

ANTI-MONEY LAUNDERING/PREVENTION OF TERRORIST FINANCING GUIDANCE NOTES

Reissued on 15th August 2018 by the Anti-Money Laundering Committee under section 118(9) of the Proceeds of Crime Ordinance.

Note: This document constitutes Guidance Notes previously issued as part of The Anti-Money Laundering and Prevention of Terrorist Financing Code 2011 (*L.N.13 of 2011*), which are now being reissued by the Anti-Money Laundering Committee as a stand-alone guideline.

PART 1 – Preliminary Provisions and Interpretation

The following guidance notes are in respect of regulations 1-3 of the Anti-Money Laundering and Prevention of Terrorist Financing Code.

Introduction

- (i) In common with all countries, both offshore and on-shore, the Turks and Caicos Islands Government (TCIG) has a responsibility to comply with international standards concerning the prevention and detection of money laundering and the combating of terrorist financing and proliferation. These standards are primarily set by the Financial Action Task Force (“the FATF”). The current version of the FATF standards can be found on the FATF website¹. The Basel Committee on Banking Supervision, the International Organization of Securities Commissions and the International Association of Insurance Supervisors also set sector specific anti-money laundering standards for banking, securities and investment business and insurance business respectively. In addition, the TCIG is a member of the Caribbean Financial Action Task Force², a grouping of Caribbean states that have agreed to implement common counter measures to address money laundering and terrorist financing.
- (ii) The TCIG is committed to complying with its international obligations and has had a framework of anti-money laundering legislation in place since 1988. The legislative framework was extensively reviewed in 2007 and The Proceeds of Crime Ordinance Chapter 3.15 (“POCO”) was enacted in October 2007. The POCO has been amended regularly and the Anti-Money Laundering and Prevention of Terrorist Financing Regulations and the Anti-Money Laundering and Prevention of Terrorist Financing Code (“the Code”) were issued in 2010 and 2011 respectively.

¹ [http://www.fatf-gafi.org/publications/?hf=10&b=0&s=desc\(fatf_releasedate\)](http://www.fatf-gafi.org/publications/?hf=10&b=0&s=desc(fatf_releasedate))

² <https://www.cfatf-gafic.org/>

In summary, POCO is designed to:

- (a) criminalise money laundering;
- (b) provide for the confiscation of the proceeds of criminal conduct;
- (c) enable the civil recovery of property which represents, or is obtained through, unlawful conduct;
- (d) provide the Financial Intelligence Agency, as the TCI's Financial Intelligence Agency, with clear functions and enhance its powers;
- (e) require persons in the financial sector to report knowledge or suspicions concerning money laundering to the Financial Intelligence Agency;
- (f) give the Supreme Court the power to make a number of orders to assist the police in their investigations into money laundering;
- (g) establish a National Forfeiture Fund; and
- (h) by providing for the making of the AML/PTF Regulations and the issuance of the Code, to enable the establishment of a framework for the prevention and detection of money laundering and terrorist financing.

(iii) POCO does not provide for the combating of terrorist financing, which is covered principally by the Prevention of Terrorism Ordinance, and the following Orders:

Anti-terrorism (Financial and Other Measures) (Overseas Territories) Order 2002

Libya (Restrictive Measures) (Overseas Territories) Order 2011

The Afghanistan (United Nations Measures) (Overseas Territories) Order 2012

Syria (Restrictive Measures) (Overseas Territories) Order 2012

Zimbabwe (Sanctions) (Overseas Territories) Order 2012

Somalia (Sanctions) (Overseas Territories) Order 2012

Guinea-Bissau (Sanctions) (Overseas Territories) Order 2012

Eritrea (Sanctions) (Overseas Territories) Order 2012

Democratic People's Republic of Korea (Sanctions) (Overseas Territories) Order 2012

Guinea (Sanctions) (Overseas Territories) Order 2013

Burma (Sanctions) (Overseas Territories) Order 2013

Ukraine (Sanctions) (Overseas Territories) (No. 2) Order 2014

Ukraine (Sanctions) (Overseas Territories) (No. 3) Order 2014

Sudan (Sanctions) (Overseas Territories) Order 2014

South Sudan (Sanctions) (Overseas Territories) Order 2014

Central African Republic (Sanctions) (Overseas Territories) Order 2014

Russia, Crimea and Sevastopol (Sanctions) (Overseas Territories) Order 2014

Yemen (Sanctions) (Overseas Territories) (No.2) Order 2015

Democratic Republic of the Congo (Sanctions) (Overseas Territories) Order 2015

Burundi (Sanctions) (Overseas Territories) Order 2015

Iraq (Sanctions) (Overseas Territories) Order 2015

ISIL (Da'esh) and Al-Qaida (Sanctions) (Overseas Territories) Order 2016

Iran (Sanctions) (Overseas Territories) Order 2016

Mali (Sanctions) (Overseas Territories) Order 2017

Policing and Crime Act (Financial Sanctions) (Overseas Territories) Order 2017

Venezuela (Sanctions) (Overseas Territories) Order 2018

- (iv) The Turks and Caicos Islands (TCI) financial businesses are one of the most important lines of defence against the use of the jurisdiction for money laundering and terrorist financing. The AML/CFT Regulations therefore impose requirements on financial businesses with respect to measures to be taken by them to prevent money laundering and terrorist financing. Most breaches of the AML/CFT Regulations constitute an offence for which the penalty is a maximum fine of \$100,000.00. The AML/PTF Regulations are supplemented by the AML/PTF Code.
- (v) The obligations contained in POCO, the AML/PTF Regulations and the Code will be rigorously enforced. However, it is in the interests of the TCI as a jurisdiction that efforts to prevent money laundering and terrorist financing are undertaken in a spirit of cooperation between the public and private sectors. Furthermore, regardless of the legal obligations imposed on them by POCO, the AML/PTF Regulations and the Code, it is very much in the interests of all financial businesses to have strong systems in place to reduce the risk that they are used in connection with money laundering or terrorist financing. The use of a TCI financial business in connection with money laundering or terrorist financing is likely to damage the reputation of the business and of the TCI as a financial services jurisdiction, which could lead to a loss of legitimate business. It is therefore important that every financial business understands the important role it plays in protecting the reputation of the TCI. Furthermore, a financial business that assists in the laundering of money or terrorist financing risks possible prosecution for a money laundering offence, enforcement action and, if a regulated person, the loss of its licence. Breaches of POCO, the AML/PTF Regulations and the Code could also result in the directors of a financial business being prosecuted for a criminal offence.
- (vi) A financial business is best able to protect itself from being used in connection with money laundering or terrorist financing by maintaining effective procedures, systems and controls, including sound customer due diligence procedures, that comply with international standards, and rigorously implementing them. The Code sets out requirements imposed on financial businesses for the prevention of money laundering and the combating of terrorist financing that supplement the requirements of the POCO and the AML/PTF Regulations. The Financial Intelligence Agency considers that the legal regime taken as a whole enables the TCI to meet international standards.

The Code

(vii) The Code:

- (a) sets out detailed requirements for the prevention of money laundering and terrorist financing that must be met by financial businesses;

- (b) assists financial businesses to design and implement appropriate systems and controls for the prevention of money laundering and terrorist financing;
- (c) promotes the use of a proportionate, risk-sensitive approach to the prevention of money laundering and terrorist financing and, in particular, to customer due diligence measures; and
- (d) enables the TCI to meet international standards concerning anti-money laundering and the combating of terrorist financing.

(iii) The Code and the Guidance provided herein cannot anticipate all circumstances and are not therefore exhaustive. Where permitted by the AML/PTF Regulations or the Code, financial businesses are expected to adopt an appropriate and intelligent risk-sensitive approach. The Code specifies minimum standards that must be complied with by every financial business, unless it is covered by a specific exemption. However, the particular circumstances of a financial business may require it to take additional measures beyond those minimum standards, and beyond the provisions of this Guidance. Financial businesses should always consider whether, on a case-by-case basis, additional measures are appropriate to prevent their products and services being used for money laundering or terrorist financing.

It is therefore essential that all persons to which the Code applies adopt an intelligent risk-sensitive approach and establish and maintain systems and procedures that are appropriate and proportionate to the risks identified.

Status of Code

(ix) The Code is issued by the Anti-Money-Laundering Committee under section 118 (1) of POCO. Section 118 (5) of the POCO provides that the Code is subordinate legislation and has full legislative effect. In the circumstances, the Code has the status of “law” in the TCI.

The Code:

- (a) must be complied with by every person to whom it applies;
- (b) has effect as law and therefore has the same legal force as if the provisions in the Code had been contained in POCO or the AML/PTF Regulations;
- (c) is enforceable by the Commission [see “Enforcement” below]; and
- (d) a breach of the Code, constitutes an offence.

(x) POCO provides that the Code is subject to a negative resolution procedure. Although the Code has full effect on the date specified in the Code, it must be laid before the House of Assembly and the House may, by resolution, annul the Code at a subsequent meeting of the House.

Status of Guidance

(xi) The Guidance has been issued by the Anti-Money-Laundering Committee under section 118 (9) of POCO and, is not part of the Code. The purpose of the Guidance is to:

- (a) outline the relevant requirements of POCO, the AML/PTF Regulations, the Prevention of Terrorism Ordinance and other relevant legislation with respect to the prevention of money laundering and terrorist financing;
 - (b) provide guidance to assist financial businesses to interpret the requirements of POCO, the AML/PTF Regulations and the Code;
 - (c) provide important background or explanatory information;
 - (d) provide practical guidance on identification and verification of identity;
 - (e) set out the factors that will be taken into account in considering whether or not a requirement in POCO, the AML/PTF Regulations or the Code has been complied with; and
 - (f) provide guidance on how financial businesses are expected to comply with the AML/PTF Regulations and the Code.
- (xii) Although the Guidance does not have the status of “law”, section 177 (5) of POCO requires the Court to consider whether a person has followed any guidance issued under section 118 (9) by the Anti-Money Laundering Committee in deciding whether a person has committed an offence under the AML/PTF Regulations. In its role as the enforcement authority for the Code, the Commission will consider whether the Guidance has been followed in deciding whether a financial business has failed to comply with the Code.
- (xiii) In order to assist in explaining the AML/CFT framework, the Guidance paraphrases some of the requirements of POCO, the AML/PTF Regulations and the Code. However, the original text of each is the authoritative source and should always be referred to in interpreting the various provisions and requirements.
- The Guidance cannot, of course, modify or in any way dilute the requirements of the AML/PTF Regulations or the Code. If there is any inconsistency between the Guidance and the AML/PTF Regulations or Code, the Regulations or the Code prevail.
- (xiv) Although it is expected that senior management of financial businesses will use the Code and the Guidance in the design of its policies, systems and controls and in the preparation of its procedures manuals, the Code and Guidance are not suitable for adoption by a financial business as its own procedures manual.

Scope of the Code

- (xv) As indicated in section 3, the Code applies, to the extent specified, to all financial businesses and their boards and directors. A “financial business” is a person specified in Schedule 2 of the AML/PTF Regulations.

Application of Regulations and Code outside the TCI

- (xvi) Regulation 10 of the AML/PTF Regulations provides that the Regulations and the Code apply to an overseas branch (which includes a representative or contact office) or subsidiary of a relevant financial business (as defined in the Regulations), to the extent that the laws in the foreign country permit. This is designed to ensure that the TCI relevant financial businesses apply standards equivalent to the FATF Recommendations throughout their financial services business, wherever the business is situated or carried on.
- (xvii) Where the laws of the foreign country do not permit this, the Commission must be informed in writing and, to the extent that the laws of the foreign country permit, the relevant financial business must apply alternative measures to ensure compliance with the FATF Recommendations and to deal effectively with the risk of money laundering and terrorist financing.

Enforcement of the Code

- (xviii) The AML/PTF Regulations and the Code are enforceable:
- (a) against regulated persons, by the Commission under the Financial Services Commission Ordinance; and
 - (b) against Designated Non-Financial Businesses and Professions (DNFBP), by the Commission (as the designated supervisory authority) under section 161 (2) of POCO.
- (xix) Each of the above enables the Commission to take enforcement action if the financial business has contravened or is in contravention of the AML/PTF Regulations or the Code and provides the Commission with a range of enforcement powers. In the case of a regulated person, non-compliance with the AML/PTF Regulations or the Code will also be taken into account by the Commission in assessing whether a regulated person is “fit and proper” to hold a licence.
- (xx) Compliance by financial businesses with their AML/PTF obligations will form part of the Commission’s assessment of financial businesses when undertaking on-site compliance visits. It will also form part of the Commission’s on-going monitoring of financial businesses.

Part 2 – Policies, Systems and Controls

The following guidance notes are in respect of regulations 4-7 of the Anti-Money Laundering and Prevention of Terrorist Financing Code.

Risk-sensitive approach

- (i) The senior management of companies and other undertakings, both within and outside the financial sector, increasingly manage the affairs of their undertaking with regard to the

inherent money laundering and terrorist financing risks in its business and put in place systems, controls and procedures that effectively manage these risks. A risk-sensitive approach is also appropriate to managing the risks associated with money laundering and terrorist financing.

(ii) Furthermore, there are substantial differences between the various types of financial business in the TCI, and in the circumstances of different financial businesses of the same type, and in their customers and their customers' businesses. This diversity makes a prescriptive, and of necessity, inflexible approach to the measures required to prevent money laundering and combat terrorist financing impracticable.

(iii) International standards recognize the benefit of a risk-sensitive approach to the prevention and detection of money laundering and terrorist financing. In its June 2007 publication "Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing", the FATF states:

"By adopting a risk-based approach, competent authorities and financial institutions are able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the risks identified. This will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention. The alternative approaches are that resources are either applied evenly, so that all financial institutions, customers, products etc. receive equal attention or that resources are targeted but on the basis of factors other than the risk assessed. This can inadvertently lead to a 'tick box' approach with the focus on meeting regulatory needs rather than combating money laundering or terrorist financing."

Sector specific approach guidance can be found at: [http://www.fatf-gafi.org/documents/riskbasedapproach/?hf=10&b=0&s=desc\(fatf_releasedate\)](http://www.fatf-gafi.org/documents/riskbasedapproach/?hf=10&b=0&s=desc(fatf_releasedate))

The TCI's AML/CFT regime therefore takes a risk-sensitive approach.

(iv) A risk-sensitive approach recognises that the money laundering and terrorist financing threat to a financial business is dependent upon a number of factors, including its customers, the countries in which it operates, the products it offers and its delivery channels and, whilst establishing minimum standards that must always be complied with, allows a financial business: (a) to differentiate between customers in a way that matches the risk in a particular business; (b) to apply its own approach to systems and controls and arrangements in particular circumstances; and (d) to design more effective systems and controls that are not required to fit all circumstances.

- (v) It is important to appreciate that systems and controls will not detect and prevent all money laundering or terrorist financing.

A risk-sensitive approach will, however, serve to balance the cost burden placed on a financial business and its customers with a realistic assessment of the threat of the business being used in connection with money laundering or terrorist financing. It focuses the effort where it is needed and will have most impact (see the FATF publication cited above and the FSTF industry specific guidance on the FATF website www.fatf-gafi.org).

Risk assessment

- (vi) A financial business can only fully appreciate the money laundering and terrorist financing risks that it faces by undertaking a money laundering and terrorist financing risk assessment. Regulation 4(1) of the Code therefore requires a financial business to carry out a formal risk assessment. The risk assessment must take account of the matters specified in regulation 4(2) of the Code.
- (vii) The risk assessment will underpin the AML/CFT policies and procedures of a financial business in all areas. The business, products and customer base of some financial businesses may be relatively straightforward; particularly if they offer few products and their customers fall into similar categories. For these financial businesses, the risk assessment may enable them to design systems and controls that focus on customers that fall outside the “norm”. In the case of other financial businesses, particularly those with more complex products and a more diverse customer base, the systems and controls will need to be more sophisticated. The risk assessment will enable a financial business to design systems and controls that are appropriate for the risks that it faces.
- (viii) Regulation 4(1) of the Code requires the risk assessment to be documented. When undertaking on-site compliance visits, as part of its assessment of a financial business, the Commission will require documented evidence that a money laundering and terrorist financing risk assessment has been undertaken.
- (ix) The money laundering and terrorist financing risk assessment should be kept under regular review and updated as necessary, particularly if there are material changes in the business or customers of the financial business or the risks that it faces. It is not possible to say how often a formal reassessment will be required as this will depend upon the circumstances of a particular financial business. For some financial businesses it may be appropriate for a reassessment to be carried out annually. However, for many financial businesses, particularly those with a relatively stable business and customer base, the reassessment would not need to be undertaken so frequently.

- (x) The risk assessment is only the first part of implementing a risk-sensitive approach, however. Building on the risk assessment, a financial business should prepare a risk profile for each customer, which will build up over time, allowing the financial business to identify transactions or activities that may be suspicious. This is covered further in the following regulations of the Code.

Responsibilities of board

- (xi) The principal responsibilities of the board are set out in regulation 5 of the Code. The MLRO, the MLCO and senior management will assist the board in fulfilling these responsibilities. Larger or more complex financial businesses may also require dedicated risk and internal audit functions to assist in the assessment and management of money laundering and terrorist financing risk.

Policies, procedures, systems and controls

- (xii) Regulation 17 of the AML/PTF Regulations sets out broad requirements with respect to the risk-sensitive money laundering and terrorist financing policies, systems and controls that must be established, maintained and implemented by a financial business. The matters required to be covered by the AML/CFT policies, systems and controls include the following:

- (a) customer due diligence measures and ongoing monitoring;
- (b) the reporting of suspicious activities;
- (c) record-keeping;
- (d) screening of employees;
- (e) internal controls;
- (f) risk assessment and management;
- (g) the monitoring and management of compliance;
- (h) the internal communication of its policies, systems and controls;
- (i) the identification and scrutiny of—
 - (I) complex or unusually large transactions;
 - (II) unusual patterns of transactions which have no apparent economic or visible lawful purpose; and
- (j) any other activity which the financial business regards as particularly likely by its nature to be related to the risk of money laundering or terrorist financing; and the taking of additional measures, where appropriate, to prevent the use for money laundering or terrorist financing of products and transactions which are susceptible to anonymity;

These are supplemented by regulation 6 of the Code. In order to be effective, the AML/CFT systems and controls must be appropriate given the circumstances of a particular financial business.

- (xiii) Regulation 5(2)(d) of the Code provides that the board has responsibility for assessing the effectiveness of, and compliance with, the policies, systems and controls established and promptly taking such actions as is required to remedy deficiencies.
- (xiv) In order to assess the effectiveness of the AML/CFT policies, systems and controls, the board will need, amongst other things, to:
- (a) ensure that it receives regular, timely and adequate information relevant to the management of the financial business's money laundering and terrorist financing risk;
 - (b) monitor the ongoing competence and effectiveness of the MLCO and the MLRO;
 - (c) undertake periodic reviews of the adequacy of policies and procedures for higher risk customers;
 - (d) consider whether the incidence of suspicious activity reports (or an absence of such reports) has highlighted any deficiencies in the financial business's customer due diligence or reporting policies and procedures and whether changes are required to address any such deficiencies;
 - (e) consider whether inquiries have been made by the Financial Intelligence Agency, or production orders received, without issues having previously being identified by customer due diligence or reporting policies and procedures;
 - (f) consider changes made or proposed in respect of new legislation, regulatory requirements or guidance, or as a result of changes in business activities.
- (xv) In order to assess compliance with the AML/CFT policies, systems and controls, the board will need to periodically commission and consider a compliance report from the MLCO.

Outsourcing

- (xvi) Regulation 7(2) of the Code provides that a financial business must not outsource its AML/CFT compliance function. This means that a financial business may not outsource the compliance function as a whole. However, where appropriate, a financial business may outsource certain specific compliance activities.

The following guidance notes are in respect of regulations 8-9 of the Anti-Money Laundering and Prevention of Terrorist Financing Code.

Money laundering reporting officer

- (xvii) Regulation 22 of the AML/PTF Regulations requires every financial business to appoint a MLRO. The MLRO has responsibility for receiving internal money laundering disclosures, deciding whether these disclosures should be reported to the Financial Intelligence Agency and, if he so decides, making the reports to the Financial Intelligence Agency, and acting as the liaison point with the Financial Intelligence Agency and the Commission.

- (xviii) A financial business with a substantial business may need to appoint other individuals to assist the MLRO. Where such other individuals are appointed, it is permissible for its procedures to permit employees to make internal reports to these individuals, on behalf of the MLRO. However, the MLRO has ultimate responsibility for all reports made by employees of the financial business and any other individuals appointed must be answerable to the MLRO.
- (xix) The MLRO will have more knowledge and experience relevant to the prevention of money laundering and terrorist financing than other employees of the financial business. The AML/PTF Regulations anticipate that the MLRO will use his knowledge and experience to fully assess the disclosure that has been made to him and that he will only make a suspicious transaction report to the Financial Intelligence Agency if he considers, after his assessment, that the information disclosed gives rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion, of money laundering or terrorist financing. The MLRO is expected to act as a filter and not to routinely pass all disclosures made to him to the Financial Intelligence Agency without making his own assessment.
- (xx) Where the size of the business permits, the MLRO may carry on other functions within the financial business, provided that they do not conflict with his duties as MLRO.
- (xxi) The MLRO must:
- (a) oversee any deputy MLRO or other staff appointed to assist him; and
 - (b) maintain full and clear records of all disclosures that he has received and all suspicious activity reports he has made.
- (xxii) The MLRO must also take great care to manage relationships with clients appropriately to avoid tipping off any third parties.

Money laundering compliance officer

- (xxiii) Regulation 21 of the AML/PTF Regulations requires every financial business to appoint a MLCO. The MLCO can be the same person as the MLRO and, in the case of a regulated person, can be the same person as the person appointed as compliance officer for the purposes of regulatory compliance, if approved by the Commission.

However, a regulated person may split the reporting and compliance functions and appoint different individuals as its MLRO and MLCO.

Part 3 – Customer Due Diligence

The following guidance notes are in respect of regulations 10-12 of the Anti-Money Laundering and Prevention of Terrorist Financing Code.

Introduction

- (i) The maintenance and operation by the financial services sector of adequate customer due diligence measures is, and has for many years, been fundamental to the TCI's efforts to combat money laundering and terrorist financing.

- (ii) A financial business needs to carry out adequate customer due diligence for the following reasons:
 - (a) customer due diligence helps to protect a financial business, and the jurisdiction, from the risk of being used as a vehicle for money laundering, terrorist financing or other financial crime, helps to protect the financial business from becoming a victim of financial crime and helps to protect against identity fraud;
 - (b) a financial business that has carried out customer due diligence is able to assist law enforcement agencies by providing information on customers and potential customers and on activities or transactions that are subject to investigation; and
 - (c) customer due diligence has an essential role to play in a financial business's own risk management procedures.

- (iii) Customer due diligence information will also assist a financial business, and its MLRO and employees, to assess whether a suspicious activity report should be made.

What is "customer due diligence"?

- (i) The term "customer due diligence measures" is defined in regulation 5 of the AML/PTF Regulations. In essence, effective customer due diligence measures will require a financial business to carry out a number of steps, addressing:
 - (a) identifying who a customer is and whose identity needs to be verified;
 - (b) verifying the identity of the customer using documents, data or information obtained from a reliable and independent source;
 - (c) determining whether the customer is acting for a third party and, if so, identifying the third party;
 - (d) where the customer (or any third party) is not an individual acting in his own right, identifying the beneficial owners of the customer or third party, or in the case of a foundation, the persons concerned with the foundation;
 - (e) verifying the identity of any third parties and of the beneficial owners of the customer and any third parties;
 - (f) understanding the circumstances and business of a customer, including where appropriate the source of wealth and funds, the purpose of the business relationship with the financial business and the expected nature and level of transactions;
 - (g) keeping the information held up to date and valid;

(h) the ongoing monitoring of transactions undertaken and the business relationship with the purpose of assessing the extent to which the transactions and activity carried on by the customer are consistent with his circumstances and business and the intended business relationship.

(i) It should be noted that the AML/PTF Regulations include within the definition of beneficial owner, an individual who exercises ultimate control over the management of a legal person, partnership or legal arrangement, whether alone or jointly.

Summary of principal requirements of AML/PTF Regulations with respect to customer due diligence

(ii) Regulation 11(1) of the AML/PTF Regulations imposes a requirement on financial businesses to apply customer due diligence measures:

- (a) before establishing a business relationship with a customer or carrying out a one-off transaction;
- (b) where the financial business suspects money laundering or terrorist financing or doubts the veracity or adequacy of documents, data or information previously obtained under its due diligence measures or when conducting on-going monitoring; and
- (c) at other appropriate times to existing customers as determined on a risk-sensitive basis.

(iii) Regulation 17(1) of the AML/PTF Regulations includes a requirement to establish, maintain and implement appropriate risk-sensitive policies and procedures relating to customer due diligence measures and on-going monitoring.

(iv) Regulation 17(2) of the AML/PTF Regulations requires that the policies and procedures, including those relating to customer due diligence measures, must include policies and procedures which provide for:

- (a) the identification and scrutiny of:
 - (i) complex or unusually large transactions;
 - (ii) unusual patterns of transactions which have no apparent economic or visible lawful purpose; and
 - (iii) any other activity which the financial business regards as particularly likely by its nature to be related to the risk of money laundering or terrorist financing;
- (b) the taking of additional measures, where appropriate, to prevent the use for money laundering or terrorist financing of products and transactions which are susceptible to anonymity;
- (c) determining whether:
 - (i) a customer, any third party for whom the customer is acting and any beneficial owner of the customer or third party, is a politically exposed person;

- (II) a business relationship or transaction, or proposed business relationship or transaction, is with a person connected with a country that does not apply, or insufficiently applies, the FATF Recommendations or there is call to apply countermeasures by the FATF, UN or EU;
- (III) a business relationship or transaction, or proposed business relationship or transaction, is with a person connected with a country or territory that is subject to measures for purposes connected with the prevention and detection of money laundering or terrorist financing, imposed by one or more countries or sanctioned by the European Union or the United Nations.

(ix) Regulation 13 of the AML/PTF Regulations sets out the circumstances in which a financial business must, on a risk-sensitive basis, apply enhanced customer due diligence measures.

Risk-sensitive approach to due diligence measures

(x) The AML/PTF Regulations and the Code require a financial business to apply a risk-sensitive approach to its customer due diligence measures. The advantages and features of a risk-sensitive approach are covered generally in the Guidance to Part 2 of the Code and this Guidance should be read together with the Guidance in Part 2. However, it should, of course, be appreciated that the minimum requirements of the AML/PTF Regulations and the Code must at all times be complied with.

(xi) Regulation 4 of the Code requires a financial business to carry out a risk assessment. The risk assessment will enable the financial business to determine its initial approach to designing appropriate customer due diligence procedures for different types of customer. A risk-sensitive approach to customer due diligence also requires a risk assessment to be undertaken with respect to a particular customer, based on that customer's individual circumstances. This will determine the extent of the identification and other customer due diligence information that will be sought, how it will be verified and the extent to which the resulting relationship will be monitored. The specific requirements of the Code concerning the obtaining of identification information and the verification of identity are covered later in this Part.

(xii) It is important to appreciate that identifying a customer as carrying a higher risk of involvement in money laundering or terrorist financing does not necessarily mean that the customer is a money launderer or financing terrorism. Similarly, identifying a customer as carrying a lower risk of involvement in money laundering or terrorist financing does not necessarily mean that the customer is not a money launderer or is not financing terrorism.

(xiii) As already indicated, the broad objective of a risk-sensitive approach is to enable a financial business to know who its customers are, what they do, and whether or not they are likely to be engaged in money laundering, terrorist financing or other criminal activity. This is achieved

by preparing a risk profile for each customer following the steps set out in regulation 4(2) of the Code.

Relationship Information

- (xiv) Customer due diligence information comprises both information on the identity of the customer [identification information] and information on the business relationship [relationship information]. Identification information is covered in the following regulations of the Code. The Guidance that follows relates to relationship information.
- (xv) Relationship information (i.e. information on the business relationship, or proposed business relationship), is the information necessary to enable a financial business to fully understand the nature of the customer's business, or proposed business and the rationale for the business relationship. This will include information on the source of the customer's funds and, in higher risk relationships, the source of the customer's wealth.
- (xvi) The nature and extent of the relationship information obtained with respect to a customer will depend on a number of factors, such as the countries with which he is connected, the product or service to be supplied how the product or service will be delivered and factors specific to the customer. The principle objective is to obtain sufficient information to identify a pattern of expected activity and to identify unusual, complex or higher risk activity and transactions that may indicate money laundering or terrorist financing. However, regulation 12(2) of the Code sets out relationship information that must be obtained by a financial business.

Source of funds and wealth

- (xvii) The "source of funds" is the business, transaction or other activity that generates the funds for a customer, which may include the customer's occupation.

A person's "source of wealth" means the business, transactions or other activities that have generated the total net worth of a person. It should be noted that it is the source of the person's wealth that is important rather than the amount of it. It may not, therefore, be necessary for information on the amount of wealth to be obtained.

- (xviii) Regulation 12(2)(c) of the Code provides that information should always be obtained with respect to the source of funds and that information with respect to the source of wealth should be obtained where the customer, business relationship or occasional transaction presents a high risk.
- (xix) When sufficient customer due diligence information has been obtained, the financial business should carry out a customer risk assessment. Regulation 11(3) of the Code provides that, in preparing a customer risk assessment, a financial business must consider the following four

risk elements: customer risk, product risk, delivery risk and country risk. An assessment of each of these risks is combined to produce a risk profile for the customer. These risk elements are considered below.

Customer risk

(xx) Customer risk is the identification of the risk posed by the type of customer. In assessing customer risk, a financial business will need to consider a number of factors, including the following:

- (a) Type of customer: For example, a politically exposed person presents a higher level of risk.
- (b) Type and complexity of the relationship: Complex business structures, for example structures involving a mixture of companies and trusts or simply a number of different companies, can make it easier to conceal underlying beneficiaries. Relationships involving these structures present a higher risk unless there is a clear and legitimate commercial rationale for the structure. The use of bearer shares will also present a higher risk, particularly where the country in which the company is incorporated or registered does not require bearer shares to be immobilised.
- (c) The value and nature of the funds or assets: Customers engaged in a business that generates significant amounts of cash, or wishing to undertake a large number of cash transactions, or with a high value of funds, especially where not fully explained, present a higher level of risk. The geographic source of the funds is also relevant to risk.
- (d) Commercial rationale: Is there a clear commercial rationale for the customer purchasing the product or service? If there is no clear rationale, the relationship should be regarded as presenting a higher level of risk.
- (e) Secrecy: Requests to associate undue levels of secrecy with a transaction or relationship or, in the case of a legal entity, reluctance to provide information as to beneficial owners or controllers present a higher level of risk.
- (f) Source of funds and wealth not easily verified: Situations where the source of funds and/or the origin of wealth cannot be easily verified, or where the audit trail has been deliberately broken and/or unnecessarily layered present a higher level of risk.
- (g) Delegation of authority: Delegation of authority by the customer, for example, through a power of attorney presents a higher level of risk.

(xxi) Other factors may suggest a lower level of risk, for example, where the customer:

- (a) has a strong reputation;
- (b) is subject to public disclosure rules, for example publicly listed companies;
- (c) is subject to regulation by a statutory regulator (not just a financial services regulator).

(xxii) Regard should always be had to external data sources that may indicate whether a person is high risk. These will include the TCI legislation applying United Nations sanctions, guidance issued by the Commission and may include information published by governments and law enforcement authorities on terrorists (e.g. United States government agencies such as the Federal Bureau of Investigation and the Office of Foreign Assets Control (OFAC)), electronic subscription databases, the internet and other media. In particular, the UK Government Treasury maintains a consolidated list of targets listed by the UN, EU, and UK under legislation relating to current financial sanctions regimes.

Product risk

(xxiii) Product risk (or service risk) is the risk posed by the product proposition itself. The following examples indicate higher risk products:

- (a) ability to make payments to third parties;
- (b) ability to pay in or withdraw cash;
- (c) ability to migrate from one product to another;
- (d) ability to hold boxes, parcels or sealed envelopes in safe custody;
- (e) ability to use numbered accounts or accounts that offer a layer of opacity;
- (f) ability to pool underlying customers.

(xxiv) The use of correspondent banking relationships is common and commercially convenient. However, this presents an increased risk as other customers of the bank may be using it to launder funds. Additional due diligence and/or controls are therefore required. Correspondent banking relationships are covered in Part 8 of the Code.

Delivery risk

(xxv) Delivery risk is the risk posed by the mechanism through which the business relationship is commenced and transacted.

The following examples indicate higher risk delivery mechanisms:

- (a) where the relationship with the customer is indirect, for example through the use of intermediaries; and
- (b) non-face to face relationships, for example where products are delivered exclusively by post or telephone or over the Internet.

Country risk

- (xxvi) Country risk is the risk posed by the geographic provenance of the economic activity of the business relationship. It should be noted that this is wider than the residence of the customer, third party or beneficial owner and will include, for example, the place where the business is being carried on. Determination of Country risk is best referred to as the geographical footprint of the customer.
- (xxvii) Countries falling into one or more of the following categories should be considered as higher risk countries:
- (a) countries that have inadequate safeguards in place against money laundering or terrorist financing;
 - (b) countries that have high levels of organised crime;
 - (c) countries that have strong links with terrorist activities;
 - (d) countries that are vulnerable to corruption;
 - (e) countries that are the subject of United Nations or European Union sanctions.
- (xxviii) In assessing which countries may present a higher risk, regard should be had to objective data published, for example, by the IMF, FATF, US Department of State (International Narcotics Control Strategy Report), Office of Foreign Assets Control (“OFAC”), and Transparency International (Corruption Perception Index).

Customer Risk Assessment

- (xxix) In preparing a customer risk assessment, a financial business should take into account:
- (a) the customer due diligence information obtained and the evaluation of that information; and
 - (b) inconsistencies between the customer due diligence information obtained.
- (xxx) The sophistication of the risk assessment process may be determined according to factors established by the business risk assessment. Where it is appropriate to do so, risk may be assessed generically for applicants and customers falling into similar categories. The business of some financial businesses, their products, and customer base, can be relatively simple, involving few products, with most applicants or customers falling into similar risk categories. In such circumstances, a simple approach, building on the risk that the business’ products are assessed to present, may be appropriate for most customers, with the focus being on those customers who fall outside the norm.

Others may have a greater level of business, but large numbers of their customers may be predominantly retail, served through delivery channels that offer the possibility of adopting a standardised approach to many procedures. Again, the approach for most customers may be relatively straight forward - building on product risk.

A more complex system may be appropriate for diverse customer bases or financial businesses with broad ranges of products or services.

Updating customer due diligence

(xxxix) Regulation 11(1)(b) and (c) of the AML/PTF Regulations require a financial business to apply customer due diligence measures subsequent to the establishment of a business relationship (i.e. to update the customer due diligence) where the financial business:

- (a) suspects money laundering or terrorist financing;
- (b) doubts the veracity or adequacy of documents, data or information previously obtained under its customer due diligence measures or when conducting ongoing monitoring;
- (c) at other appropriate times to existing customers as determined on a risk-sensitive basis.

(xxxix) In order to demonstrate compliance with paragraph (c), a financial business would usually be expected to:

- (a) review and update its customer due diligence information on at least an annual basis where it has assessed a customer relationship as presenting a higher risk; and
- (b) review and update its customer due diligence information on a risk-sensitive basis, but not less than once in every 5 years, where it has assessed a customer relationship as presenting a normal or low risk.

Events such as the opening of a new account, the purchase of a further product, or meeting with a customer may present a convenient opportunity to update customer due diligence information.

The following guidance notes are in respect of regulation 13 of the Anti-Money Laundering and Prevention of Terrorism Regulations and regulation 13 of the Anti-Money Laundering and Prevention of Terrorist Financing Code.

Enhanced customer due diligence - introduction

(xxxix) Regulation 13(2) of the AML/PTF Regulations requires a financial business, on a risk-sensitive basis to apply enhanced customer due diligence measures (and undertake enhanced ongoing monitoring) in the following specified circumstances:

- (a) where the customer has not been physically present for identification purposes;
- (b) where the financial business has, or proposes to have, a business relationship with, or proposes to carry out an occasional transaction with, a person connected with a country or territory that does not apply, or insufficiently applies, the FATF recommendations and there is call to apply countermeasures by the FATF, UN or EU;

- (c) where the financial business is a domestic bank that has or proposes to have a banking or similar relationship with an institution whose address for that purpose is outside the TCI;
- (d) where the financial business has or proposes to have a business relationship with, or to carry out an occasional transaction with, a politically exposed person;
- (e) where any of the following is a politically exposed person:
 - (I) a third party;
 - (II) a beneficial owner of the customer or a third party;
 - (III) a person acting, or purporting to act, on behalf of the customer;
 - (IV) in any other situation which by its nature can present a higher risk of money laundering or terrorist financing.

(xxxiii) Regulation 13 of the AML/PTF Regulations sets out a number of specific circumstances where enhanced customer due diligence measures must be applied and enhanced ongoing monitoring undertaken. However, enhanced ongoing monitoring is also required in any other situation which by its nature can present a higher risk of money laundering or terrorist financing. A financial business must decide whether a particular situation can present a higher risk of money laundering using the customer risk assessment that it is required to carry out. However, certain factors should always be considered to indicate higher level of risk, such as:

- (a) customers who are connected with business sectors that are vulnerable to corruption, for example arms or oil sales; and
- (b) customers who are connected to countries that are perceived to have a higher level of corruptions (see the further guidance below with respect to politically exposed persons).

Enhanced customer due diligence measures and ongoing monitoring

(xxxvi) Regulation 13(1) of the AML/PTF Regulations provides that: ““enhanced customer due diligence measures” and “enhanced ongoing monitoring” mean customer due diligence measures, or ongoing monitoring, that involve specific and adequate measures to compensate for the higher risk of money laundering or terrorist financing.”

(xxxvii) Where a financial business is required by the AML/PTF Regulations to apply enhanced due diligence measures and undertake enhanced ongoing monitoring, the financial business must determine, on the basis of the particular circumstances, what “specific and adequate measures” will be required to compensate for the higher money laundering and terrorist financing risks. These measures are almost certain to include obtaining further identification information and relationship information, including further information on the source of funds and the source of wealth. These should be obtained from appropriate sources, which may be the customer or an independent source.

(xxxviii) Other enhanced due diligence measures that should be considered include:

- (a) taking additional steps to verify the customer due diligence information obtained;
- (b) obtaining due diligence reports from independent experts to confirm the veracity of customer due diligence information held;
- (c) requiring board or senior management approval for higher risk customers;
- (d) requiring more frequent reviews of high risk business relationships; and
- (e) setting lower monitoring thresholds for transactions connected with the business relationship.

Politically exposed persons

(~~xxxviii~~) Politically exposed person (or “PEPs”) are individuals who are, or have been, entrusted with prominent public functions in a country together with their immediate family members and their close associates.

(~~xxxix~~) PEPs present a high risk to financial businesses because their position makes them vulnerable to corruption and corruption is invariably associated with money laundering. The risk to a financial business is even higher where the PEP has connections with countries, or types of business, where corruption is prevalent. The FATF 40 recommendations therefore requires all PEPs to be regarded as high-risk customers. Although PEP status places a customer into a higher risk category, it does not, of itself, incriminate the person concerned.

(~~xi~~) The AML/PTF Regulations provide a comprehensive definition of a PEP (regulation 6). It should be noted that the definition includes, not just the individual who has a prominent function, but also that person’s immediate family members and his close associates.

(~~li~~) Regulation 13 of the AML/PTF Regulations requires a financial business, on a risk-sensitive basis, to apply enhanced due diligence measures and undertake enhanced ongoing monitoring where a customer, third party or beneficial owner is a PEP and regulation 13 of the Code supplements these provisions by setting out a number of detailed additional requirements with respect to PEPs.

(~~lii~~) Establishing whether a person is a PEP is not always straightforward and can present difficulties. The risk assessment carried out in compliance with regulation 4 of the Code will assist a financial business to determine the extent to which PEPs are a significant risk to it. PEPs will present a greater risk to some financial businesses than to others, depending in part on their business and delivery channels. Whilst the requirements of the AML/PTF Regulations and the Code apply to all financial businesses, where the business assessment indicates that a financial business faces a more significant risk, it will need to take that into account in designing its systems and controls with respect to PEPs.

(~~liii~~) The following checks may assist a financial business to determine whether a person is a PEP:

- (a) Assess the corruption risks posed by any countries with which the person has a connection. There are a number of specialist reports and databases published by specialised national, international, non-governmental and commercial organisations that may be used for this purpose. One potential reference resource is the Transparency International Corruption Perception Index, which ranks approximately 150 countries according to their perceived level of corruption.
 - (b) If, on a risk-sensitive basis, the financial business needs to conduct more thorough checks, or if there is a high likelihood of a financial business having PEPs as customers, subscription to a specialist PEP database may be the only adequate risk mitigation tool.
 - (c) Ascertain the identity of individuals who hold, or formerly held, prominent public functions in any country with which the person concerned is connected and, as far as reasonably practicable, determine whether the person concerned has any associations with those individuals. The Websites of international organizations, such as the UN, may assist in determining the identity of such individuals.
- (xlii) The above checks do not represent a comprehensive list and the Commission would expect them to be used on a risk-sensitive basis. The extent to which a service needs to utilize the checks, if at all, will depend upon its business risk assessment and its customer risk assessment.
- (xliii) Although new and existing customers may not initially meet the definition of a PEP, financial businesses should, as far as practicable, be alert to public information relating to possible changes in the status of its customers with regard to political exposure.

The following guidance notes are in respect of regulations 14-15 of the Anti-Money Laundering and Prevention of Terrorist Financing Code.

Introduction

- (i) Regulation 14 to 27 of the Code provide for, and the following Guidance describes:
 - (a) the identification information that must be obtained by a financial business in applying customer due diligence measures (and ongoing monitoring, which is covered in a separate Part of the Code);
 - (b) the verification of the identity information; and
 - (c) exceptions to the requirements to obtain and verify identity information. 40

This Guidance also covers the requirements of the AML/CFT Regulations concerning the obtaining and verification of identity evidence.

Requirements of AML/PTF Regulations

(ii) As indicated in the Guidance to previous sections of the Code, the AML/PTF Regulations (regulation 5(1)) provide that the customer due diligence measures to be applied by a financial business include:

- (a) identifying the customer, any third parties and any beneficial owners;
- (b) verifying the identity of the customer and any third parties; and
- (c) taking reasonable measures, on a risk-sensitive basis, to verify the identity of each beneficial owner of the customer and any third parties.

(iii) In essence, all persons who are not individuals, including companies, foundations, partnerships or trusts and any other type of legal arrangement are regarded as having a beneficial owner who is an individual. The definition of “beneficial owner” is contained in regulation 3 of the AML/PTF Regulations which, in summary, provides that beneficial owners are:

- (a) individuals who are ultimate beneficial owners of the legal person, partnership or legal arrangement; and
- (b) individuals who exercise ultimate control over the management of the legal person, partnership or legal arrangement.

It should be noted that it makes no difference whether:

- (a) an individual’s ultimate ownership or control of a legal person, partnership or legal arrangement is direct or indirect; and
- (b) an individual is the sole beneficial owner or a joint beneficial owner.

(iv) As indicated in the guidance to the sections on customer due diligence above, regulation 11 of the AML/PTF Regulations specifies when customer due diligence measures must be applied. These circumstances are supplemented by regulation 11 of the Code.

(v) Although customer due diligence measures must in most cases be applied before the establishment of a business relationship or the carrying out of an occasional transaction, regulation 11(5) and (6) of the AML/PTF Regulations permit two exceptions. Regulation 11 (5) provides that a financial business may complete the verification of the identity of a customer, third party or beneficial owner after the establishment of a business relationship if—

- (a) it is necessary not to interrupt the normal conduct of business;
- (b) there is little risk of money laundering or terrorist financing occurring as a result; and
- (c) verification of identity is completed as soon as reasonably practicable after the contact with the customer is first established.

- (vi) Regulation 11(6) of the AML/PTF Regulations permits a bank to verify the identity of a bank account holder after the opening of the bank account provided that there are adequate safeguards 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 to the account holder.

- (vii) These are the only exceptions, and it is expected that they should be applied only on an infrequent basis. In all other cases, customer due diligence measures must be applied before the establishment of a business relationship or the carrying out of an occasional transaction.

Identification information

- (viii) Customer identification is a two stage process. First it is necessary to obtain identity information, i.e. information concerning the identity of the person concerned. Next, the identity information must be verified.

The objective of obtaining identity information is to establish that the named person actually exists. The objective of the second stage is to verify from reliable, independent documentary or other acceptable evidence that the person concerned is that person.

- (ix) The identity of a person has a number of different aspects. In respect of an individual, identity includes the individual's full name (which may change), gender and date and place of birth. Other facts about an individual may also be relevant, including family circumstances and addresses, employment and career, contacts with Government and other authorities and with other financial institutions, in and outside the TCI, and physical appearance. In respect of a legal entity, identity is a combination of its constitution, its business and its legal and ownership structure.

Identification of an individual

- (x) A financial business is required by the AML/PTF Regulations to obtain identification on, and verify the identity of, any individual:
 - (a) who, as a customer, seeks to enter into a business relationship with the financial business or undertake an occasional transaction, whether solely or jointly;
 - (b) who is a third party; or
 - (c) who is the beneficial owner of a customer or of a third party;

- (xi) Regulation 14(1) of the Code sets out the identification that must always be obtained with respect to an individual. Regulation 14(2) requires a financial business to obtain additional identity information where it determines that the individual presents a higher risk and regulation 14(3) specifies additional identification information that must be obtained. Although a financial business is only required to obtain two types of additional identification

information, a financial business should consider whether it should obtain all three and, where it only obtains two of the specified types, it should consider obtaining a third (different) type of identification information.

Verification of identity of an individual

- (xii)* It is an overriding requirement of both the AML/PTF Regulations and the Code that a financial business verifies the identity of a person using documents, data or information obtained from a reliable and independent source.
- (xiii)* Evidence of identity can take a number of forms. In respect of individuals, much weight is placed on identity documents, such as passports, and these are often the easiest way of being reasonably satisfied as to someone's identity. It is, however, possible to be reasonably satisfied as to a customer's identity based on other forms of evidence. However, financial businesses should appreciate that different sources of identification evidence vary in their integrity and independence. For example, some documents are issued after a due diligence check, for example passports, whilst others are not. Also, some documents are more easily forged. If a financial business is not familiar with the form of evidence obtained to verify identity, it may be necessary for the financial business to take appropriate measures to satisfy itself that the evidence is genuine.
- (xiv)* Given the range of sources available to a financial business, and the risk profiles of different customers, the Code is not prescriptive as to how the identity of any person should be verified. However, a financial business should be able to demonstrate that it has complied with its obligations to verify the identity of an individual if it follows the Guidance set out in the following paragraphs. Financial businesses are reminded that section 149(5) of POCO provides that, in deciding whether a person has committed an offence under the AML/CFT Regulations, the Court shall consider whether the person has followed any guidance issued by the Financial Intelligence Agency.
- (xv)* The Anti Money Laundering Committee regards the following general methods of verifying the identity of an individual to be acceptable:

 - (a)* a current passport, which provides photographic evidence of identity;
 - (b)* a current national identity card or document, but only if it provides photographic evidence of identity;
 - (c)* a current driving licence, but only if the licensing authority carries out an identity check before issuing the licence and that the licence provides photographic evidence of identity;
 - (d)* an independent data source (including an electronic source), subject to the Guidance on independent data sources that follows.

- (xvi) The Financial Intelligence Agency considers the following methods of verifying an individual's residential address to be acceptable:
- (a) a bank statement or a utility bill;
 - (b) correspondence from a central or local government department or agency;
 - (c) a letter of introduction confirming residential address from a regulated person or a foreign regulated person; or
 - (d) a personal visit to the individual's residential address.
- (xvii) Where the general methods of identifying the identity of an individual are not practical and the individual concerned presents a low risk, the individual's identity may be verified using:
- (a) a TCI (i.e. not a temporary) driver's licence; or
 - (b) a birth certificate, in conjunction with:
 - (I) a bank statement or utility bill;
 - (II) documentation issued by a government source; or
 - (III) a letter of introduction from a regulated person.

The use of independent data sources

- (xviii) A financial business may be able to rely on an independent data source to provide satisfactory evidence of identity, or an aspect of it. Data sources include both sources of reliable independent public information, such as a register of electors or a telephone directory, commercially available databases maintained by, for example, credit reference agencies, business information services and commercial agencies that provide electronic identity checks.
- (xix) In principle, the Anti Money Laundering Committee regards such independent data sources as acceptable for the verification of the identity. However, where a financial business uses an independent data source or sources, the Anti Money Laundering Committee would expect the financial business to ensure that:
- (a) the source, scope and quality of the data are satisfactory;
 - (b) to obtain at least two matches of each component of an individual's identity being verified; and
 - (c) it is able to capture and record the information used to verify identity.
- (xx) In considering whether an independent third party data source is satisfactory, a financial business should consider the following:
- (a) whether the third party is registered with a data protection agency;
 - (b) the range of positive information sources that the third party can call upon to link an applicant to both current and historical data;
 - (c) whether the third party accesses negative information sources such as databases relating to fraud and deceased persons;

- (d) whether the third party accesses a wide range of alert data sources; and
- (e) whether the third party has transparent processes that enable a financial business to know what checks have been carried out, what the results of these checks were and to be able to determine the level of satisfaction provided by those checks.

The following guidance notes are in respect of paragraphs 16-18 of the Anti-Money Laundering and Prevention of Terrorist Financing Code.

Introduction

- (i) Regulations 16 and 17 of the Code specify requirements concerning the identification of, and the verification of the identity of, legal entities, other than foundations. Foundations are covered in regulations 21 to 23 of the Code. A legal entity is defined in the AML/PTF Regulations to include a company, a partnership, whether limited or general, an association or any unincorporated body of persons, but it does not include a trust. The definition therefore includes clubs, societies, charities, church bodies and institutes, amongst others.

Identification of a legal entity

- (ii) There is a wide range of potential customers that are not individuals. These include legal entities (such as companies) and trusts, which are not strictly entities at all. The legal owners of a legal entity may be specific individuals or other legal entities. However, the beneficial ownership may rest with others, either because the legal owner is acting for the beneficial owner, or because there is a legal obligation for the ownership to be registered in a particular way.
- (iii) In deciding who the customer is when it is not an individual, the objective of a financial business must be to know who has control over the funds which form or otherwise relate to the relationship, and/or form the controlling mind and/or management of any legal entity involved in the funds. The subsequent judgment as to whose identity to verify will be made following a risk-based approach, and will take account of the number of individuals, the nature and distribution of their Verification of directors and beneficial owners interests in the entity and the nature and extent of any business, contractual or family relationship between them.
- (iv) Certain information about the legal entity comprising the non-individual customer should be obtained as a standard requirement. Thereafter, on the basis of the money laundering/terrorist financing risk assessed through the customer risk assessment, a financial business should decide the extent to which the identity of the entity and of specific individuals should be verified, using reliable, independent source documents, data or information. The financial business should also decide what additional information in respect of the legal entity and, potentially, some of the individuals behind it should be obtained.

- (v) Whilst information on an entity's website may be useful, financial businesses will understand that this information should be treated with caution as it has not been independently verified before being made publicly available on the Internet.
- (vi) Where the person seeking to establish a business relationship or carry out an occasional transaction is a legal entity, a financial business should ensure that it fully understands the legal form, structure and ownership of the legal entity and should obtain sufficient additional information on the nature of the entity's business, and the reasons for seeking the product or service.
- (vii) A financial business is required by the AML/PTF Regulations to obtain identification information on, and verify the identity of, any legal entity:
 - (a) that, as a customer, seeks to enter into a business relationship with the financial business or undertake an occasional transaction, whether solely or jointly; or
 - (b) that is a third party;
- (viii) Regulation 17(1) of the Code sets out the identification that must always be obtained with respect to a legal entity. Section 17(3) requires a financial business to obtain additional identity information where it determines that the legal entity presents a higher risk.

Verification of identity of a legal entity

- (ix) The Anti Money Laundering Committee regards the following general methods of verifying the identity of a legal entity to be acceptable:
 - (a) certificate of incorporation, registration or equivalent;
 - (b) memorandum and articles of association or equivalent constituting documents;
 - (c) a company registry search, including confirmation that the legal entity is not in the process of being dissolved, struck off, wound up or terminated;
 - (d) the latest audited financial statements of the legal entity;
 - (e) independent data sources, including electronic sources, e.g. business information services; and
 - (f) where the financial business determines that the legal entity does not present a low risk, a personal visit to the legal entity's principal place of business.
- (x) Where the financial business determines that the legal entity presents a low level of risk, at least one of the methods specified above should be used. Where it determines that the legal entity presents a higher level of risk, at least two of the methods specified above should be used.

- (xi) In the case of unincorporated bodies of persons, such as clubs, a financial business will need to identify the persons who fulfil equivalent functions to the directors of a company, such as the members of the board or governing council.
- (xii) Where a financial business verifies the identity of a director, or equivalent, on a remote basis, regulation 24 of the Code applies.
- (xiii) In the case of a regulated entity, the identity of a director may be verified if the full name of the director is obtained together with written confirmation from the regulated person that the person concerned is a director.

The following guidance notes are in respect of regulations 19-20 of the Anti-Money Laundering and Prevention of Terrorist Financing Code.

Identification information, trusts and trustees

- (i) There are a wide variety of trusts, ranging from large, nationally and internationally active organisations subject to a high degree of public interest and quasi-accountability, through to trusts set up under testamentary arrangements, and trusts established for wealth management purposes. It is important, in putting proportionate anti-money laundering or prevention of terrorism financing policies, systems and controls in place, and in carrying out risk assessments, that financial businesses take account of the different money laundering or terrorist financing risks that trusts of different sizes and areas of activity present.
- (ii) Trusts are not separate legal entities – it is the trustees collectively who are the customer. In these cases, the obligation to identify the customer attaches to the trustees, rather than to the trust itself, although certain identification information concerning the trust is also required to be obtained. The purpose and objects of most trusts are set out in a trust deed.
- (iii) A trustee will also have to be identified and verified where a trustee is the beneficial owner or the controller of an applicant for business or is a third party on whose behalf an applicant for business is acting.
- (iv) A financial business is not required to establish the detailed terms of the trust, nor the rights of the beneficiaries.
- (v) The AML/PTF Regulations require a financial business to obtain identification information concerning a trust when the trustee of a trust (in that capacity) is:
 - (a) a customer;
 - (b) a third party; or
 - (c) a beneficial owner.

- (vi) As provided by the Code, the relevant regulations of the Code relating to individuals, legal entities or foundations apply depending upon whether the trustee whose identity information is required to be obtained, or whose identity is required to be verified, is an individual, a legal entity or a foundation.

The following guidance notes are in respect of regulations 21-23 of the Anti-Money Laundering and Prevention of Terrorist Financing Code.

- (i) Regulations 21 to 23 of the Code specify requirements concerning the identification of, and the verification of the identity of, foundations. Although the legislation of the TCI does not provide for the establishment of foundations, financial businesses are likely to have, or acquire, foundations as customers and given their special constitution, it is important that they are properly identified.
- (ii) Where a financial business is required to identify a foundation, certain identification information (as specified in the Code) should be obtained as a standard requirement. Thereafter, on the basis of the money laundering/terrorist financing risk assessed in the customer risk assessment, a financial business should decide the extent to which the identity of the foundation and of specific individuals should be verified, using reliable, independent source documents, data or information. The financial business should also decide what additional information in respect of the foundation and, potentially, some of the individuals concerned with it should be obtained.
- (iii) Where the person seeking to establish a business relationship or carry out an occasional transaction is a foundation, the financial business should ensure that it fully understands the legal form and structure of the foundation and should obtain sufficient additional information on the nature of the foundation's business, and the reasons for seeking the product or service.
- (iv) A financial business is required by the AML/PTF Regulations to obtain identification information on, and verify the identity of, any foundation:
 - (a) that, as a customer, seeks to enter into a business relationship with the financial business or undertake an occasional transaction, whether solely or jointly; or
 - (b) that is a third party.
- (v) Regulation 21(1) of the Code sets out the identification that must always be obtained with respect to a foundation. Regulation 21(2) of the Code requires a financial business to obtain additional identity information where it determines that the foundation presents a higher risk.

- (vi) The Anti Money Laundering Committee regards the following general methods of verifying the identity of a foundation to be acceptable:
- (a) the declaration of establishment (or equivalent);
 - (b) a search of the Registry of Foundations in the country in which it is established, formed, registered or incorporated, including confirmation that the foundation is not in the process of being dissolved or struck off (or the equivalent);
 - (c) the latest audited financial statements of the foundation;
 - (d) independent data sources, including electronic sources, e.g. business information services; and
 - (e) where the financial business determines that the foundation does not present a low risk, a personal visit to the foundation's principal place of business.
- (vii) Where the financial business determines that the foundation presents a low level of risk, at least one of the methods specified above should be used. Where it determines that the foundation presents a higher level of risk, at least two of the methods specified above should be used.
- (viii) Where a financial business verifies the identity of a person concerned with the foundation on a remote basis, regulation 23 of the Code applies.
- (ix) In the case of a regulated foundation, the identity of a Foundation Council member may be verified if the full name of the member is obtained together with written confirmation from the regulated person that the person concerned is a Foundation Council member.

The following guidance notes are in respect of regulations 24-25 of the Anti-Money Laundering and Prevention of Terrorist Financing Code.

Non-Face to Face Identification and Verification Procedures

- (i) Face to face to contact with an applicant presents the lowest risk to a financial business. This is because face-to-face contact enables the staff of the financial business to verify the likeness of the applicant to the photograph on the documentary evidence and to identify any inconsistencies.
- (ii) It follows that any mechanism that enables an applicant to apply for a product without face-to-face contact increases the risk to the financial business. Indeed, many financial businesses only accept applications remotely and do not offer them the opportunity of attending the financial business's premises. Non-face to face applications are now increasingly common as applications are made and accepted by post, telephone or via the internet.

Although applications and transactions undertaken across the internet may, in themselves, not pose any greater risk than other non-face to face business, such as applications submitted by post, there are other factors that may, taken together, aggravate the typical risks, for example:

- (a) the ease of access to the facility, regardless of time and location;
 - (b) the ease of making multiple fictitious applications without incurring extra cost or the risk of detection;
 - (c) the absence of physical documents; and
 - (d) the speed of electronic transactions.

- (iii) The extent of verification in respect of non-face to face customers will depend on the nature and characteristics of the product or service requested and the assessed money laundering risk presented by the customer. There are some circumstances where the applicant is typically not physically present, such as when purchasing some types of collective investments, which would not in themselves increase the risk attaching to the transaction or activity. A financial business should take account of such cases in developing their systems and procedures.

- (iv) Where a prospective customer approaches a financial business remotely (by post, telephone or over the internet), the financial business should carry out non-face to face verification, either electronically or by reference to documents.

- (v) Non-face to face identification and verification carries an inherent risk of identity fraud. Therefore, the Code requires a financial business to perform at least one additional check which is designed to mitigate the risk of identity fraud. The Code is not prescriptive as to the additional checks or checks that should be carried out as this is for the financial business to determine, depending upon the circumstances and its customer risk assessment. However, the additional checks that can be taken include:
 - (a) verification of identity using a further method of verification;
 - (b) obtaining copies of identification documents certified by a suitable certifier;
 - (c) requiring the first payment for the financial services product or service to be drawn on an account in the customer's name at a bank that is a regulated person or a foreign regulated person;
 - (d) verifying additional aspects of identity or other customer due diligence information from independent sources;
 - (e) telephone contact with the customer on a home or business number which has been verified prior to establishing a relationship, or telephone contact before transactions are permitted, using the call to verify additional aspects of identification information that have previously been provided;

- (f) internet sign-on following verification procedures where the customer uses security codes, tokens, and/or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address; and
- (g) specific card or account activation procedures.

Certification of documents

- (vi) The use of a certifier guards against the risk that copy documentation provided is not a true copy of the original document and that the documentation does not correspond to the customer whose identity is to be verified. For certification to be effective, the certifier will need to have seen the original documentation and, where documentation is to be used to provide satisfactory evidence of identity for an individual, have met the individual (where certifying evidence of identity containing a photograph). For this reason, obtaining copies of identification documents certified by a suitable certifier is one of the additional verification checks that should be considered for non-face to face business.

- (vii) The Code requires that a certifier shall not be relied upon unless the certifier is subject to professional rules (or equivalent) which provide the financial business with a reasonable level of comfort as to the integrity of the certifier. Suitable certifiers may include:
 - (a) a member of the judiciary, a senior public servant, or a serving police or customs officer;
 - (b) an officer of an embassy, consulate or high commission of the country of issue of documentary evidence of identity;
 - (c) a lawyer or notary public who is a member of a recognised professional body;
 - (d) an actuary who is a member of a recognised professional body;
 - (e) an accountant who is a member of a recognised professional body;
 - (f) a notary public or equivalent;
 - (g) a director, officer, or manager of a regulated person, or of a branch or subsidiary of a group headquartered in a well-regulated jurisdiction which applies group standards to subsidiaries and branches worldwide, and tests the application of and compliance with such standards.

- (viii) The Code requires that the certifier must have provided adequate information so that he may be contacted in the event of a query. The Anti Money Laundering Committee considers that this requirement would be met when the certifier include his name, position or capacity, his address and a telephone number or email address at which he can be contacted.

- (ix) A higher level of assurance will be provided where the relationship between the certifier and the person whose identity is being verified is of a professional rather than a personal nature.

The following guidance notes are in respect of regulation 26 of the Anti-Money Laundering and Prevention of Terrorist Financing Code.

Introduction

- (i) Regulation 15 of the AML/PTF Regulations specifies circumstances in which a financial business is not required to apply customer due diligence measures before establishing a business relationship of undertaking an occasional transaction. In summary, the exceptions apply:
 - (a) when the customer is a regulated person or a foreign regulated person, a company, the securities of which are listed on a recognized exchange, or a public authority in the TCI; and
 - (b) in respect of certain low value life insurance contracts.

- (ii) It is important to appreciate that the customer exceptions only apply where the customer satisfies the criteria referred to in subparagraph (a) above. They do not apply with respect to any third parties for whom the customer may be acting, or the beneficial owners of any third parties.

- (iii) The exceptions do not apply where the financial business suspects money laundering or terrorist financing.

- (iv) The following may be regarded as a public authority in the TCI:
 - (a) the Government of the TCI;
 - (b) any statutory body established under a TCI enactment;
 - (c) any company wholly owned by the Government of the TCI.

The following guidance notes are in respect of regulation 27 of the Anti-Money Laundering and Prevention of Terrorist Financing Code.

Introduction

- (i) The AML/PTF Regulations require a financial business to determine whether a customer is acting for a third party and, if so, to:
 - (a) identify the third party and verify the third party's identity;
 - (b) to identify each beneficial owner of the third party and, taking reasonable measures on a risk-sensitive basis, to verify each of the third party's beneficial owners.

Where a customer acts for a third party, the relationship is referred to as an intermediary relationship as there is no direct relationship between the financial business and the underlying customer.

- (ii) An intermediary relationship is different from an introduced relationship where, following the introduction, a direct relationship between the financial business and the underlying customer is established. The terms “intermediary” and “introducer” are defined in regulation 3(1) of the AML/PTF Regulations.
- (iii) However, where a financial business relies on an introducer or intermediary to apply customer due diligence measures, the financial business remains liable for any failure to apply those measures.
- (iv) A financial business does not have to rely on an intermediary to apply customer due diligence measures, or to apply all the customer due diligence measures. Once the business relationship is established, the financial business cannot rely on the introducer or intermediary to undertake ongoing monitoring on its behalf.
- (v) The intermediary/introducer provisions do not affect arrangements whereby a financial business outsources the application of customer due diligence measures, although the financial business remains responsible for any failure to apply these measures.

Reliance on intermediary or introducer

- (vi) In the circumstances specified in regulation 14 of the AML/PTF Regulations, a financial business can rely on an intermediary to apply the customer due diligence measures with respect to the customer, third parties and beneficial owners. In summary, an intermediary or introducer can be relied on if:
 - (a) the intermediary or introducer is a regulated person or a foreign regulated person; and
 - (b) the intermediary or introducer consents to being relied on.
- (vii) The AML/PTF Regulations expressly provide that the provisions are subject to any requirements of the Code. The Code imposes a number of additional conditions before an intermediary or introducer can be relied upon. First, a financial business must satisfy itself that the intermediary or introducer satisfies the criteria in the AML/PTF Regulations and then it must carry out a risk assessment to determine whether it is appropriate for it to rely on the intermediary or introducer and, if so, whether it should put in place any measures to mitigate the additional risk.
- (viii) In carrying out a risk assessment, the financial business will need to consider a number of factors, including the following:

- (a) the stature and regulatory track record of the intermediary or introducer;
- (b) the adequacy of the framework to combat money laundering and financing of terrorism in place in the country in which the intermediary or introducer is based and the period of time that the framework has been in place;
- (c) the adequacy of the supervisory regime to combat money laundering and financing of terrorism to which the intermediary or introducer is subject;
- (d) the adequacy of the measures to combat money laundering and financing of terrorism in place at the intermediary or introducer;
- (e) previous experience gained from existing relationships connected with the intermediary or introducer;
- (f) the nature of the business conducted by the intermediary or introducer;
- (g) whether relationships are conducted by the intermediary or introducer on a face to face basis;
- (h) whether specific relationships are fully managed by an introducer;
- (i) the extent to which the intermediary or introducer itself relies on third parties to identify its customers and to hold evidence of identity or to conduct other due diligence procedures, and if so who those third parties are; and
- (j) whether or not specific intermediary or introduced relationships involve PEPs or other higher risk relationships.

(ix) Where, as a result of its risk assessment, a financial business determines that additional measures are necessary to mitigate the additional risk, these may include:

- (a) making specific enquiries of the intermediary or introducer to determine the adequacy of measures to combat money laundering and financing of terrorism in place;
- (b) reviewing the policies and procedures to combat money laundering and financing of terrorism in place at the intermediary or introducer;
- (c) requesting specific customer due diligence information and/or copy documentation to be provided, to confirm that the intermediary or introducer is able to satisfy any requirement for such information and documentation to be available without delay at the request of the financial business; and
- (d) where an intermediary or introduced relationship presents higher money laundering or financing terrorism risk, considering whether it is appropriate to rely solely upon the information provided by the intermediary or introducer, and whether additional customer due diligence information and/or documentation should be required.

Part 4 – Monitoring Customer Activity

The following guidance notes are in respect of regulation 28 of the Anti-Money Laundering and Prevention of Terrorist Financing Code.

Requirements of the AML/PTF Regulations concerning ongoing monitoring

- (i)* Regulation 11(3) of the AML/PTF Regulations requires a financial business to undertake ongoing monitoring of a business relationship. Ongoing monitoring is defined in regulation 5 of the Regulations as:
 - (a)* scrutinising transactions undertaken throughout the course of the relationship, including where necessary the source of funds, to ensure that the transactions are consistent with the financial business’s knowledge of the customer and his business and risk profile; and
 - (b)* keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up-to-date and relevant by undertaking reviews of existing records.

- (ii)* Regulation 28(1) of the Code requires a financial business to have policies systems and controls relating to ongoing monitoring that which provide for, amongst other things—
 - (a)* the identification and scrutiny of—
 - (I)* complex or unusually large transactions;
 - (II)* unusual patterns of transactions which have no apparent economic or visible lawful purpose; and
 - (III)* any other activity which the financial business regards as particularly likely by its nature to be related to the risk of money laundering or terrorist financing; and
 - (b)* determining whether—
 - (I)* a customer, any third party for whom the customer is acting and any beneficial owner of the customer or third party, is a politically exposed person;
 - (II)* a business relationship or transaction, or proposed business relationship or transaction, is with a person connected with a country that does not apply, or insufficiently applies, the FATF Recommendations or there is call to apply countermeasures by the FATF;
 - (III)* a business relationship or transaction, or proposed business relationship or transaction, is with a person connected with a country or territory that is subject to measures for purposes connected with the prevention and detection of money laundering or terrorist financing, imposed by one or more countries or sanctioned by the FATF, the European Union or the United Nations.

- (iii) Regulation 13(2) of the AML/PTF Regulations requires a financial business to undertake enhanced ongoing monitoring in the same circumstances as enhanced customer due diligence measures are required to be applied, i.e.—
- (a) where the customer has not been physically present for identification purposes;
 - (b) where the financial business has, or proposes to have, a business relationship with, or proposes to carry out an occasional transaction with, a person connected with a country or territory that does not apply, or insufficiently applies, the FATF recommendations or for which there is a call to apply enhanced or countermeasures by the FATF, UN or EU;
 - (c) where the financial business is a domestic bank that has or proposes to have a banking or similar relationship with an institution whose address for that purpose is outside the TCI;
 - (d) where the financial business has or proposes to have a business relationship with, or to carry out an occasional transaction with, a politically exposed person;
 - (e) where any of the following is a politically exposed person—
 - (I) a beneficial owner of the customer;
 - (II) a third party for whom a customer is acting;
 - (III) a beneficial owner of a third party described in subparagraph (II) above;
 - (IV) a person acting, or purporting to act, on behalf of the customer; and
 - (f) in any other situation which by its nature can present a higher risk of money laundering or terrorist financing.

Undertaking ongoing monitoring

- (iv) The principal objective of ongoing monitoring is to identify higher risk activity and business relationships so that money laundering and terrorist financing can be identified and, if possible, prevented.
- (v) The essentials of any monitoring systems and controls are that:
- (a) they flag up transactions and/or activities for further examination;
 - (b) ongoing monitoring reports are reviewed promptly by the right person(s); and
 - (c) appropriate action is taken on the findings of any further examination.
- (vi) Monitoring can either take place:
- (a) as transactions and/or activities take place or are about to take place, or
 - (b) after the event, through some independent review of the transactions and/or activities that a customer has undertaken, and in either case, unusual transactions or activities must be flagged for further examination.

- (vii) Monitoring may be by reference to specific types of transactions, to the profile of the customer, or by comparing their activity or profile with that of a similar peer group of customers or through a combination of these approaches.
- (viii) A financial business should also have systems and procedures to deal with customers who have not had contact with it for some time, in circumstances where regular contact might be expected, and with dormant accounts or relationships, to be able to identify future reactivation and unauthorized use.
- (ix) In designing monitoring systems and controls, it is important that appropriate account is taken of the frequency, volume and size of transactions with customers, in the context of the assessed customer and product risk.
- (x) Monitoring is not a mechanical process and does not necessarily require sophisticated electronic systems. Nevertheless, where a financial business has a substantial number of customers of a high level of transactions, an automated monitoring system may be effective. However, use of an automated monitoring system does not remove the requirement for a financial business to remain vigilant to the risk of money laundering or terrorist financing.

Part 5 – Reports to Financial Intelligence Agency

The following guidance notes are in respect of regulations 29-32 of the Anti-Money Laundering and Prevention of Terrorist Financing Code.

Introduction

- (i) POCO and the PTO contain disclosure requirements concerning knowledge or suspicion (or grounds for knowledge or suspicion) of money laundering or terrorist financing. Part 5 of the Code, and the Guidance that follows, is designed to outline and amplify the statutory disclosure requirements. The obligations to disclose are so important that they are set out in detail in this Guidance.

Statutory requirements (POCO)

- (ii) Section 127 of POCO requires a person to make a disclosure to the Financial Intelligence Agency or his MLRO if the person:
 - (a) knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering; and
 - (b) the information or other matter on which his knowledge or suspicion is based, or which gives reasonable grounds for such knowledge or suspicion, came to him in the course of a relevant business.

The information or other matter must be disclosed as soon as is practicable and in any event, within twenty-four hours after it comes to him.

(iii) It is beyond the scope of this Guidance to consider the money laundering offences themselves, but broadly, there are three:

- (a) concealing, disguising, converting, transferring and removing criminal property;
- (b) entering into or becoming concerned in an arrangement which a person knows or suspects facilitates, by whatever means, the acquisition, retention, use or control of criminal property by or on behalf of another person; and
- (c) acquisition, use or possession of criminal property.

It is essential that every financial business provides relevant staff with training concerning the money laundering offences.

(iv) Relevant business is the business of a financial business. In the circumstances, the obligation to disclose is imposed on any person where the information came to that person “in the course of the relevant business”. The disclosure requirements therefore apply to the financial business itself as well as directors and all employees of a financial business. The knowledge or suspicion may relate to any person, including the financial business itself. Therefore, if a financial business (or one of its employees) believes that the financial business may have, itself, committed a money laundering or terrorist financing offence, for example by becoming concerned in an arrangement facilitating money laundering or terrorist financing, a report must be made.

(v) All financial businesses are required by the AML/PTF Regulations to establish procedures for the reporting of disclosures. This applies both to internal reports, i.e. disclosure reports within the financial business to the MLRO and external report, i.e. disclosure reports to the Financial Intelligence Agency. An employee is expected to make a suspicious activity report (SAR) in accordance with the employer’s internal reporting procedures, not directly to the Financial Intelligence Agency. Provided an employee does this, the employee will not commit an offence under section 127 of POCO. Although the term “suspicious activity report” is used, the disclosure in the report could be one of knowledge, rather than suspicion.

(vi) The effect of section 123 of POCO is to require that the disclosure must be made before any actions are taken with respect to the business relationship or occasional transaction concerned, unless

- (a) the financial business has the consent, or the deemed consent, of the Financial Intelligence Agency; or

(b) the person who takes the action had good reason for his failure to make the disclosure before he took action concerning the business relationship or occasional transaction and the disclosure is made on his own initiative and as soon as it is practicable for him to make it afterwards.

(iii) A person who fails to make a report when required to do so, in accordance with section 120, commits an offence. As indicated above, an offence may be committed not just by the financial business but also by its employees.

Statutory requirements (terrorist financing disclosures)

(iii) There are several Orders that contain mandatory reporting requirements with respect to terrorist financing. These are:

Anti-terrorism (Financial and Other Measures) (Overseas Territories) Order 2002

Libya (Restrictive Measures) (Overseas Territories) Order 2011

The Afghanistan (United Nations Measures) (Overseas Territories) Order 2012

Syria (Restrictive Measures) (Overseas Territories) Order 2012

Zimbabwe (Sanctions) (Overseas Territories) Order 2012

Somalia (Sanctions) (Overseas Territories) Order 2012

Guinea-Bissau (Sanctions) (Overseas Territories) Order 2012

Eritrea (Sanctions) (Overseas Territories) Order 2012

Democratic People's Republic of Korea (Sanctions) (Overseas Territories) Order 2012

Guinea (Sanctions) (Overseas Territories) Order 2013

Burma (Sanctions) (Overseas Territories) Order 2013

Ukraine (Sanctions) (Overseas Territories) (No. 2) Order 2014

Ukraine (Sanctions) (Overseas Territories) (No. 3) Order 2014

Sudan (Sanctions) (Overseas Territories) Order 2014

South Sudan (Sanctions) (Overseas Territories) Order 2014

Central African Republic (Sanctions) (Overseas Territories) Order 2014

Russia, Crimea and Sevastopol (Sanctions) (Overseas Territories) Order 2014

Yemen (Sanctions) (Overseas Territories) (No.2) Order 2015

Democratic Republic of the Congo (Sanctions) (Overseas Territories) Order 2015

Burundi (Sanctions) (Overseas Territories) Order 2015

Iraq (Sanctions) (Overseas Territories) Order 2015

ISIL (Da'esh) and Al-Qaida (Sanctions) (Overseas Territories) Order 2016

Iran (Sanctions) (Overseas Territories) Order 2016

Mali (Sanctions) (Overseas Territories) Order 2017

Policing and Crime Act (Financial Sanctions) (Overseas Territories) Order 2017

Venezuela (Sanctions) (Overseas Territories) Order 2018

(ix) With respect to financial businesses and terrorist financing disclosures, the obligations in the above Orders are similar in effect to the money laundering disclosure obligations in POCO outlined above. A wider consideration of the Orders is beyond the scope of this Guidance. The Orders provide that a terrorist financing disclosure may be made to a "constable", but POCO enables the Financial Intelligence Agency to receive such disclosures and financial

businesses should ensure that terrorist financing disclosures are always made to the Financial Intelligence Agency rather than directly to a police officer.

Part VI – Employee Training and Awareness

The following guidance notes are in respect of regulation 33 of the Anti-Money Laundering and Prevention of Terrorist Financing Code.

Introduction

- (i)* The staff of a financial business, as its “eyes and ears”, are crucial to its efforts to prevent the financial business being used for the purposes of money laundering or terrorist financing. However, unless those employees that have access to information which may be relevant in determining whether any person is engaged in money laundering or terrorist financing are properly trained and understand how to recognize suspicious transactions and activities, they will not be in a position to fulfil this vital role.

- (ii)* The employees of a financial business must also understand and be able to apply the procedures, systems and controls that a financial business has put in place to prevent and detect money laundering and terrorist financing. If staff do not apply the procedures, systems and controls properly, they will not be effective, however well designed they may be. In particular, it is important that staff understand the risk-sensitive approach to the prevention of money laundering and terrorist financing.

- (iii)* It is, of course, also vital that staff are honest. One dishonest member of staff could cause substantial problems for a financial business. Put simply, the staff of a financial business may be either its greatest asset or its greatest liability in its efforts to prevent it being used for money laundering and terrorist financing.

- (iv)* It is for these reasons that the AMLR and the Code contain a number of requirements concerning staff training and awareness.

Statutory requirements

- (v)* Regulation 20 of the AML/PTF Regulations contains the following requirements with respect to training and employee awareness:

A financial business must take appropriate measures for the purposes of making employees whose duties relate to the provision of relevant business aware of—

- (a)* the anti-money laundering and counter-terrorist financing policies, procedures, systems and controls maintained by the financial business in accordance with these Regulations or an applicable Code;

- (b) the law of the TCI relating to money laundering and terrorist financing offences; and
 - (c) these Regulations, applicable Codes and any Guidance issued by the Commission or a supervisory authority.
- (vi) A financial business must provide employees specified in regulation 20(1) with training in the recognition and handling of—
- (a) transactions carried out by or on behalf of any person who is or appears to be engaged in money laundering or terrorist financing; and
 - (b) other conduct that indicates that a person is or appears to be engaged in money laundering or terrorist financing.
- (vii) Training is required to include the provision of information on current money laundering techniques, methods, trends and typologies.
- (viii) The requirements of the AML/CFT Regulations are supplemented by the Code.

Employees whose duties relate to the provision of relevant business

- (ix) The principal training obligations are in respect of employees whose duties relate to the provision of relevant business. When considering whether an employee falls within this criterion, a financial business should take the following into account:
- (a) whether the employee is undertaking any customer facing functions, or handles or is responsible for the handling of business relationships or transactions;
 - (b) whether the employee is directly supporting a colleague who carries out the above activity; and
 - (c) whether an employee’s role has changed to involve the above activities.
- (x) The directors and senior managers of a financial business should always be considered to fall within the criterion, whatever their roles.

Vetting of relevant employees

- (xi) The Code requires a financial business to vet the competence and probity of employees whose duties relate to the provision of relevant business at the time of their recruitment and at any subsequent change in role and that their competence and probity is subject to ongoing monitoring. As discussed above, it is vital that employees are honest. The most effective way of achieving this is for the financial business to vet and then to monitor its employees, particularly those subject to this requirement for competence and probity.

(xii) Whilst the most appropriate methods for vetting and monitoring employees is a matter for the judgment of each financial business, there are a number of obvious steps that may be taken, including:

- (a) obtaining and confirming references with respect to prospective new employees;
- (b) confirming the employment history and qualifications of prospective new employees;
- (c) requesting and verifying details of any regulatory action taken against the employee concerned;
- (d) requesting and verifying details of any criminal convictions.

Staff Awareness

(xiii) The requirements of the AML/PTF Regulations cover awareness and training. As indicated above, it is a statutory requirement that a financial business takes appropriate measures for the purpose of making all relevant employees aware of POCO, the AML/PTF Regulations, any applicable Code and any Guidance issued by the Financial Intelligence Agency, the Commission or a relevant supervisory body and the AML/PTF policies, procedures, systems and controls maintained by the financial business.

(xiv) In order to demonstrate compliance with the AML/PTF Regulations, a financial business is required to have measures in place to make employees aware of:

- (a) the AML/PTF procedures, systems and controls in place to prevent and detect money laundering and terrorist financing;
- (b) employees' potential personal liability (criminal, regulatory and disciplinary) for breaches of the statutory provisions and in particular for any failure to make a disclosure as required by section 127 of POCO;
- (c) potential implications to the financial business for any breaches of POCO, the AML/PTF Regulations and any applicable Code.

(xv) The design of appropriate awareness measures is a matter for each financial business to determine. However, such measures would usually include:

- (a) providing relevant employees with a copy of the AML/CFT procedures manual;
- (b) providing relevant employees with a document outlining the financial business's and their own obligations and potential criminal liability under POCO, the Terrorism Orders, the AML/PTF Regulations and any applicable Code;
- (c) requiring employees to acknowledge that they have received and understood the business' procedures manual and document outlining statutory obligations; and
- (d) periodically testing employees' awareness of policies and procedures and statutory obligations.

- (xvi) It should be noted that it is not sufficient simply to provide employees with copies of POCO, Prevention of Terrorism Ordinance, the Terrorism Orders, the AML/PTF Regulations and any applicable Codes. Given the risk-sensitive approach adopted by the TCI regime, every financial business will have to put in place its own systems and controls and procedures that are appropriate for its business.
- (xvii) Regulation 33(1)(a) of the Code requires basic AML/CFT awareness training to be provided to employees whose duties do not relate to the provision of relevant business. This will usually require the financial business, at a minimum to:
- (a) inform employees of the identity of the MLRO and the procedures to make internal suspicious activity reports;
 - (b) provide employees with a document outlining the financial business's and their own obligations and potential criminal liability under POCO, Prevention of Terrorism Ordinance, the Terrorism Orders and the AML/PTF Regulations and providing some basic information concerning this Code; and
 - (c) require employees to acknowledge that they have received and understood the business' procedures for making internal suspicious activity reports and the document outlining statutory obligations.
- (xviii) One-off awareness training should not be considered to be sufficient. It is important that staff, particularly employees whose duties relate to the provision of relevant business, are kept up to date with AML/CFT developments both in the TCI and internationally.

Staff training

- (xix) The AML/PTF Regulations require that a financial business must provide all employees whose duties relate to the provision of relevant business with appropriate training in the recognition and handling of transactions carried out by or on behalf of any person who is, or appears to be, engaged in money laundering. In order to demonstrate compliance with this, a financial business should consider including within its training to relevant employees training on:
- (a) the recognition and handling of unusual, complex, or higher risk activity and transactions, such as activity outside of the expected patterns, unusual settlements, abnormal payment or delivery instructions and changes in the patterns of business relationships;
 - (b) money laundering and terrorist financing trends and typologies;
 - (c) management of customer relationships which have been the subject of a suspicious activity report, e.g. risk of committing the offence of tipping off, and dealing with questions from such customers, and/or their adviser.
- (xx) Regulation 33(1)(d) of the Code requires a financial business to provide training, where appropriate, to the staff of any third parties fulfilling a function in relation to a financial business under an outsourcing agreement. A financial business should not enter into an

outsourcing agreement with a third party unless it is satisfied that the third party is suitably qualified and knowledgeable to undertake the outsourced work. The Anti Money Laundering Committee does not, therefore, expect that a financial business will need to provide basic money laundering training to the staff of third parties. However, some training may be appropriate. For example, staff of the third party may require training concerning the specific AML/CFT procedures of the financial business or concerning the specific AML/CFT risks that the financial business faces.

Monitoring the effectiveness of AML/CFT training

- (xxxi) Monitoring the effectiveness of AML/CFT training will usually require:
- (a) periodic testing of employees' understanding of the financial business's AML/CFT policies, procedures, systems and controls and their ability to recognise money laundering and terrorist financing activity;
 - (b) monitoring the compliance of employees with the AML/CFT systems and controls; and
 - (c) monitoring internal reporting patterns.

Part 7 – Record Keeping

The following guidance notes are in respect of regulations 34-40 of the Anti-Money Laundering and Prevention of Terrorist Financing Code.

Introduction

- (i) The principal reason for imposing record keeping requirements on financial businesses is to ensure that the law enforcement agencies in the TCI are not prevented from investigating and prosecuting money laundering and terrorist financing offences and investigating claims for the confiscation of the proceeds of crime and from assisting overseas law enforcement agencies in their investigations and prosecutions. If law enforcement agencies, either in the TCI or elsewhere, are unable to trace criminal property due to inadequate record keeping, then prosecution for money laundering, terrorist financing and the confiscation of criminal property may not be possible. If the funds used to finance terrorist activity cannot be traced back through the financial system, it will not be possible to identify the sources and the destination of terrorist funding.
- (ii) The AML/CFT Regulations therefore impose certain record keeping requirements on financial businesses. These are summarized in the following paragraphs.
- (iii) Financial businesses are required to keep:
 - (a) copies of evidence of identity, or information that enables a copy of the evidence to be obtained;

- (b) the supporting documents, data or information that have been obtained in respect of a business relationship or occasional transaction, which must include sufficient information to enable the reconstruction of individual transactions;
 - (c) a record containing details relating to each transaction carried out by the financial business in the course of any business relationship or occasional transaction.
- (iv) Records relating to transactions must include sufficient information to enable the reconstruction of individual transactions.
- (v) The AML/PTF Regulations also include requirements with respect to records to be kept when a financial business is relied on by another person and when the financial business is an introducer or an intermediary.
- (vi) Records must be kept for 5 years from the date on which an occasional transaction is completed or the business relationship ends, or in the case transaction records, 5 years from when the transaction is completed and for all other records, 5 years from the date on which the business relationship end, unless the Commission specifies a longer period.

Form of records

- (vii) The Code requires records to be kept in a manner that will enable them to be readily retrieved. In practice this will require that records are kept:
 - (a) by way of original documents;
 - (b) by way of copies of original documents, certified where appropriate;
 - (c) as computerized or other electronic data;
 - (d) as scanned documents; or
 - (e) using a combination of the above.

Part 8 – Correspondent Banking

The following guidance notes are in respect of regulations 41-43 of the Anti-Money Laundering and Prevention of Terrorist Financing Code.

- (i) Regulation 7(1) of the AML/PTF Regulations defines “correspondent banking” as meaning the provision of banking services by one bank, (the “correspondent bank”) to another bank (the “respondent bank”). The term has this meaning in Part 8 of the Code.

A correspondent banking relationship enables the respondent bank to provide its own customers with the cross-border products and services that it cannot provide them, with itself. In effect, the correspondent bank is an agent or intermediary for the respondent bank and provides services to the customers of the respondent bank. In most cases, TCI banks will be a respondent bank, rather than a correspondent bank.

(ii) Regulation 7(2) of the AML/PTF Regulations sets out a list of banking services included within the definition of correspondent banking as follows:

- (a) cash management, including establishing interest-bearing accounts in different currencies;
- (b) international wire transfers of funds;
- (c) cheque clearing;
- (d) payable-through accounts; and
- (e) foreign exchange services.

Correspondent banking services can also include facilitating securities transactions and other services.

(iii) As a correspondent bank will usually have no direct relationship with the customers of the respondent bank, it will not usually be possible for it to verify their identities. Correspondent banks also usually have limited information regarding the nature of the underlying transactions, particularly when processing wire transfers or clearing cheques. Correspondent banking must, therefore, be regarded as having a higher money laundering and terrorist financing risk attached to them.

(iv) Part 8 of the Code therefore specifies additional customer due diligence measures that must be applied to a correspondent banking relationship.

Payable through accounts

(v) A payable through account is an account through which a correspondent bank extends payment facilities or other services directly to the customers of the respondent bank.

(vi) Payable through accounts pose additional AML/CFT risks to the correspondent bank and the Code therefore imposes additional obligations with respect to such accounts.

Part 9 – Wire Transfers

The following guidance notes are in respect of regulation 44-46 of the Anti-Money Laundering and Prevention of Terrorist Financing Code.

Introduction

(i) The purpose of this Part of the Code is to give effect in the TCI to FATF Recommendation 16 concerning wire transfers.

(ii) Recommendation 16 was issued by the FATF with the objective of enhancing the transparency of electronic payment transfers (commonly referred to as “wire transfers”) of all types,

whether domestic or cross border, thereby making it easier for law enforcement agencies to track funds transferred electronically by money launderers, terrorists and other criminals.

- (iii) A number of countries have put codes, rules or regulations in place to give effect to the Recommendation. For example, in Europe, an EEC-wide Regulation came into effect on 1 January 2007. Although this Part of the Code ensures that the TCI continues to comply with international standards, compliance with Recommendation 16 is also important to the financial sector in the TCI because banks and payment service providers that fail to comply may in future find it difficult to send wire transfers to, or receive wire transfers from, countries that have given legal effect to Recommendation 16.
- (iv) In summary, this Part requires all payment service providers, as defined in the Code, to provide certain information in each wire transfer about the person who gives the instruction for the wire transfer to be made (the payer). Subject to a number of permitted exemptions and variations, the information must always include the name, address and account number of the payer.
- (v) However, the information does not have to be obtained and verified each time a customer requests a wire transfer; where the information had previously been obtained and verified and the entity effecting the transfer remains satisfied regarding the accuracy of the information on record, that information may be relied upon for subsequent transactions by the customer.
- (vi) The application of this Part of the Code is subject to certain specified exemptions. These exemptions are transfers that present a very low risk for money laundering and terrorist financing.

The following guidance notes are in respect of regulation 47 of the Anti-Money Laundering and Prevention of Terrorist Financing Code.

- (vii) One of the fundamental AML/CFT principles with respect to wire transfers, especially as they relate to cross-border batch transfers, is the timely provision of full originator information by the payment service provider of the payer to the payment service provider of the payee when so requested. While it is acceptable to rely on oral requests in circumstances where there is assurance that the requested information would be provided within the specified period of three days after the date of the request, it is advisable that such requests be documented; this is particularly important for enforcement purposes where a request is not complied with as provided under this Code. Similarly, where the Commission is notified of a failure to accede to a request within the specified period, the directives issued by the Commission must be reduced in writing. A record of regular or persistent breach on the part of a payment service provider of the payer should itself, where the payment service provider of the payer is

licensed by the Commission, be a serious cause for concern and for necessary action by the Commission against the payment service provider of the payer.

- (viii)* While routine batched wire transfers may not ordinarily present money laundering and terrorist financing risks, entities are required to adopt relevant measures to ensure that non-routine transactions are not batched in circumstances where doing so will or is likely to present such risks.

Dated the 7th day of August 2018.

Rhondalee Knowles
Attorney General
Chairman, Anti-Money Laundering Committee