payment made in relation to the customer's account is carried out through an account in the customer's name with a bank licensed by the FSRA or an overseas bank which is: (i) incorporated or established in the United Kingdom or an equivalent jurisdiction; (ii) has measures in place to ensure compliance with AML/CFT requirements that are consistent with standards published by the FATF; and (iii) is supervised for compliance with those requirements by a statutory regulator.
4.91	A relevant business should ensure that the additional measures taken under 4.90 are commensurate with the ML/TF risks posed by the customer. Examples of practical steps that a relevant business could take as part of those additional include (i) use of an appropriate person to certify identification documents; (ii) checking relevant data against reliable databases or registers; or (iii) using technological resources. The FSRA will expect a relevant business to be able to demonstrate that the measures taken effectively mitigate the risk of impersonation.

4.92	A relevant business should also be alive to the risks of fraud or deception in relation to a company, body corporate, partnership, trust or similar legal arrangement that seeks to establish a business relationship through a non-face-to-face channel. This might happen when the individuals acting on behalf of the customer to establish the business relationship are not physically present for identification purposes. In such a case, a relevant business should apply additional due diligence measures both to those individuals and to documents provided that purport to identify the company, body corporate, partnership, trust or similar legal arrangement.

RELIANCE ON CDD MEASURES CARRIED OUT BY AN INTERMEDIARY

4.93	Subject to compliance with the terms of this Directive, a relevant business may rely upon CDD measures carried out by an intermediary in relation to a customer, beneficial owner, PPTA or connected party. This arrangement may have benefits of speed and convenience for a relevant business. However, a relevant business remains responsible for ensuring the effective application of those CDD measures and liable for any failure of the intermediary to properly apply them. The senior management of a relevant business remain fully accountable to the FSRA for compliance requirements concerning CDD measures in this Directive, notwithstanding that it may have chosen to rely on an intermediary's CDD measures. The potential to rely on CDD measures may arise where an intermediary has an existing relationship with the customer of the relevant business and has accepted that customer through its own CDD procedures. Reliance on an intermediary's CDD measures is not the same as the case where a relevant business outsources implementation of the relevant business's CDD measures to an outsourced service provider or other agent.
4.94	For the avoidance of doubt, a relevant business: (a) may not rely on an intermediary to conduct ongoing monitoring of a business relationship, including financial sanctions screening or other financial sanctions compliance controls; and (b) may not "pass on" the results of CDD measures carried out for it by an intermediary to another relevant business.
4.95	If a relevant business chooses to rely on an intermediary, it should: (a) put in place a written agreement between it and the intermediary to document the intermediary's consent to being relied upon; and (b) be confident that the intermediary will on request provide promptly to the relevant business a copy of any document, data or information obtained by the intermediary in the course of carrying out the CDD measures, including where the relevant business makes that request on behalf of the FSRA.
4.96	A relevant business that relies on an intermediary to carry out CDD measures should obtain from that intermediary the information that it has obtained in the course of carrying out that CDD measure and should do so immediately after completion of that CDD measure. It is for a relevant business to decide whether it obtains at the same time copies of the data and documents collected and records made by the intermediary while carrying out the CDD measure. If the data, documents and records are retained by the intermediary, a relevant business should ensure that it obtains an undertaking from the intermediary to retain all underlying CDD information throughout the lifetime of the business relationship between the relevant business and its customer, and for at least five years beginning on the date on which the business relationship terminates. A relevant business should ensure that the intermediary will, at any point in that

	period, provide promptly to the relevant business, or to the relevant business for onward provision to the FSRA, a copy of any data or document obtained by that intermediary in the conduct of the CDD measures. In the case that the relationship of reliance between a relevant business and an intermediary ceases, the relevant business should obtain without delay all CDD data, documents and records collected by the intermediary in relation to the customers (and their beneficial owners, PPTAs and connected parties) of the relevant business.
4.97	Subject to compliance with the requirements in this Directive, a relevant business may in principle rely on an intermediary where that intermediary is: (a) a relevant business that is a bank in St Helena; (b) an overseas bank, custodian, financial institution, insurer, investment manager, or trustee corporation; (c) an overseas lawyer or notary public; or (d) an overseas auditor or professional accountant.
4.98	A relevant business may only rely on the CDD measures carried out by an intermediary where that intermediary: (a) is required to be, and is, licensed and regulated; (b) is subject to law or regulation in its home jurisdiction that imposes AML/CFT standards that are consistent with the standards published by the FATF; (c) is effectively supervised for compliance with those standards by a regulatory body; and (d) has measures in place to give effect to those standards in its business.
4.99	A relevant business should ensure that it properly checks that an intermediary meets the conditions in 4.98, including by: (a) obtaining and reviewing the intermediary's AML/CFT policies; (b) confirming its licensed and regulated status by inspecting the relevant public registers; (c) ascertaining whether the intermediary has been subject to regulatory enforcement action in relation to AML, CFT or financial sanctions compliance matters; and (d) obtaining where available a copy of any independent audit of the third party's AML/CFT systems and controls.
APPLICATION TO EXISTING CUSTOMERS	
4.100	Subject to 4.101, a relevant business should carry out the relevant CDD measures in relation to existing customers based on its own assessment of materiality and risk, taking into account any previous measures applied, the time when the measures were last applied to such existing customers and the adequacy of data, documents or information obtained.

4.101	A relevant business should always apply the CDD measures in this Directive to existing customers: (a) if ever the relevant business suspects that the customer is involved in ML/TF, regardless of the monetary levels of transactions; (b) if ever the relevant business has reason to question the adequacy or veracity of any documents, data or information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity; (c) if it becomes aware that any circumstances of a customer that are material to its risk assessment for that customer have changed; (d) a transaction occurs with regard to the customer, which is, unusual or suspicious or is not consistent with the relevant business's knowledge of the source of the customer's funds; or (e) on the occurrence of any other trigger event.
4.102	Trigger events should include at least: (a) a change in the identity of the customer or beneficial owner; (b) a change in the ML/TF risk rating of the customer; (c) a customer seeking to restart a dormant account; and (d) a change in the purpose or nature of the business relationship.
4.103	A relevant business should ensure that it adopts a policy in relation to trigger events that is appropriate to its own business.
4.104	A relevant business should ensure that as far as reasonably practical it performs the CDD measures required by this Directive, to the extent that they have not already been performed, on a customer that wishes to close their account before the relevant business releases funds to that customer.
4.105	For the avoidance of doubt, the requirements of this Directive in relation to ongoing monitoring and screening apply to all existing customers from the effective date of the Directive.

Section 5 – ONGOING MONITORING

5.1	Ongoing monitoring is essential for effective AML/CFT Controls. A relevant business should therefore continuously monitor its business relationship with a customer.
5.2	In relation to the ongoing monitoring of a business relationship, a relevant business should put in place and implement adequate AML/CFT Controls, commensurate with its nature, size and complexity to: (a) detect and report suspicious, complex, unusually large or unusual patterns of transactions; (b) screen in accordance with Section 6; and (c) ensure that the information that it holds for the purpose of complying with Section 4 remains relevant and up to date.

5.3	A relevant business should put in place a written procedure for the ongoing monitoring of its business relationships. Monitoring arrangements should be risk-based, driven by the nature, size and complexity of the relevant business's activities. For effective monitoring, resources should be targeted towards business relationships presenting a higher risk of ML/TF.
5.4	Where a relevant business is unable to conduct ongoing monitoring in relation to a business relationship, it should terminate that business relationship, and it should assess whether as a result there are grounds for knowledge or suspicion of ML/TF.
5.5	A relevant business should consider whether it has the technical skills and systems that are needed for the effective ongoing monitoring of a higher-risk business relationship. If a relevant business does not have a good faith belief that it can effectively monitor the risks of such a business relationship, it should not establish that relationship and should terminate any such existing relationship.
5.6	A monitoring system may be manual or automated (such as the production of a range of standard exception reports) or it may be a combination of the two. Some electronic tools may be used which enable automated monitoring of client/transaction features as set against quantitative limits or parameters or other risk indicators.
5.7	A relevant business should ensure that it keeps the results of its ongoing monitoring for at least 5 years after the end of a business relationship.
TRANSACTION MONITORING	
5.8	A relevant business should, during the lifetime of a business relationship with a customer, observe the activity of the customer's account and scrutinise transactions undertaken, to ensure that the transactions are consistent with the business's knowledge of the customer, its business and risk profile and, as appropriate, the source of funds and wealth.
5.9	A relevant business should ensure that it: (a) carries out appropriate scrutiny of transactions carried out for the customer to ensure that they are consistent with the business's knowledge of the customer, the customer's business, risk profile and source of funds and wealth; and (b) puts in place arrangements to identify transactions that (i) are complex, unusually large in amount or of an unusual pattern; or (ii) have no apparent economic or lawful purpose.
5.10	For the purpose of establishing appropriate transaction monitoring arrangements, a relevant business should ensure that it takes account of: (a) the nature and type of transactions (e.g., abnormal size or frequency); (b) the nature of a series of transactions; (c) the identity of the recipient or beneficiary of a transaction, not just the identity of the customer; (d) the jurisdiction of origin and destination of a payment or receipt; and (e) a customer's normal account activity.

5.11	A relevant business should take appropriate steps (e.g., examining the purpose of the transaction or obtaining additional CDD information) when: (a) the customer's transactions are not consistent with a relevant business's knowledge of the customer, the customer's business, risk profile or source of funds or wealth; or (b) the relevant business identifies a transaction that does not have any apparent economic or lawful purpose or is complex or unusually large.
5.12	For potentially unusual transactions, such examination may include asking the customer appropriate questions. This should not constitute tipping-off if conducted properly and in good faith. However, if in the particular circumstances a relevant business reasonably concludes that questioning will tip-off the customer, it may cease its enquiries and file an SAR which includes its assessment of the tip-off risk.
5.13	A relevant business should ensure that it documents in writing the results of its transaction monitoring, the actions that it has taken in relation to any transaction identified as potentially suspicious and its conclusions in relation to that transaction. A relevant business should be able to provide any such documentation to the FSRA on request.
ONGOING CDD MONITORING	
5.14	A relevant business should ensure that the data, documents and information obtained when applying the CDD measures are kept up to date and continue to be relevant.
5.15	A relevant business should carry out a review of existing CDD records of each customer on a regular basis and/or upon the occurrence of a trigger event. A relevant business should ensure that it has in place policies and procedures to govern the frequency of such periodic reviews and the identification of trigger events. In relation to a customer that has been identified as posing a higher ML/TF risk, a relevant business should ensure that any such customer is subject to a review at least annually, or more frequently if deemed necessary by the relevant business.
OTHER CONSIDERATIONS	
5.16	As part of its ongoing monitoring, a relevant business should be alert to changes in the nature of the business relationship with a customer that might cause it to reassess the level of ML/TF risk posed by that customer and to adjust the CDD measures that it applies accordingly. Examples of such changes include a customer: (a) setting up new corporate or trust structures, especially where the commercial purpose is unclear; (b) frequent changes of directors where the customer is a corporate customer; (c) the customer buying new products or services that pose higher ML/TF risk; or (d) the customer entering new markets which may present a higher ML/TF risks.

Section 6 – FINANCIAL SANCTIONS

FINANCIAL SANCTIONS – OVERVIEW

6.1	The government of the United Kingdom has implemented a number of financial sanctions measures. Some of these measures derive from agreements in the United Nations while others have been determined by the UK acting autonomously. The UK gives effect to financial sanctions measures primarily through the Sanctions and Anti-Money Laundering Act 2018. It is the long-standing policy of the government of the UK that the same financial sanctions measures should be applied by the Overseas Territories, including St Helena. To that end, Orders in Council are made under the 2018 Act which extend those financial sanctions measures to St Helena and some other Overseas Territories.
6.2	A list of such Orders in Council is published by the St Helena Government on its website at **https://www.sainthelena.gov.sh/government/legislation/general-introduction/** (see under "UK sanctions regimes"). Detailed explanation as to the application and scope of the UK financial sanctions measures is published by the Office of Financial Sanctions Implementation: **https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation**.
6.3	A relevant business is required to comply with the financial sanctions measures that apply in St Helena in respect of its conduct in St Helena. A relevant business that is an individual who is St Helenian or another British citizen ordinarily resident in St Helena, or an entity that is incorporated or constituted in St Helena, must also comply with the financial sanctions measures in relation to their conduct overseas. A relevant business will be prohibited from carrying out certain activities or behaving in a certain way if financial sanctions measures apply. A breach of the financial sanctions measures will involve the commission of a criminal offence. For the avoidance of any doubt, while this Directive is addressed to each relevant business, the financial sanctions measures that apply in St Helena apply more broadly and not just to relevant businesses.
6.4	Authorities in other jurisdictions may impose unilateral financial sanctions measures and a relevant business with international operations will need to be aware of the financial sanctions measures in those jurisdictions. A relevant business should consider the implications and take appropriate measures where necessary, including seeking legal advice.
6.5	For example, where a relevant business processes financial transactions, especially those denominated in US dollars, through a US financial institution that pertain to commercial activity involving an OFAC-sanctioned country, region, or person, the relevant business may be engaging in a prohibited activity under the OFAC sanctions regime, which in turn would lead to very serious legal consequences for that relevant business.
6.6	An individual or entity that is made subject to financial sanctions measures by Order in Council is known as a "designated person". The details of those designations are publicised through a sanctions list maintained by the Office of Financial Sanctions Implementation. The St Helena Government website includes a link to the UK Government's Sanctions List which enables users to find information relating to all designated persons under the various UK sanctions regimes: (**https://www.gov.uk/government/publications/the-uk-sanctions-list**) A relevant business should ensure that its Compliance Officer and other relevant staff subscribe to the sanctions email alert service provided by the Office of Financial Sanctions Implementation. The FSRA will expect a relevant business to be able to provide evidence that all relevant staff have been subscribed to the service.

6.7	There are many types of financial sanctions measures (and also trade and geographic sanctions, which may have a financial services aspect) that apply in St Helena and a relevant business should ensure that it has a full understanding of all measures that are relevant to its business. The scope and application of these sanctions measures is complex and the consequences of non-compliance are very serious. Every relevant business should ensure that it takes regular professional advice on sanctions compliance matters to ensure that it has properly identified, interpreted and implemented all relevant sanctions measures. The contents of this Directive do not constitute legal advice.
6.8	Where an individual or entity is a designated person, it will be an offence for a relevant business: (a) to make available, directly or indirectly, any funds or other financial assets or economic resources to, or for the benefit of, (i) designated persons or entities; (ii) persons or entities acting on behalf or at the direction of the designated persons or entities mentioned in (i); or (iii) entities owned or controlled by any persons or entities mentioned in (i) or (ii); or (b) to deal with, directly or indirectly, any funds or other financial assets or economic resources belonging to, or owned or controlled by, such persons and entities falling within paragraph (a) above.
6.9	Typically, financial sanctions measures do not prohibit the use by a designated person of their own economic resources for everyday personal consumption e.g., using their car to do the shopping, but a designated person could not sell or use the resource to generate funds except with a licence.
6.10	A relevant business should note that the application of such designations extends to entities owned or controlled by any persons or entities which are designated persons or which act on behalf of designated persons. Entities owned or controlled, and indeed persons acting on behalf of designated persons, might not be designated persons in their own right. Therefore, it will not be sufficient for a relevant person to conduct sanctions due diligence only be reference to the names of designated persons that appear on the UK government's Sanctions List. A relevant business's due diligence processes should therefore be capable of identifying customers who make use of corporate vehicles to obscure ownership parties or source of funds. A relevant business should use the processes described in Section 4 for customers that are not individuals, to determine whether they are owned or controlled by a designated person, or their affairs are conducted in accordance with the instructions of a designated person.
6.11	An entity should be considered owned or controlled directly or indirectly by another person in any of the following circumstances: (a) the person holds (directly or indirectly) more than 50% of the shares or voting rights in an entity; (b) the person has the right (directly or indirectly) to appoint or remove a majority of the board of directors of the entity; or (c) it is reasonable to expect that the person would be able to ensure the affairs of the entity are conducted in accordance with the person's wishes.

6.12	In addition, the UK government also imposes trade and geographic sanctions which may also affect a relevant business. Trade sanctions may prohibit the provision of financial services related to specified goods and technology to any person connected with a specified country. Geographic sanctions are often wider and may prohibit the provision of financial services to any person in a specified country or to a class of person in a specified country or to a national of that country. While it is likely that some individuals or entities connected to a country that is specified in trade or geographic sanctions measures, will be designated persons, many more will not be so designated. Therefore, a relevant business will not be able to rely on the UK Sanctions List for the purpose of complying with trade or geographic sanctions measures and must instead undertake wider due diligence in relation to its customers, their transactions and their overall business activities.
6.13	The Governor of St Helena has the power (subject to the consent of the Foreign Secretary of the UK) to grant a "financial sanctions licence" to allow otherwise prohibited financial transactions to take place under certain circumstances. Such licences may be extended, varied or revoked. The Governor's power also extends to the issue of a "general licence" which authorises acts fitting within a particular description without the need to apply for an individual licence. Such acts include, for example, making funds available for the payment of normal living expenses. A relevant business may consult the UK's list of general licences published as guidance to the kind of act that might in principle be permitted under such a licence: **https://www.gov.uk/government/collections/ofsi-general-licences**.

FINANCIAL SANCTIONS - MEASURES TO BE TAKEN BY A RELEVANT BUSINESS

6.14	A relevant business should establish and maintain effective policies, procedures and controls to ensure compliance with the relevant regulations and legislation on financial sanctions measures.
6.15	It is the responsibility of the senior management of a relevant business to ensure that the business complies with the relevant regulations and legislation on financial sanctions measures. In discharging its responsibility, the senior management should ensure that they: (a) approve the policies, procedures and controls that are put in place to ensure the business's compliance with financial sanctions measures; (b) allocate adequate resource to sanctions compliance matters, including appointing a competent and knowledgeable individual to oversee the day-to-day operation of the policies, procedures and controls; (c) take steps to inform themselves as to the financial sanctions measures that apply to the relevant business; and (d) are made aware without delay of any proposed customer or existing customer being within, or being brought within, the scope of financial sanctions measures, and of any breach of such a measure.

6.16	A relevant business must carry out and document a sanctions risk assessment in relation to its exposure to the risks associated with a violation of financial sanctions measures. A relevant business should ensure that its sanctions risk assessment is comprehensive in scope and: (a) accurately identifies the sanctions measures which apply to that business; (b) accurately analyses the content of those measures; (c) takes account of all relevant sanctions risk indicators, including risks posed by customers, products, services, supply chain, intermediaries, counterparties, transactions, and geographic locations, depending on the nature of the business; (d) is updated promptly to take account of new sanctions measures and changes in the activities of a relevant business; (e) is reviewed by senior management at least annually; and (f) is used as the basis for setting the policies, procedures and controls that a relevant business chooses to implement for sanctions compliance purposes.
6.17	The purpose of the sanctions risk assessment is to analyse the inherent sanctions compliance risks associated with the activities of a relevant business. The process should enable a relevant business to understand how its activities might be most at risk of breaching financial sanctions and to then devise systems and controls to mitigate the identified inherent risks. A relevant business should focus its resources on areas of their business that carry a greater likelihood of involvement with individuals, entities, activities and jurisdictions that may be the subject of sanctions.
6.18	A relevant business should ensure that it has in place robust and comprehensive screening arrangements to prevent breaches of financial sanctions measures, as set out in Section 7.
6.19	A relevant business should ensure that its policies, procedures and controls in relation to compliance with financial sanctions measures, including its screening arrangements, are subject to regular testing and audit. Testing or audit are important tools to ensure that the sanctions compliance programme is working as designed and to identify weaknesses and deficiencies within that programme.

Section 7 – SCREENING

7.1	A relevant business should ensure that it screens a customer, its beneficial owner, its connected parties and any PPTA of the customer, against relevant money laundering and terrorism financing information sources, as well as financial sanctions measures lists, as part of its arrangements for determining if there are any money laundering, terrorism financing or sanctions risks in relation to the customer.
7.2	A relevant business should screen the persons referred to in 7.1: (a) when the relevant business establishes a business relationship with a customer; (b) when a relevant business undertakes any transaction of a value exceeding SHP 500 for a customer with which it has not otherwise established a business relationship; (c) on a periodic basis after the relevant business establishes a business relationship with the customer; and (d) immediately, when there are any changes or updates to the financial sanctions measures that apply in St Helena.

7.3	A relevant business should ensure that it maintains a database of names and particulars of designated persons under the UK financial sanctions measures. The database should also be subject to timely update whenever there are changes, and it should be made easily accessible by relevant staff. Alternatively, a relevant business may subscribe to such a database maintained by a third-party service provider and undertake periodic testing to ensure the completeness and accuracy of the database. More generally, to the extent that information technology solutions factor into the screening arrangements of a relevant business, it should ensure that it selects and calibrates the solutions in a manner that is appropriate to address its risk profile and compliance needs, and that it routinely tests the solutions to ensure effectiveness.
7.4	A relevant business which makes payments or transfers to other parties for a customer should ensure that it screens the customer and beneficiaries against financial sanctions lists that apply in St Helena prior to processing any such payment or transfer. Except under a licence, a relevant business may not make payments to a designated person. This would include dealing directly with the designated persons themselves or through intermediaries (including lawyers or accountants). A relevant business must therefore ensure that it does not give effect to a transaction that benefits a designated person. It will need to have a means of screening payment instructions to ensure that proposed payments to designated persons or their agents are not made.
7.5	A relevant business will also need to ensure that it has adequate controls to ensure that the persons referred to in 7.1 can be screened to determine whether they are connected to a jurisdiction that is, or becomes, subject to geographic sanctions measures or their business activities are, or become, ones which are the subject of trade sanctions measures.
7.6	When a possible name match is identified during screening, a relevant business should conduct enhanced checks to determine whether the possible match is a true match. In the event of a true match, or in case of any other suspicions of terrorist financing, money laundering or sanctions violations, a relevant business should make a disclosure to the relevant authorities as explained in Section 8.
7.7	A relevant business should ensure that it documents and retains the results of screening, assessment and enhanced checking results.

Section 8 – DISCLOSURE

MONEY LAUNDERING AND TERRORIST FINANCING

8.1	Where a relevant business knows or suspects, or has reasonable grounds for knowing or suspecting, that a person is engaged in money laundering or terrorist financing, the relevant business must as soon as reasonably practicable, and in any event within 7 days, report the matter to the Royal St Helena Police and to the Money Laundering Regulatory Authority by submitting a Suspicious Activity Report (SAR).
8.2	Suspicion is not the same as knowledge. Suspicion is more subjective and to form a suspicion a relevant business does not need proof based on concrete evidence. For a relevant business to have knowledge or suspicion, it does not need to know the nature of the underlying criminal activity, or that the funds definitely arose from that activity.

8.3	A relevant business should submit a SAR: (a) regardless of the amount of the transaction; (b) regardless of whether the transaction was completed; and (c) even where no transaction is conducted by or through the relevant business.
8.4	A customer's awareness of a possible SAR or investigation could prejudice future efforts to investigate the suspected ML or TF. Doing or saying anything that makes any person aware that a disclosure to the law enforcement authorities has been made, or doing or saying anything else that might prejudice an investigation, is commonly referred to as "tipping-off". A relevant business should ensure that its actions do not lead to tipping-off.
8.5	If a relevant business forms a suspicion that a transaction relates to ML/TF, they should take into account the risk of tipping-off when performing CDD measures. The business should ensure that their employees are aware of, and sensitive to, these issues when conducting CDD measures. If a relevant business forms a suspicion of ML or TF, and it reasonably believes that performing any of the CDD measures required in this Directive will tip-off a customer, a customer's PPTA, a connected party of the customer or a beneficial owner of the customer, a relevant business may stop performing those measures. In those circumstances, a relevant business should document the basis for its assessment and submit a SAR.
PROCEDURES RELATING TO SUSPICIOUS ACTIVITY IDENTIFICATION AND DISCLOSURE	
8.6	A relevant business should implement appropriate AML/CFT Controls in order to ensure that it can make a disclosure to the law enforcement authorities promptly when knowledge or suspicion of ML or TF arises. These AML/CFT Controls should include: (a) appointment of an MLRO; (b) establishing policies and procedures in relation to internal reporting, submission of SARs, and tipping-off; and (c) keeping records of internal reports and SARs.
8.7	To that end, a relevant business should put in place arrangements to ensure that: (a) a member of staff who in the course of their employment knows or suspects, or has reasonable grounds to know or suspect, that a person is engaged in ML or TF, discloses that matter to the MLRO of the relevant business as soon as practicable; and (b) where the MLRO knows or suspects, or has reasonable grounds to know or suspect, that a person is engaged in ML or TF, the MLRO discloses that matter to the law enforcement authorities as soon as reasonably practicable and in any event within 7 days of the matter being brought to the MLRO's attention.
8.8	The MLRO should act as a central reference point for reporting suspicious transactions. A relevant business should make and maintain arrangements to ensure that all staff are made aware of the identity of the relevant business's MLRO, and the procedures to follow when making an internal report about a suspicious transaction, including that all such reports should reach the MLRO without delay.

8.9	The lines of communication between staff and the MLRO should be as short as possible to facilitate access to the MLRO and ensure the promptness and confidentiality of the reporting. Managers and supervisors of staff should have no role in selecting which suspicious activity reports are received by the MLRO. The obligation to act in relation to a suspicious activity remains with the member of staff having the suspicion and it remains their decision whether to make an internal report. The MLRO should acknowledge receipt of an internal report and remind the person making the report that they should avoid tipping-off.
8.10	A relevant business should provide training and guidance to its staff to enable them to recognise or form a suspicion that ML or TF might be taking place. The training and guidance should take into account the nature of the customers and transactions that staff are likely to encounter, the type of product or service being provided and the means of delivery, i.e., whether in person or remotely.
8.11	Examples of situations which might give rise to a suspicion of ML or TF include where: (a) a relevant business is for any reason unable to complete CDD measures required by this Directive; or (b) the customer is reluctant, unable or unwilling to provide any information requested by the relevant business, or they decide to withdraw a pending application to establish a business relationship or a pending transaction, or to terminate an existing business relationship.
8.12	A relevant business should ensure that all staff at that business understand that they must raise an internal report with the MLRO as soon as they know or suspect, or where there are reasonable grounds for knowing or suspecting, that a person is engaged in ML or TF. A standard internal disclosure form may be provided for staff to use to notify the MLRO if they come across suspicious activity.
8.13	An internal report should be raised in respect of suspicious transactions or activities relating to a customer even if a previous report has already been made in relation to other suspicious transactions or events involving the same customer, whether the new suspicions are similar or different to those in the earlier report.
8.14	Any suspicion should be documented or recorded electronically and include the full details of the customer and a statement of the information on which the suspicion is based. Where a report is made verbally in case of urgency it should be followed up in writing without delay.
8.15	The MLRO should diligently consider each internal report to determine whether it gives rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion. The MLRO should have access to and consider all relevant information, including CDD and ongoing monitoring information available within the relevant business.
8.16	The MLRO will be expected to review transaction patterns and volumes through relevant accounts, consider any previous patterns of instructions, how long the relevant business has had a relationship with the person concerned and any CDD and ongoing monitoring information. The MLRO should consider appropriate questioning of the customer. In a case where the MLRO will need to conduct a potentially time-consuming examination of information, this should be balanced against the need to reach a conclusion promptly.
8.17	The MLRO should document or record electronically the evaluation process and their conclusions in relation to each internal report that they receive.

8.18	If the MLRO considers that there is knowledge, suspicion, or reasonable grounds for knowledge or suspicion, that a person is engaged in ML or TF the MLRO should, as soon as reasonably practicable, and in any event within 7 days, make a Suspicious Activity Report (SAR) by email to the Royal St Helena Police Service on **cid@sainthelena.gov.sh** and to the Money Laundering Regulatory Authority on **info@fsra.sh**.
8.19	Where the relevant knowledge or suspicion arises only after the transaction has been completed, the SAR should be made as soon as reasonably practicable after completion.
8.20	A relevant business should not proceed with a suspicious transaction unless consent has been given by the Money Laundering Regulatory Authority or the Royal St Helena Police Service, or 20 working days has elapsed without a response having been received.
8.21	All contact between a relevant business and law enforcement authorities should be controlled through, or reported back to a single contact point, which will typically be the MLRO.
8.22	If the MLRO decides not to submit a SAR after receiving an internal report, e.g., on the basis that the information does not meet the threshold for suspicion, they should document the reasons for their decision and keep a record of them with the original internal report.
8.23	A sole trader who knows or suspects, or where there are reasonable grounds to know or suspect, that a customer of theirs - or the person on whose behalf the customer is acting - is or has been engaged in, or attempting, ML or TF, should submit a SAR by email to the Royal St Helena Police Service on **cid@sainthelena.gov.sh** and to the Money Laundering Regulatory Authority on **info@fsra.sh**.
8.24	A form for use in making a SAR is included as Appendix 1 to this Directive.
FINANCIAL SANCTIONS MEASURES	
8.25	The financial sanctions measures that apply in St Helena require that a relevant business must make a report to the Governor of St Helena in a number of specified scenarios. However, a relevant business should also consider in each scenario whether it also has knowledge or suspicion, or reasonable grounds for knowledge of suspicion that ML or TF might be taking place. In that case, a relevant business should submit a SAR to the Royal St Helena Police Service and the Money Laundering Regulatory Authority, in addition to making a report to the Governor.
8.26	A relevant business is required to make a report to the Governor if it knows or has reasonable cause to suspect that a customer, a PPTA, a beneficial owner of a customer, a customer's connected person, or any person involved in a transaction or other commercial activity with the relevant business: (a) is a designated person; or (b) has committed a specified offence under the relevant financial sanctions measure.

8.27	For the purpose of 8.26, a specified offence refers to a range of offences, including, the offences of: (a) making available, directly or indirectly, any funds or other financial assets or economic resources to, or for the benefit of, (i) designated persons or entities; (ii) persons or entities acting on behalf or at the direction of the designated persons or entities mentioned in (i); or (iii) entities owned or controlled by any persons or entities mentioned in (i) or (ii); or (b) dealing with, directly or indirectly, any funds or other financial assets or economic resources belonging to, or owned or controlled by, such persons and entities falling within paragraph (a) above.
8.28	Where a relevant business informs the Governor of a matter arising under 8.26, it is required to state: (a) the information or other matter on which the knowledge or suspicion is based, and (b) any information it holds about the person by which the person can be identified.
8.29	Where a relevant business informs the Governor of a matter arising under 8.26, and the person is a designated person and is also a customer of the relevant business, it is required to state the nature and amount or quantity of any funds or economic resources held by it for the customer at the time when it first had the knowledge or suspicion.
8.30	A relevant business is required to inform the Governor without delay if that business (a) credits a frozen account, or (b) transfers funds from a frozen account, in either case relying on an exception from a prohibition in the relevant sanctions order.
8.31	A relevant business should keep records of any communications to the Governor that are required by the relevant sanctions order.

Section 9 – STAFF TRAINING

9.1	A relevant business should have effective systems and controls to prevent and detect ML/TF activities and to ensure compliance with applicable financial sanctions measures. The implementation of those systems and controls will be undermined if staff responsible for implementing those controls are not adequately trained and equipped with appropriate AML, CFT and financial sanctions awareness, skills and knowledge.
9.2	It is important that all staff of a relevant business are aware of the expectations of them in respect of AML, CFT and sanctions compliance and are alert to the risks that may be present in their role at the business. The same applies to any agents who act on behalf of the relevant business, so that "staff" is used here to include employees and agents. "Staff" should also be treated as including non-executive directors on the Board of the relevant business.
9.3	A relevant business should implement a clear and comprehensive policy for ensuring that relevant staff receive adequate training in relation to AML, CFT and sanctions compliance.
9.4	The senior management of a relevant business has overall responsibility for the establishment of an effective AML, CFT and sanctions compliance training programme. The CO is responsible for overseeing the timely implementation of that training programme.

9.5	A relevant business should ensure that its AML, CFT and sanctions compliance training programme explains to staff: (a) its policies and procedures relating to AML, CFT and sanctions compliance, including suspicious transaction identification, tipping-off and disclosure; (b) its statutory and regulatory obligations and the possible consequences for failure to comply with CDD and record keeping requirements; and (c) its statutory obligations in respect of financial sanctions measures compliance and the possible consequences for that business of a failure to comply.
9.6	It is particularly important that training on financial sanctions measures is continuous because, over time, new sanctions regimes may be introduced or existing regimes may be altered and the extent of general licences might vary. A relevant business should have a process for making staff aware of new or imminent changes in the financial sanctions area.
9.7	A relevant business may choose to use a mix of training techniques and tools, depending on the learning needs of their staff. These may include on-line learning as well as face-to-face and classroom training as well as one-to-one training. Training may include in-house or external training seminars or webinars by suitably qualified and experienced trainers. Training might include providing relevant employees with case studies and examples related to the relevant business. A relevant business may consider making use of publications and materials from other jurisdictions such as the United Kingdom provided that they are appropriate for St Helena. A relevant business may also consider using publications and materials from international organisations with an AML/CFT remit, such as FATF publications and typologies as part of the training materials. All materials should be kept up-to-date and in line with current requirements and standards.
9.8	No matter which training approach is adopted, a relevant business should maintain records of which staff have been trained, when they received the training and the type of training provided. Records should be maintained for the duration of an individual's employment or engagement and in any event for no less than three years.
9.9	The training should be focussed appropriately and different levels of training will be applicable to different categories of staff, depending on how their work is relevant to the business's compliance with AML, CFT and financial sanctions requirements, or how their role is capable of contributing to the identification or mitigation of the risks faced by the business, or the prevention or detection of ML/ TF or sanctions non-compliance. A relevant business might decide that members of staff in ancillary roles such as cleaning, property maintenance or catering do not require training. Those staff would be excluded from descriptions of training identified in the categories below.
9.10	Staff new to the relevant business, other than excluded staff, should have training that covers: (a) an introduction to ML, TF and sanctions and the importance of AML, CFT and sanctions compliance to the relevant business; and (b) the need to identify and disclose suspicious transactions to the MLRO, and the need to avoid tipping-off.

9.11	New staff should be trained as soon as possible after they start work at the relevant business, ideally as part of their induction process, and before undertaking any work to which AML, CFT or sanctions compliance requirements are applicable.
9.12	Staff who deal directly with customers should have training that covers, at least the following: (a) the importance of that staff member's role in the relevant business's AML, CFT and sanctions compliance strategy, i.e., potentially being the relevant business's first point of contact with persons engaged in suspicious transactions; (b) the relevant business's policies and procedures in relation to CDD and record-keeping requirements relevant to their job responsibilities; (c) guidance on identifying unusual activities in various circumstances that may give rise to a suspicion of ML/TF; and (d) the circumstances where extra vigilance might be required and the relevant policies and procedures for reporting unusual activities, including the line of reporting to the MLRO.
9.13	Staff who do not deal directly with customers but are involved in processing customer information and/or transactions should have training that covers, at least customer verification, and guidance on how to recognise unusual activities or transactions including abnormal payments or instructions
9.14	Staff undertaking the role of the MLRO should have training that covers, at least the following: (a) specific training in relation to the MLRO's responsibilities for assessing internal disclosures about suspicious activity submitted to them and making SARs to the Royal St Helena Police Service and the Money Laundering Regulatory Authority and reports to the Governor in relation to financial sanctions compliance matters; and (b) technical training on an ongoing basis to enable the MLRO to keep abreast of AML, CFT and sanctions compliance requirements or developments generally.
9.15	Staff at a management level are not excused from training in relation to AML, CFT and financial sanctions compliance. In addition to training on the requirements of the AML, CFT and financial sanctions compliance requirements that apply to a relevant business, training for senior management should address their role in supervising other staff in that business in respect of AML, CFT and financial sanctions compliance and techniques for exercising effective oversight.
9.16	Sole traders should ensure that they are trained in appropriate areas in order to adequately protect their business from ML, TF and sanctions compliance risks and should record all relevant training undertaken.
9.17	A relevant business should include in its training programme a way of monitoring the effectiveness of the training so that further training needs may be identified and appropriate action can be taken. This may be achieved by (a) including tests of staff understanding of the relevant business's policies and procedures to combat ML/TF and their ability to identify suspicious transactions; and (b) monitoring staff adherence to relevant business's AML, CFT and sanctions compliance systems and controls.
9.18	Staff should receive training at regular and appropriate intervals both to update on new developments and to refresh existing knowledge. The CO, MLRO and senior management of a relevant business should receive training of this kind at least annually.

9.19	A relevant business may consider whether it would be appropriate for some members of staff, such as the CO or MLRO, to obtain relevant professional financial crime-related qualifications.

Section 10 – RECORD-KEEPING

10.1	Good record-keeping is essential to the detection and investigation of ML/TF and the confiscation of criminal or terrorist funds or property. Accurate and comprehensive records help law enforcement to establish the financial profile of a suspect, trace the criminal's or terrorist's funds or property and assist in the examination of relevant past transactions to determine whether funds or property are the proceeds of, or relate to, criminal offences or terrorist activities.
10.2	Keeping appropriate records enables a relevant business to demonstrate that it has adopted appropriate measures for the identification and management of ML/TF risks in their business. A relevant business may choose to be cautious and keep a record of any matter that involves a judgement or a decision or any matter that will help demonstrate the relevant business's actions in relation the identification and management of ML/TF risks.
10.3	In addition to any other record keeping requirements stated elsewhere in this Directive, a relevant business should ensure that it keeps the following records: (a) a copy of any data, documents and information obtained by the business in applying CDD measures or ongoing monitoring, or records that enable the business to obtain a copy; (b) all correspondence in relation to a business relationship or occasional transaction; (c) client risk assessments; (d) records of senior management approval in relation to the establishment of business relationships or the carrying out of occasional transactions where there was assessed to be a higher risk of ML/TF; (e) minutes or other records of the proceedings and decisions of the client acceptance committee or equivalent body; (f) reports and analysis in relation to ongoing monitoring, including screening results and suspicious transactions; (g) reports and analysis in relation to internal disclosures about suspicious transactions; (h) SARs and internal and external correspondence in relation thereto; and (i) a record containing details relating to each transaction carried out by a relevant business in the course of a business relationship or in relation to an occasional transaction.
10.4	In relation to transaction records a relevant business should keep sufficient information to enable the reconstruction of an individual transaction, including: (a) the identity of the parties to the transaction; (b) the nature, date, currency and amount of the transaction; (c) system-generated transaction confirmations, including SWIFT records; and (d) the destination of the funds.

10.5	A relevant business should keep records of all internal ML/TF disclosures made to the MLRO. The record should include the date the disclosure was made, the names of staff members handling the report, the results of the evaluation, whether the report eventually resulted in an SAR and details of where a copy of the report may be found. The relevant business should keep records of all SARs made. The record should include the date of the SAR, the person who made it, and details of where a copy of the report may be found. Record should be kept of conversations with the law enforcement agencies and supervisory authorities regarding disclosures made.
10.6	Subject to 10.7, a relevant business should keep the records to which 10.3 refers for at least five years from the date that an occasional transaction is considered complete, or that the business relationship has come to an end.
10.7	In relation to records falling into 10.3(i), records should be kept for at least 5 years after the completion of a transaction.
10.8	In relation to compliance with financial sanctions measures, a relevant business should keep: (a) the results of its screening against the UK Sanctions List of designated persons; (b) a copy of investigations into screening results and into control and ownership.

APPENDIX 1: SUSPICIOUS ACTIVITY DISCLOSURE FORM

Complete a separate form in respect of each suspected person, company or business.

Either type or print this form. Complete all sections or state "N/A" for a section that is not applicable. When submitting this form attach all relevant material. For each section attach additional sheets as necessary.

Suspicious Activity Reports should be delivered by email, indicated as "Confidential", for the attention of the Chief of Police, Royal St Helena Police Service on **cid@sainthelena.gov.sh** and copied to the Chair of the Money Laundering Regulatory Authority of Saint Helena on **info@fsra.sh**

1. DETAILS OF REPORTING ENTITY:

Date report submitted to the RSHPS: _____

Name of entity or person making the report: _____

The name of an individual who is authorised to discuss the contents of this report should be provided, if different.

_____

Contact details: _____

Address of reporting entity or person:

_____

_____

_____

Company name *(if applicable)*: _____

Type of business: _____ *(e.g. Bank, Insurance Manager/Agent)*

Telephone No: _____

E-mail address: _____

Reporting entity's reference: _____

Nature of service(s) provided to the individual and/or entity that is the subject of this report:

2. SUBJECT(S) OF REPORT (NATURAL PERSONS):

First name:_____ Surname: _____

Date of birth:_____ Place of birth:_____Nationality:_____

Occupation/Profession:_____

Name and address of employer *(if applicable)*:_____

Address(es): _____

_____

_____

Telephone No (H):_____ E-Mail: _____

Telephone No (W):_____

ID document type:_____ ID document number:_____

(i.e. passport, driver's licence etc.)

Date of issue:_____ Place of issue:_____

Is the person an existing client, prospective client or something else_____

(if something else e.g. accountant, employee, provide details)

Account number(s) if applicable:_____

Other signatories on the account: *if applicable*_____

Include identity information, addresses, and other relevant information.

3. SUBJECT(S) OF REPORT (LEGAL ENTITIES):

Name of Entity:_____

Entity type:_____ *(Company, Trust, Partnership, Charity, Other)*

Jurisdiction of incorporation/registration:_____

Date of incorporation/registration:_____

Purpose of entity:_____

Registered office address (or address of Trustee or General Partner etc.):_____

_____

_____

_____

Business address (if different from registered office address):_____

_____

_____

_____

For each of the following which is a natural person provide the identity information noted in Section 2 as far as known.

Shareholder(s) name(s):_____

_____

_____

Director(s) name(s): _____

_____

_____

Ultimate beneficial owner(s) if different from above: _____

Name(s): _____

_____

_____

Account number(s) if applicable: _____

Other signatories on the account: _____

_____

_____

Include identity information, addresses, and other relevant information.

4. OTHER FINANCIAL SERVICE PROVIDERS INVOLVED IN ACTIVITY:

Name: _____ Address: _____

_____

_____

Account number if applicable: _____

Name: _____ Address: _____

_____

_____

Account number if applicable: _____

5. REASON FOR SUSPICION:

Provide an account of the activity, detailing what is unusual, irregular or suspicious. The information should be provided in a chronological order that allows for clear understanding of the suspicion being reported.

The following checklist may assist in preparing the account.

A. Provide full details of any third party individual or company on whose behalf the transaction is being conducted.
B. Explain who benefitted financially or otherwise, from the transaction. How much and when.
C. Retain any admission or explanation of the transaction provided by the individual or any other person and indicate to whom and when it was given.
D. Retain any evidence of concealment or evidence of an attempt to deceive.
E. Indicate where the possible violation took place e.g. main office, branch etc.
F. Indicate whether the possible violation is an isolated incident or related to other transactions.
G. Recommend any further investigation that might assist authorities.
H. Indicate whether currency (cash) and/or monetary instruments were involved. If so, provide the amount, the country of currency, e.g., British pounds and/or other description.
I. Indicate any transactions that may be involved or affected.

Name and Signature of Money Laundering Reporting Officer