The Joint Money Laundering Steering Group

Prevention of money laundering/ combating terrorist financing

2026 REVISED VERSION

GUIDANCE FOR THE UK FINANCIAL SECTOR

PART I

OCTOBER 2026

© JMLSG. All rights reserved.
For permission to copy please contact JMLSG.
Any reproduction, republication, transmission or reuse in whole or part requires our consent.

Draftsperson/Editor: Carol J. Smit

Contents

Paragraphs

Preface

Executive summary

Chapter 1 Senior management responsibility

Introduction 1.1-1.8
International AML/CFT standards and legislation 1.9-1.16
The UK legal and regulatory framework 1.17-1.24
General legal and regulatory obligations and expectations 1.25-1.27
Relationship between money laundering, terrorist financing and other financial crime 1.28
Obligations on all firms 1.29-1.32
Obligations on FCA-regulated firms subject to the Senior Manager Regime 1.33-1.34
Obligations on all FCA-regulated firms 1.35-1.48
Exemptions from legal and regulatory obligations 1.49-1.52
Senior management should adopt a formal policy, and carry out a risk assessment, in relation to financial crime prevention 1.53-1.59
Application of group policies outside the UK 1.60-1.64
Extra-territoriality of some overseas jurisdictions' regimes 1.65

Chapter 2 Internal controls

General legal and regulatory obligations 2.1-2.2
Appropriate controls in the context of financial crime prevention 2.3-2.4
Internal controls – specific requirements 2.5-2.15
Outsourcing and non-UK processing 2.16-2.21

Chapter 3 Nominated officer/MLRO

General legal and regulatory obligations
Legal obligations 3.1-3.3
Regulatory obligations 3.4-3.9
Standing of the MLRO 3.10-3.20
Internal and external reports 3.21-3.27
National and international findings in respect of countries and jurisdictions 3.28-3.32
Monitoring effectiveness of money laundering controls 3.33-3.36
Reporting to senior management 3.37-3.45
Reporting to the FCA 3.46-3.49

Chapter 4 Risk-based approach

Introduction and legal obligations
General 4.1-4.2
Risk assessment 4.3-4.5
Obligation to adopt a risk-based approach 4.6-4.10
Risk assessment – Identification and assessment of business risks 4.11-4.23
A risk-based approach - Design and implement controls to manage and mitigate the risks 4.24-4.32
A risk-based approach – customer risk assessments
General 4.33-4.36
Customer risk assessments 4.37-4.42
General principles – use of risk factors and categories 4.43-4.48

Weighting of risk factors *4.49-4.52*
Lower risk/simplified due diligence *4.53-4.58*
Higher risk/enhanced due diligence *4.59-4.69*
A risk-based approach - Monitor and improve the effective operation of the firm's controls *4.70-4.73*
A risk-based approach - Record appropriately what has been done and why *4.74-4.77*
Risk management is dynamic *4.78-4.82*

Annex 4-I – Considerations in assessing the level of ML/TF risk in different jurisdictions
Annex 4-II – Illustrative risk factors relating to customer situations
Annex 4-III – Considerations in keeping risk assessments up to date

Chapter 5 Customer due diligence

Meaning of customer due diligence measures and ongoing monitoring *5.1.1-5.1.4*
What is customer due diligence? *5.1.5-5.1.8*
What is ongoing monitoring? *5.1.9*
Why is it necessary to apply CDD measures and ongoing monitoring? *5.1.10-5.1.14*
Other material, pointing to good practice *5.1.15*
Timing of, and non-compliance with, CDD measures *5.2.1*
Timing of verification *5.2.2-5.2.5*
Requirement to cease transactions, etc *5.2.6-5.2.9*
Electronic transfer of funds *5.2.10-5.2.13*
Application of CDD measures *5.3.1*
Identification and verification of the customer *5.3.2-5.3.7*
Identification and verification of a beneficial owner *5.3.8-5.3.16*
Existing customers *5.3.17-5.3.20*
Acquisition of one financial services firm,or a portfolio of customers,by another *5.3.21-5.3.22*
Nature and purpose of proposed business relationship *5.3.23-5.3.26*
Keeping information up to date *5.3.27-5.3.28*
Characteristics and evidence of identity *5.3.29-5.3.35*
Documentary evidence *5.3.36-5.3.38*
Electronic evidence *5.3.39-5.3.45*
Nature of electronic checks *5.3.46-5.3.50*
Criteria for use of an electronic data provider *5.3.51-5.3.53*
Persons whom a firm should not accept as customers
Persons and entities subject to financial sanctions *5.3.54-5.3.62*
Illegal immigrants *5.3.63-5.3.65*
Shell banks and anonymous accounts *5.3.66-5.3.68*
Private individuals *5.3.69-5.3.70*
Obtain standard evidence
Identification *5.3.71*
Verification *5.3.72*
A- Documentary evidence *5.3.73-5.3.78*
B- Electronic evidence and Digital Identity *5.3.79-5.3.84*
C- Mitigation of impersonation risk *5.3.85-5.3.91*
Other considerations *5.3.92-5.3.94*
Executors and personal representatives *5.3.95-5.3.96*
Court of Protection orders and court-appointed deputies *5.3.97-5.3.98*
Attorneys *5.3.99-5.3.101*
Source of funds as evidence *5.3.102-5.3.107*
Customers who cannot provide the standard evidence *5.3.108-5.3.114*
Persons without standard documents, in care homes, or in receipt of pension *5.3.115*
Those without the capacity to manage their financial affairs *5.3.116*
Gender re-assignment *5.3.117*
Students and young people *5.3.118-5.3.120*
Financially excluded *5.3.121-5.3.125*
Customers other than private individuals *5.3.126-5.3.132*
Regulated financial services firms subject to the ML Regulations (or equivalent) *5.3.133-5.3.138*

Other firms that are subject to the ML Regulations (or equivalent) 5.3.139-5.3.142
Corporate customers (other than regulated firms) 5.3.143-5.3.150
Obtain standard evidence 5.3.151-5.3.154
Companies listed on regulated markets (EEA or equivalent) 5.3.155-5.3.159
Other publicly listed or quoted companies 5.3.160-5.3.162
Private and unlisted companies 5.3.163-5.3.168
Directors 5.3.169
Beneficial owners 5.3.170
Signatories 5.3.171
Other considerations 5.3.172-5.3.174
Bearer shares 5.3.175-5.3.176
Partnerships and unincorporated businesses 5.3.177-5.3.178
Obtain standard evidence 5.3.179-5.3.186
Other considerations 5.3.187-5.3.190
Principals and owners 5.3.191
Public sector bodies, Governments, state-owned companies and supranationals (other than sovereign wealth funds) 5.3.192-5.3.193
Obtain standard evidence 5.3.194-5.3.197
Signatories 5.3.198
Schools, colleges and universities 5.3.199-5.3.200
Other considerations 5.3.201-5.3.203
Sovereign wealth funds 5.3.204-5.3.210
Nature and legal form 5.3.211
Obtain standard evidence 5.3.212-5.3.218
Beneficial ownership 5.3.219
Nature and purpose 5.3.220-5.3.225
Other considerations 5.3.226-5.3.227
Pension schemes 5.3.228-5.3.231
Obtain standard evidence 5.3.232-5.3.233
Signatories 5.3.234
Other considerations 5.3.235
Payment of benefits 5.3.236-5.3.237
Charities, church bodies and places of worship 5.3.238-5.3.245
Obtain standard evidence 5.3.246-5.3.247
Registered charities – England and Wales, and Scotland 5.3.248-5.3.249
Charities in Northern Ireland 5.3.250
Church bodies and places of worship 5.3.251
Unregistered charities or church bodies 5.3.252
Independent schools and colleges 5.3.253-5.3.254
Other considerations 5.3.255-5.3.257
Other trusts and foundations 5.3.258-5.3.266
Obtain standard evidence 5.3.267-5.3.268
Beneficial owners 5.3.269-5.3.273
Other considerations 5.3.274-5.3.276
Non-UK trusts and foundations 5.3.277-5.3.282
Clubs and societies 5.3.283-5.3.286
Obtain standard evidence 5.3.287-5.3.290
Other considerations 5.3.291-5.3.293
Simplified due diligence 5.4.1-5.4.10
Enhanced due diligence 5.5.1-5.5.12
Politically exposed persons 5.5.13-5.5.23
Risk based procedures 5.5.24-5.5.28
Source of wealth 5.5.29-5.5.32
Senior management approval 5.5.33-5.5.34
On-going monitoring 5.5.35-5.5.36
Multipartite relationships, including reliance on third parties 5.6.1-5.6.3
Reliance on third parties 5.6.4-5.6.9
Basis of reliance 5.6.10-5.6.23
Group introductions 5.6.24-5.6.27
Use of pro forma confirmations 5.6.28-5.6.30

Situations which are not reliance
One firm acting solely as introducer *5.6.31-5.6.32*
Where the intermediary is the agent of the product/service provider *5.6.33-5.6.34*
Where the intermediary is the agent of the customer *5.6.35-5.6.40*
Monitoring customer activity
The requirement to monitor customer activities *5.7.1-5.7.2*
What is monitoring? *5.7.3-5.7.8A*
Nature of monitoring *5.7.9-5.7.12*
Manual or automated? *5.7.13-5.7.21*

Annexes 5-I/1- 5II/2 - Pro-forma confirmations of identity
Annexes 5-III/IV – Risk factor guidelines
Annex 5-V – Pooled Client Accounts

Chapter 6 Suspicious activities, reporting and data protection

General legal and regulatory obligations *6.1-6.9*
What is meant by 'knowledge' and 'suspicion'? *6.10-6.14*
What is meant by 'reasonable grounds to know or suspect'? *6.15-6.17*
Internal reporting *6.18-6.24*
Non-UK offences *6.25-6.28*
Evaluation and determination by the nominated officer *6.29-6.32*
External reporting *6.33-6.39*
Where to report *6.40-6.42*
Sanctions and penalties *6.43-6.44*
Consent *6.45*
Consent under POCA *6.46-6.50*
Consent under Terrorism Act *6.51-6.55*
General *6.56-6.59*
Tipping off, and prejudicing an investigation *6.60-6.62*
Permitted disclosures *6.63-6.71*
Transactions following a disclosure *6.72-6.82*
Constructive trusts *6.83-6.89*
Data protection – subject access requests, where a suspicion report has been made *6.90-6.99*

Chapter 7 Staff awareness, training and alertness

Why focus on staff awareness and training? *7.1-7.4*
General legal and regulatory obligations *7.5-7.15*
Responsibilities of the firm, and its staff
Responsibilities of senior management *7.16.7.22*
Responsibilities of staff *7.23-7.24*
Legal obligations on staff *7.25-7.28*
Training in the firm's procedures *7.29-7.31*
Staff alertness to specific situations *7.32-7.40*
Staff based outside the UK *7.41*
Training methods and assessment *7.42-7.45*

Chapter 8 Record keeping

General legal and regulatory obligations *8.1-8.5*
What records have to be kept? *8.6-8.7*
Customer information *8.8-8.16*
Transactions *8.17-8.20*
Internal and external reports *8.21-8.23*
Other *8.24-8.25*
Form in which records have to be kept *8.26-8.28*
Location *8.29-8.33*
Sanctions and penalties *8.34*

Glossary of terms

Appendix I – Anti-money laundering responsibilities in the UK

Appendix II – Summary of UK legislation

Proceeds of Crime Act 2002 (as amended)
Terrorism Act 2000, and the Anti-terrorism, Crime and Security Act 2001
Counter-Terrorism Act 2008, Schedule 7
Financial sanctions
Money Laundering Regulations 2017 (as amended)
FCA regulated firms – the FCA Handbook

PREFACE

1. In the UK, there has been a long-standing obligation to have effective procedures in place to detect and prevent money laundering. The UK Money Laundering Regulations, applying to financial institutions, date from 1993, the current Regulations being those of 2017 (as amended). The offence of money laundering was contained in various acts of parliament (such as the Criminal Justice Act 1988 and the Drug Trafficking Offences Act 1986). The Proceeds of Crime Act 2002 (POCA) consolidated, updated and reformed the law relating to money laundering to include any dealing in criminal property. Specific obligations to combat terrorist financing were set out in the Terrorism Act 2000. Many of the procedures which will be appropriate to address these obligations are similar, and firms can often employ the same systems and controls to meet them.

Purpose of the guidance

2. The purpose of this guidance is to:

   - outline the legal and regulatory framework for anti-money laundering/countering terrorist financing (AML/CTF) requirements and systems across the financial services sector;
   - interpret the requirements of the relevant law and regulations, and how they may be implemented in practice;
   - indicate good industry practice in AML/CTF procedures through a proportionate, risk-based approach; and
   - assist firms to design and implement the systems and controls necessary to mitigate the risks of the firm being used in connection with money laundering and the financing of terrorism.

Scope of the guidance

3. This guidance sets out what is expected of firms and their staff in relation to the prevention of money laundering and terrorist financing, but allows them some discretion as to how they apply the requirements of the UK AML/CTF regime in the particular circumstances of the firm, and its products, services, transactions and customers.

4. This guidance relates solely to how firms should fulfil their obligations under the AML/CTF law and regulations. It is important that customers understand that production of the required evidence of identity does not automatically qualify them for access to the product or service they may be seeking; firms bring to bear other, commercial considerations in deciding whether particular customers should be taken on.

What is the offence of money laundering?

5. Money laundering takes many forms, including:

   - trying to turn money raised through criminal activity into 'clean' money (that is, classic money laundering);
   - handling the benefit of acquisitive crimes such as theft, fraud and tax evasion;
   - handling stolen goods;
   - being directly involved with any criminal or terrorist property, or entering into arrangements to facilitate the laundering of criminal or terrorist property; and
   - criminals investing the proceeds of their crimes in the whole range of financial products.

6. The techniques used by money launderers constantly evolve to match the source and amount of funds to be laundered, and the legislative/regulatory/law enforcement environment of the market in which the money launderer wishes to operate.

7. There are three broad groups of offences related to money laundering that firms need to avoid committing. These are:

- knowingly assisting (in a number of specified ways) in concealing, or entering into arrangements for the acquisition, use, and/or possession of, criminal property;
- failing to report knowledge, suspicion, or where there are reasonable grounds for knowing or suspecting, that another person is engaged in money laundering; and
- tipping off, or prejudicing an investigation.

8. It is also a separate offence under the ML Regulations not to establish adequate and appropriate policies and procedures in place to forestall and prevent money laundering (regardless of whether or not money laundering actually takes place).

The guidance also covers terrorist financing

9. There can be considerable similarities between the movement of terrorist property and the laundering of criminal property: some terrorist groups are known to have well established links with organised criminal activity. However, there are two major differences between terrorist property and criminal property more generally:

- often only small amounts are required to commit individual terrorist acts, thus increasing the difficulty of tracking the terrorist property;
- terrorists can be funded from legitimately obtained income, and it is extremely difficult to identify the stage at which legitimate funds become terrorist property.

10. Terrorist organisations can, however, require quite significant funding and property to resource their infrastructure. They often control property and funds from a variety of sources and employ modern techniques to manage these funds, and to move them between jurisdictions.

11. In combating terrorist financing, the obligation on firms is to report any suspicious activity to the authorities. This supports the aims of the law enforcement agencies in relation to the financing of terrorism, by allowing the seizure and/or freezing of property where there are grounds for suspecting that such property could be used to finance terrorist activity, and depriving terrorists of this property as and when links are established between the property and terrorists or terrorist activity.

What about other financial crime?

12. Money laundering and terrorist financing risks are closely related to the risks of other financial crime, such as fraud. Fraud and market abuse, as separate offences, are not dealt with in this guidance. The guidance does, however, apply to dealing with any proceeds of crime that arise from these activities.

13. Firms increasingly look at fraud and money laundering as part of an overall strategy to tackle financial crime, and there are many similarities – as well as differences - between procedures to tackle the two. When considering money laundering and terrorist financing issues, firms should consider their procedures against fraud and market abuse and how these might reinforce each other. Where responsibilities are given to different departments, there will need to be strong links between those in the firm responsible for managing and reporting on these various areas of risk. When

measures involving the public are taken specifically as an anti-fraud measure, the distinction should be made clear.

Who is the guidance addressed to?

14. The guidance prepared by JMLSG is addressed to firms in the industry sectors represented by its member bodies (listed at paragraph 30 below), and to those firms regulated by the FCA. All such firms – which, for the avoidance of doubt, include those which are members of JMLSG trade associations but not regulated by the FCA - should have regard to the contents of the guidance.

15. Financial services firms which are neither members of JMLSG trade associations nor regulated by the FCA may choose to have regard to this guidance as industry good practice. Firms which are outside the financial sector, but subject to the ML Regulations, particularly where no specific guidance is issued to them by a body representing their industry, may also find this guidance helpful.

16. The guidance will be of direct relevance to senior management, nominated officers and MLROs in the financial services industry. The purpose is to give guidance to those who set the firm's risk management policies and its procedures for preventing money laundering and terrorist financing. Although the guidance will be relevant to operational areas, it is expected that these areas will be guided by the firm's own, often more detailed and more specific, internal arrangements, tailored by senior management, nominated officers and MLROs to reflect the risk profile of the firm.

How should the guidance be used?

17. The guidance gives firms a degree of discretion in how they comply with AML/CTF legislation and regulation, and on the procedures that they put in place for this purpose.

18. It is not intended that the guidance be applied unthinkingly, as a checklist of steps to take. Firms should encourage their staff to 'think risk' as they carry out their duties within the legal and regulatory framework governing AML/CTF. The FCA has made clear its expectation that FCA-regulated firms address their management of risk in a thoughtful and considered way, and establish and maintain systems and procedures that are appropriate, and proportionate to the risks identified. This guidance assists firms to do this.

19. When provisions of the statutory requirements and of FCA's regulatory requirements are directly described in the text of the guidance, it uses the term 'must', indicating that these provisions are mandatory. In other cases, the guidance uses the term 'should' to indicate ways in which the statutory and regulatory requirements may be satisfied, but allowing for alternative means of meeting the requirements. References to 'must' and 'should' in the text should therefore be construed accordingly.

20. Many defined terms and abbreviations are used in the guidance; these are highlighted, and their meanings are explained in the Glossary.

The content of the guidance

21. This guidance emphasises the responsibility of senior management to manage the firm's money laundering and terrorist financing risks, and how this should be carried out on a risk-based approach. It sets out a standard approach to the identification and verification of customers, separating out basic identity from other aspects of customer due diligence measures, as well as giving guidance on the obligation to monitor customer activity.

22. The guidance incorporates a range of reference material which it is hoped that senior management, nominated officers and MLROs will find helpful in appreciating the overall context of, and obligations within, the UK AML/CTF framework.

23. The guidance provided by the JMLSG is in a number of parts. The main text in Part I contains generic guidance that applies across the UK financial sector. Part II provides guidance for a number of specific industry sectors, supplementing the generic guidance contained in Part I. Part III provides additional guidance on a number of specific areas of activity.

24. Part I comprises eight separate chapters, followed by a Glossary of terms and abbreviations, and a number of appendices setting out other generally applicable material. Some of the individual chapters are followed by annexes specific to the material covered in that chapter.

25. Part I sets out industry guidance on:

- the importance of senior management taking responsibility for effectively managing the money laundering and terrorist financing risks faced by the firm's businesses (Chapter 1);
- appropriate controls in the context of financial crime (Chapter 2);
- the role and responsibilities of the nominated officer and the MLRO (Chapter 3);
- adopting a risk-based approach to the application of CDD measures (Chapter 4);
- helping a firm have confidence that it has properly carried out its CDD obligations, including monitoring customer transactions and activity (Chapter 5);
- the identification and reporting of suspicious activity (Chapter 6);
- staff awareness, training and alertness (Chapter 7);
- record keeping (Chapter 8).

26. Parts II and III of the guidance comprises the sector specific additional material, which has been principally prepared by practitioners in the relevant sectors. The sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the guidance.

Status of the guidance

27. POCA requires a court to take account of industry guidance that has been approved by a Treasury minister when considering whether a person within the regulated sector has committed the offence of failing to report where that person knows, suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering. Similarly, the Terrorism Act requires a court to take account of such approved industry guidance when considering whether a person within the financial sector has failed to report under that Act. The ML Regulations also provide that a court must decide whether similar industry guidance was followed in determining whether a person or institution within the regulated sector has complied with any of the requirements of the ML Regulations.

28. The FCA Handbook also confirms that the FCA will have regard to whether a firm has followed relevant provisions of this guidance when:

- Considering whether to take action against an FCA-regulated firm in respect of a breach of the relevant provisions in SYSC (see SYSC 3.2, SYSC 5.3, and DEPP 6.2.3); and
- Considering whether to prosecute a breach of the Money Laundering Regulations (see EG 12.1).

29. The guidance therefore provides a sound basis for firms to meet their legislative and regulatory obligations when tailored by firms to their particular business risk profile. Departures from this guidance, and the rationale for so doing, should be documented, and firms will have to stand prepared to justify departures, for example to the FCA.

Who are the members of JMLSG?

30. The members of JMLSG are:

Association of British Credit Unions (ABCUL)
Association of British Insurers (ABI)
Association for Financial Markets in Europe (AFME)
Association of Foreign Banks (AFB)
Building Societies Association (BSA)
Electronic Money Association (EMA)
European Values & Intermediaries Association (EVIA)
Finance & Leasing Association (FLA)
The Investment Association (IA)
Loan Market Association (LMA)
Personal Investment Management & Financial Advice Association (PIMFA)
The Investing and Savings Alliance (TISA)
UK Finance (UKF)
UK Private Capital

CHAPTER 1

SENIOR MANAGEMENT RESPONSIBILITY AND GOVERNANCE

- **International recommendations and authorities**
  - FATF Recommendations (February 2012)
  - UN Security Council Resolutions 1267 (1999), 1373 (2001) and 1390 (2002)
- **International regulatory pronouncements**
  - Basel paper – *Sound management of risks related to money laundering and financing of terrorism* (updated July 2020)
  - IAIS Guidance Paper 5
  - IOSCO Principles paper
- **EU Directives**
  - Fourth Money Laundering Directive 2015/849 (as amended by 2018/843)
- **EU Regulations**
  - EC Regulation 2580/2001
  - EC Regulation 847/2015 (the Wire Transfer Regulation)
- **UK framework**
  - Legislation
    - FSMA 2000 (as amended)
    - Proceeds of Crime Act 2002 (as amended)
    - Terrorism Act 2000 (as amended by the Anti-terrorism, Crime and Security Act 2001)
    - Money Laundering Regulations 2017 (as amended)
    - Counter-terrorism Act 2008, Schedule 7
  - Financial Sanctions
    - HM Treasury Sanctions Notices and News Releases
  - Regulatory regime
    - FCA Handbook –APER, COND, DEPP, PRIN, and SYSC
    - FCA Financial Crime Guide
    - FCA PEPs Guidance
  - Industry guidance
- **Other matters**
  - Extra-territoriality of some overseas jurisdictions' regimes
- **Core obligations**
  - Senior management in all firms must:
    - identify, assess, and manage effectively, the risks in their businesses
    - if in the regulated sector, appoint a nominated officer to process disclosures
  - Senior management in FCA-regulated firms must appoint individual(s) (including an MLRO) with certain responsibilities
  - Adequate resources must be devoted to AML/CTF
  - Potential personal liability if legal obligations not met
- **Actions required, to be kept under regular review**
  - Prepare a formal policy statement in relation to the prevention, and risk assessment of, money laundering/terrorist financing
  - Ensure adequate resources devoted to AML/CTF
  - Commission annual report from the MLRO and take any necessary action to remedy deficiencies identified by the report in a timely manner

Introduction

SYSC 3.1.1 R, 6.1.1 R 6.3.1 R	1.1	Being used for money laundering or terrorist financing involves firms in reputational, legal and regulatory risks. Senior management has a responsibility to ensure that the firm's policies, controls and procedures are appropriately designed and implemented, and are effectively operated to reduce the risk of the firm being used in connection with money laundering or terrorist financing.
Regulation 18	1.2	The ML Regulations require firms to take appropriate steps to identify and assess the risks of money laundering and terrorist financing to which their business is subject, taking into account: ➢ information on money laundering and terrorist financing made available to them by the FCA; ➢ risk factors, including factors relating to their customers, countries or geographic areas in which they operate, products, services, transactions and delivery channels. In considering what steps are appropriate, firms must take into account the size and nature of its business.
Regulation 16(2)	1.3	The assessment should be informed by relevant findings in the National Risk Assessment.
	1.4	Senior management in financial firms is accustomed to applying proportionate, risk-based policies across different aspects of its business. A firm must take such an approach to the risk of being used for the purposes of money laundering or terrorist financing.
	1.5	Under a risk-based approach, firms start from the premise that most customers are not money launderers or terrorist financiers. However, firms must have systems in place to highlight those customers who, on criteria established by the firm, may indicate that they present a higher risk of this.
Regulation 3(1) 19(2)(b)	1.6	Senior management must be fully engaged in the decision-making processes, and must take ownership of the risk-based approach, since they will be held accountable if the approach is inadequate. Senior management approval is specifically required for the firm's policies, controls and procedures for mitigating and managing effectively the risks of money laundering and terrorist financing identified in the firm's risk assessment. Such policies, controls and procedures must be kept up-to-date, and should reflect changes in the money laundering and/or terrorist financing risks faced by a firm.
Regulation 21(1)(a)	1.7	Where appropriate with regard to the size and nature of its business, a firm must appoint a member of its board of directors (or equivalent management body) or of its senior management as the officer responsible for the firm's compliance with the ML Regulations.

1.8 Senior management must be aware of the level of money laundering risk the firm is exposed to and take a view whether the firm is equipped to mitigate that risk effectively; this implies that decisions on entering or maintaining high-risk business relationships must be escalated to senior management. That said, provided the assessment of the risks has been approached in a considered way, the selection of risk mitigation procedures is appropriate, all the relevant decisions are properly recorded, and the firm's policies, controls and procedures are followed and applied effectively, the risk of censure by the regulator should be minimised.

International AML/CTF standards and legislation

1.9 Governments across the world are increasingly enacting legislation to make money laundering and terrorist financing criminal offences, and putting legal and regulatory processes in place to enable those engaged in these activities to be identified and prosecuted.

1.10 FATF issue International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation (the FATF Recommendations), aimed at setting minimum standards for action in different countries, to ensure that AML/CTF efforts are consistent internationally. The text of the FATF Recommendations is available at www.fatf-gafi.org. FATF also maintains an International Co-operation Review Group (ICRG) and publishes a regularly updated list of those countries and jurisdictions that have strategic deficiencies and works with them to address those deficiencies that pose a risk to the international financial system.

1.11 European legislation provided a common legal basis for the implementation of the FATF Recommendations, including supporting guidance, by Member States. An EU Directive was targeted at money laundering prevention, and was implemented in the UK, mainly through the Money Laundering Regulations 2017, to implement the revised FATF Standards which were published in February 2012.

1.12 In terms of the ML Regulations, a FATF call for action country is a country named on the list of High-Risk Jurisdictions subject to a Call for Action, as published by FAFT from time to time. This list identifies high-risk jurisdictions with serious strategic deficiencies in the areas of anti-money laundering, counter terrorist financing or counter proliferation financing.

See also https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html

1.13 The extent of ML/TF risk associated with individual countries may also be assessed through other sources, for example, HM Treasury

Sanctions[1], FATF high-risk and non-cooperative jurisdictions[2], FATF Mutual Evaluation Reports, Transparency International Corruption Perceptions Index[3], FCDO Human Rights Report[4], and Department for International Trade overseas country risks[5].

1.14 Internationally, the FATF Recommendations, the Basel paper *Sound management of risks related to money laundering and financing of terrorism* (www.bis.org), IAIS Guidance Paper 5 (www.iaisweb.org) and the IOSCO Principles paper (www.iosco.org) encourage national supervisors of financial firms to require firms in their jurisdictions to follow specific due diligence procedures in relation to customers. These organisations explicitly envisage a risk-based approach to AML/CTF being followed by firms.

1.15 The United Nations and the EU have sanctions in place to deny a range of named individuals and organisations, as well as nationals from certain countries, access to the financial services sector. In the UK, HM Treasury (through the Office for Financial Sanctions Implementation) issues sanctions notices whenever a new name is added to the list, or when any details are amended.

1.16 Some international groupings, official or informal, publish material that may be useful as context and background in informing firms' approaches to AML/TF. These groupings include Transparency International (www.transparency.org.uk) and the Wolfsberg Group (www.wolfsberg-principles.com).

The UK legal and regulatory framework

1.17 The UK approach to fighting financial crime is based on a partnership between the public and private sectors. Objectives are specified in legislation and in the FCA Rules, but there is usually no prescription about how these objectives must be met. Often, the objective itself would have been a requirement of an EU Directive, incorporated into UK law without any further elaboration, leaving UK businesses with a degree of discretion in interpreting how it should be met.

1.18 Key elements of the UK AML/CTF framework are:

- Proceeds of Crime Act 2002 (as amended);
- Terrorism Act 2000 (as amended by the Anti-terrorism, Crime and Security Act 2001);
- The Counter-Terrorism (Sanctions) (EU Exit) Regulations 2019
- Money Laundering Regulations 2017 (as amended);
- Counter-terrorism Act 2008, Schedule 7
- HM Treasury Sanctions Notices, Guidance and News Releases; and
- FCA Handbook.

[1] https://www.gov.uk/government/publications/the-uk-sanctions-list
[2] http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/
[3] http://cpi.transparency.org/cpi2013/results/
[4] https://www.gov.uk/government/collections/human-rights-and-democracy-reports
[5] https://www.gov.uk/government/collections/overseas-business-risk

1.19 Implementation guidance for the financial services industry is provided by JMLSG.

1.20 In view of the nature of the risks associated with financial crime, multiple UK bodies share responsibility for combating money laundering and terrorist financing. Responsibilities are set out in Appendix I. In its capacities as a supervisory authority and a law enforcement authority HMRC may use the UK anti-money laundering regime to gather information for tax purposes.

Regulation 8(1),(2)

1.21 The ML Regulations apply to a range of specified firms undertaking business in the UK. POCA and the Terrorism Act consolidated, updated and reformed the scope of UK AML/CTF legislation to apply it to any dealings in criminal or terrorist property. The UK financial sanctions regime imposes additional obligations on firms. Thus, in considering their statutory obligations, firms need to think in terms of involvement with any crime or terrorist activity.

Serious and Organised Crime Strategy, October 2013

1.22 Firms should be aware of the Home Office's *Serious and Organised Crime Strategy*, issued in October 2013[6].

The strategy uses the framework developed for counter-terrorist work and has four components:

- prosecuting and disrupting people engaged in serious and organised crime (PURSUE);
- preventing people from engaging in this activity (PREVENT);
- increasing protection against serious and organised crime (PROTECT); and
- reducing the impact of this criminality where it takes place (PREPARE).

Action Plan for anti-money laundering and counter-terrorist finance, April 2016

1.23 In order to deliver these objectives successfully, the government believes action in this area must be underpinned by four priority areas, set out in the Action Plan for anti-money laundering and counter-terrorist finance, published in April 2016[7]:

- **A stronger partnership with the private sector**

Law enforcement agencies, supervisors and the private sector working in partnership to target resources at the highest money laundering and terrorist financing risks.

New means of information sharing to strengthen the application of the risk-based approach and mitigate vulnerabilities.

A collaborative approach to preventing individuals becoming involved in money laundering.

---

[6] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf

[7] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/517992/6-2118-Action_Plan_for_Anti-Money_Laundering__web_.pdf

- **Enhancing the law enforcement response**

New capabilities and new legal powers to build the intelligence picture, disrupt money launderers and terrorists, recover criminal proceeds, and protect the integrity of the UK's financial system.

- **Improving the effectiveness of the supervisory regime**

Investigate the effectiveness of the current supervisory regime, and consider radical options for improvement to ensure that a risk-based approach is fully embedded, beginning with the understanding of specific risks, and the spotting of criminal activity, rather than a focus on tick-box compliance.

- **Increasing our international reach**

Increase the international reach of law enforcement agencies and international information sharing to tackle money laundering and terrorist financing threats.

1.24 HM Treasury and the Home Office jointly published the first UK national risk assessment (NRA) of money laundering and terrorist financing in October 2015, the second in 2017, the third in 2020, and the fourth in July 2025*.

General legal and regulatory obligations and expectations

Regulation 19 POCA ss327-330 Terrorism Act ss18, 21A

1.25 Senior management of any enterprise is responsible for managing its business effectively. Certain obligations are placed on all firms subject to the ML Regulations, POCA and the Terrorism Act and under the UK financial sanctions regimes - fulfilling these responsibilities falls to senior management as a whole. These obligations are summarised in Appendix II.

SYSC

1.26 For FCA-regulated firms the specific responsibilities, and the FCA's obligations and expectations, of senior management are set out in FSMA and the FCA Handbook. These responsibilities and obligations are outlined in Appendix II.

1.27 Following the completion of thematic and other reviews, the FCA may clarify their expectations of firms in the relevant areas; firms should be aware of these expectations. The FCA has also issued a publication "*Financial Crime Guide: A firm's guide to countering financial crime risks*" (FCG), which provides practical assistance and information for firms on FCA's expectations of actions they can take to counter the risk that they might be used to further financial crime. This guide includes

*https://assets.publishing.service.gov.uk/media/6877be59760bf6cedaf5bd4f/National_Risk_Assessment_of_Money_Laundering_and_Terrorist_Financing_2025_FINAL.pdf

consolidated examples of the good and poor practice published with FCA thematic reviews.

Relationship between money laundering, terrorist financing and other financial crime

Regulations 19(2), 21(1)(a)

1.28 From a practical perspective, firms must consider how best they should assess and manage their overall exposure to financial crime. This does not mean that fraud, market abuse, money laundering and terrorism financing prevention, and financial sanctions obligations, must be addressed by a single function within a firm; there will, however, need to be close liaison between those responsible for each activity. This guidance relates only to the prevention of money laundering and terrorism financing.

Obligations on all firms

Regulations 19 and 86

1.29 The ML Regulations place a general obligation on firms within their scope to establish adequate and appropriate policies, controls and procedures to prevent money laundering and terrorist financing. Failure to comply with this obligation risks a prison term of up to two years and/or a fine. Depending on the nature and extent of any such failure, it may also attract regulatory sanction.

Regulation 21(1)(a)

1.30 Where appropriate with regard to the size and nature of its business, a firm must appoint a member of its board of directors (or equivalent management body) or of its senior management as the officer responsible for the firm's compliance with the ML Regulations.

Regulation 92

1.31 In addition to imposing liability on firms, the ML Regulations impose criminal liability on certain individuals in firms subject to the ML Regulations. Where the firm is a body corporate, an officer of that body corporate (i.e., a director, manager, secretary, chief executive, member of the committee of management, or a person purporting to act in such a capacity), who consents or connives in the commission of an offence by the firm, or where that offence (by the firm) is attributable to the lack of supervision or control on his part, himself commits a criminal offence and may be prosecuted. Similarly, where the firm is a partnership, a partner who consents to or connives in the commission of offences under the ML Regulations, or where the commission of any such offence is attributable to any neglect on his part, will be individually liable to be prosecuted for the offence. A similar rule applies to officers of unincorporated associations.

POCA ss 327-330
Terrorism Act s 21A
Regulation 24

1.32 The offences of money laundering under POCA, and the obligation to report knowledge or suspicion of possible money laundering, affect members of staff of firms. The similar offences and obligations under the Terrorism Act also affect members of staff. However, firms have an obligation under the ML Regulations to take appropriate measures to ensure that their employees and agents are made aware of the law relating to money laundering, and terrorist financing (and to data protection), and are regularly given training in how to recognise and deal with transactions and other activities which may be related to money laundering or terrorist financing. Guidance on meeting obligations in relation to staff training is given in Chapter 7.

Obligations on FCA-regulated firms subject to the Senior Managers and Certification Regime

SYSC 4.5.4 R
SYSC 25.2.1 R
SYSC 25.4.14 G

1.33 Under the SMCR, deposit takers, insurers and investment banks are required to maintain a Management Responsibilities Map, which allocates prescribed responsibilities to individual SMF Managers. The management responsibility map of a small and non-complex firm is likely to be simple and short, possibly no more than a single sheet of paper.

SYSC 24.3.9 G

1.34 One prescribed responsibility - for the firm's policies and procedures for countering the risk that the firm might be used to further financial crime - must be allocated to an SMF Manager. The firm may allocate this responsibility to the MLRO, but does not have to. If it is allocated to another SMF Manager, this prescribed responsibility includes responsibility for supervision of the MLRO.

Obligations on all FCA-regulated firms

1.35 A number of the financial sector firms regulated by the FCA are so-called 'common platform' firms, because they are subject both to MiFID and to the Capital Requirements Directive. The FCA Rules relating to systems and controls to prevent firms being used in connection with the commission of financial crime are in two parts: those which apply to most firms, set out in SYSC 6.1.1, and those which apply to non-common platform firms, set out in SYSC 3.2.6. To avoid confusing the vast majority of firms by including a multitude of references to SYSC 3.2.6, this guidance is constructed in terms of following the requirements of SYSC 6.1.1; non common platform firms should follow this guidance, interpreting it as referring as necessary to the relevant parts of SYSC 3.2.6.

FSMA, s 1B(5)
FSMA, s 1D(2)(b)
SYSC 2.1.1 R,
6.1.1 R, 6.3

1.36 FSMA makes the prevention of financial crime integral to the discharge of the FCA's functions and fulfilment of its objectives. This means that the FCA is concerned that the firms it regulates and their senior management are aware of the risk of their businesses being used in connection with the commission of financial crime, and take appropriate measures to prevent financial crime, facilitate its detection and monitor its incidence. Senior management has operational responsibility for ensuring that the firm has appropriate systems and controls in place to combat financial crime.

SYSC 6.3.8 R
SYSC 24.3.9 G

1.37 In FCA-regulated firms (but see paragraph 1.49 for general insurance firms and mortgage intermediaries), a director or senior manager must be allocated overall responsibility for the establishment and maintenance of the firm's anti-money laundering systems and controls.

SYSC 6.3.9 R

1.38 In FCA-regulated firms (but see paragraph 1.49 for general insurance firms and mortgage intermediaries), an individual must be allocated responsibility for oversight of a firm's compliance with the FCA's Rules on systems and controls against money laundering: this is the firm's

MLRO. The FCA requires the MLRO to have a sufficient level of seniority within the firm to enable him to carry out his function effectively. In some firms the MLRO will be part of senior management (and may be the person referred to in paragraph 1.37); in firms where they are not, they will be directly responsible to someone who is.

SYSC 6.3.9 R

1.39 Senior management of FCA-regulated firms must appoint an appropriately qualified senior member of the firm's staff as the MLRO (see Chapter 3); and must provide direction to, and oversight of the firm's AML/CTF strategy.

1.40 Although the FCA Rule referred to in paragraph 1.37 requires overall responsibility for AML/CTF systems and controls to be allocated to a single individual, in practice this may often be difficult to achieve, especially in larger firms. As a practical matter, therefore, firms may allocate this responsibility among a number of individuals, provided the division of responsibilities is clear.

1.41 The relationship between the MLRO and the director/senior manager allocated overall responsibility for the establishment and maintenance of the firm's AML/CTF systems (where they are not the same person) is one of the keys to an effective AML/CTF regime. It is important that this relationship is clearly defined and documented, so that each knows the extent of their, and the other's, role and day to day responsibilities.

Regulation 21(1)(a)

1.42 Where the firm is required to appoint a board member or member of its senior management as the officer responsible for the firm's compliance with the ML Regulations, it is important that this individual, the MLRO and the director/senior manager allocated overall responsibility for the establishment and maintenance of the firm's AML/CTF systems (where they are not the same person) are all clear as to the responsibilities of each.

SYSC 6.3.7(2) G

1.43 At least once in each calendar year, an FCA-regulated firm should commission a report from its MLRO (see Chapter 3) on the operation and effectiveness of the firm's systems and controls to combat money laundering. In practice, senior management should determine the depth and frequency of information they feel is necessary to discharge their responsibilities. The MLRO may also wish to report to senior management more frequently than annually, as circumstances dictate.

1.44 When senior management receives reports from the firm's MLRO it should consider them and take any necessary action to remedy any deficiencies identified in a timely manner.

SUP 16.23.4 R
SUP 16.23.2 R

1.45 All firms, other than credit unions and certain firms with limited permissions and total revenues of less than £5 million, must submit an Annual Financial Crime Report to the FCA in respect of their financial year ending on its latest accounting reference date (see paragraphs 3.46-3.49).

SYSC 3.2.6 R,
6.3.9(2) R

1.46 Those FCA-regulated firms required to appoint an MLRO are specifically required to provide the MLRO with adequate resources. All firms, whether or not regulated by the FCA for AML purposes, must apply adequate resources to counter the risk that they may be used for

the purposes of financial crime. This includes establishing, and monitoring the effectiveness of, systems and controls to prevent ML/TF. The level of resource should reflect the size, complexity and geographical spread of the firm's customer and product base.

1.47 The role, standing and competence of the MLRO, and the way the internal processes for reporting suspicions are designed and implemented, impact directly on the effectiveness of a firm's money laundering/terrorist financing prevention arrangements.

1.48 As well as supervisory expectations (as referred to in paragraph 1.26), firms should be aware of the FCA's published enforcement findings in relation to individual firms, and its actions in response to these; this information is available on the FCA website at www.fca.org.uk.

Exemptions from legal and regulatory obligations

SYSC 1.1A.1, 3.2.6 R

1.49 General insurance firms and mortgage intermediaries are regulated by the FCA, but are not covered by the ML Regulations, or by the provisions of SYSC specifically relating to money laundering. They are, therefore, under no obligation to appoint an MLRO. They are, however, subject to the general requirements of SYSC, and so have an obligation to have appropriate risk management systems and controls in place, including controls to counter the risk that the firm may be used to further financial crime. Guidance for general insurance firms is given in Part II Sector 7A: *General insurers*.

POCA ss 327-329, 335, 338
Terrorism Act s 21

1.50 These firms are also subject to the provisions of POCA and the Terrorism Act which establish the primary offences. These offences are not committed if a person's knowledge or suspicion of ML/TF is reported to the NCA, and (if relevant) appropriate consent for the transaction or activity obtained. Certain of these firms may also be subject to the provisions of Schedule 7 to the Counter-Terrorism Act 2008.

POCA s 332
Terrorism Act ss 19, 21

1.51 For administrative convenience, and to assist their staff fulfil their obligations under POCA or the Terrorism Act, general insurance firms and mortgage intermediaries may choose to appoint a nominated officer. Where they do so, they will be subject to the reporting obligations in s 332 of POCA and s 19 of the Terrorism Act (see Chapter 6).

1.52 E-money issuers and payment institutions are regulated under the Electronic Money Regulations and the Payment Services Regulations, rather than FSMA. This means that they are subject to the AML/CTF provisions in legislation, but not to most of the FCA's Handbook rules. The FCA has issued guidance that sets out its expectations of e-money issuers' and payment institutions' AML/CTF controls:

- http://www.fca.org.uk/static/documents/emoney-approach.pdf for e-money issuers;
- http://www.fca.org.uk/your-fca/documents/payment-services-approach for payment institutions.

Guidance for e-money issuers is also set out in Part II Sector 3.

Senior management should adopt a formal policy, and carry out a risk assessment, in relation to financial crime prevention

SYSC 3.1.1 R, 3.2.6 R 6.1.1 R 6.3.1 R Regulation 16(2)

1.53 As mentioned in paragraph 1.1 above, senior management in FCA-regulated firms has a responsibility to ensure that the firms' policies, controls and procedures are appropriately designed and implemented, and are effectively operated to manage the firm's risks. This includes taking appropriate steps to identify and assess the risks of money laundering and terrorist financing to which its business is subject. This assessment should take into account relevant findings in the UK national risk assessments of money laundering and terrorist financing.

Regulation 18

1.54 A firm's risk assessment must be documented, kept up-to-date and made available to the FCA on request. The FCA may decide that a documented risk assessment is not required in the case of a particular firm, where the specific risks inherent in the sector in which the firm operates are clear and understood.

SYSC 6.3.7(3) G

1.55 For FCA-regulated firms (but see paragraph 1.49 for general insurance firms and mortgage intermediaries, and 1.52 for e-money issuers and payment institutions) SYSC 6.3.7 (3) G says that a firm should produce "appropriate documentation of its risk management policies and risk profile in relation to money laundering, including documentation of its application of those policies".

1.56 A statement of the firm's AML/CTF policy and the controls and procedures to implement it will clarify how the firm's senior management intends to discharge its responsibility for the prevention of money laundering and terrorist financing. This will provide a framework of direction to the firm and its staff, and will identify named individuals and functions responsible for implementing particular aspects of the policy. The policy will also set out how senior management undertakes its assessment of the money laundering and terrorist financing risks the firm faces, and how these risks are to be managed. Even in a small firm, a summary of its high-level AML/CTF policy will focus the minds of staff on the need to be constantly aware of such risks, and how they are to be managed.

1.57 A policy statement should be tailored to the circumstances of the firm. Use of a generic document might reflect adversely on the level of consideration given by senior management to the firm's particular risk profile.

1.58 The policy statement might include, but not be limited to, such matters as:

- Guiding principles:
  - an unequivocal statement of the culture and values to be adopted and promulgated throughout the firm towards the prevention of financial crime;

- a commitment to ensuring that customers' identities will be satisfactorily verified before the firm accepts them;
- a commitment to the firm 'knowing its customers' appropriately - both at acceptance and throughout the business relationship - through taking appropriate steps to verify the customer's identity and business, and his reasons for seeking the particular business relationship with the firm;
- a commitment to ensuring that staff are trained and made aware of the law and their obligations under it, and to establishing procedures to implement these requirements; and
- recognition of the importance of staff promptly reporting their suspicions internally.

- Risk mitigation approach:
  - a summary of the firm's approach to mitigating and managing effectively the risks of money laundering and terrorist financing it identifies;
  - allocation of responsibilities to specific persons and functions;
  - a summary of the firm's controls and procedures for carrying out appropriate identification and monitoring checks on the basis of their risk-based approach; and
  - a summary of the appropriate monitoring arrangements in place to ensure that the firm's policies and procedures are being carried out.

1.59 It is important that the firm's policies, controls and procedures are communicated widely throughout the firm, to increase the effectiveness of their implementation.

Application of group policies outside the UK

1.60 The UK legal and regulatory regime is primarily concerned with detecting and preventing money laundering which is connected with the UK. Where a UK financial institution has overseas branches, subsidiary undertakings or associates, where control can be exercised over business carried on outside the United Kingdom, or where elements of its UK business have been outsourced to offshore locations (see paragraphs 2.16-2.21), the firm must put in place a group AML/CTF strategy.

Regulation 20(1)

1.61 A firm that is a parent undertaking must ensure that its policies, controls and procedures apply to all subsidiary undertakings and non-UK branches. Such a firm must establish and maintain throughout its group, policies, controls and procedures for data protection and sharing, with other members of the group, information for the purposes of preventing money laundering and terrorist financing. This includes policies on the sharing of information about customers, customer accounts and transactions. Reporting processes must nevertheless follow local laws and procedures.

Regulation 20(3), (4)

1.62 If any subsidiary undertaking or branch is established in a third country which does not impose AML/CTF requirements as strict as those of the UK, the firm must ensure that such subsidiary undertakings or branches apply measures equivalent to those required by the ML Regulations. Where the law of a third country does not permit the application of such equivalent measures, the firm must inform the FCA accordingly, and take additional measures to handle the risk of money laundering and terrorist financing effectively.

Regulation 19(6)

1.63 Firms must communicate their policies, controls and procedures established to prevent activities related to money laundering and terrorist financing to branches and subsidiary undertakings located outside the UK.

1.64 Whilst suspicions of money laundering or terrorist financing may be required to be reported within the jurisdiction where the suspicion arose and where the records of the related transactions are held, there may also be a requirement for a report to be made to the NCA (see paragraph 6.25).

Extra-territoriality of some overseas jurisdictions' regimes

1.65 Where a firm has a listing in, or activities in, or is linked to, certain overseas jurisdictions, whether through a branch, subsidiary undertaking, associated company or correspondent relationship, or where a firm deals in another jurisdiction's currency, there is a risk that the application of that jurisdiction's AML/CTF and financial sanctions regimes may apply to the non-domestic activities of the firm. Senior management should take advice on the extent to which the firm's activities may be affected in this way.

CHAPTER 2

INTERNAL CONTROLS

➢ **Relevant law/regulation** ▪ Regulations 19 - 24 ▪ SYSC Chapters 2, 3, 6
➢ **Core obligations** ▪ Firms must establish and maintain adequate and appropriate policies and procedures to forestall and prevent operations relating to money laundering ▪ Appropriate controls should take account of the risks faced by the firm's business
➢ **Actions required, to be kept under regular review** ▪ Establish and maintain adequate and appropriate policies and procedures to forestall and prevent money laundering ▪ Introduce appropriate controls to take account of the risks faced by the firm's business ▪ Maintain appropriate control and oversight over outsourced activities

General legal and regulatory obligations

General

Regulation 19(1)(a) SYSC 3, 6

2.1 Firms are required to establish and maintain policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified in its risk assessment. FCA-regulated firms have similar, regulatory obligations under SYSC.

2.2 This chapter provides guidance on the internal controls that will help firms meet their obligations in respect of the prevention of money laundering and terrorist financing. There are general obligations on firms to maintain appropriate records and controls more widely in relation to their business; this guidance is not intended to replace or interpret these wider obligations.

Appropriate controls in the context of financial crime prevention

Regulation 19(1)(b), (c), (2)

2.3 A firm's policies, controls and procedures must be proportionate with regard to the size and nature of its business, and must be approved by its senior management and kept under regular review. A firm must maintain a written record of its policies, controls and procedures.

Regulation 19, 21(1)

2.4 There are specific requirements under the ML Regulations for the firm to establish adequate and appropriate policies, controls and procedures relating to: internal controls, including where appropriate employee screening and the appointment of an internal audit function; risk management practices (see Chapter 4); customer due diligence and ongoing monitoring (see Chapter 5); record keeping (see Chapter 8); reporting of suspicions (see Chapter 6); the monitoring and management of the effectiveness of, and compliance with, such policies and procedures, (see paragraphs 3.33-3.36); and the internal communication of such policies and procedures (which includes staff awareness and training) (see Chapter 7).

Internal controls - specific requirements

Regulation 21(1) 2.5 Where appropriate with regard to the size and nature of its business, a firm must

- Appoint a member of its board (or equivalent management body) or of its senior management as the officer responsible for the firm's compliance with the ML Regulations;
- Carry out screening of relevant employees and agents appointed by the firm, both before the appointment is made, and at regular intervals during the course of the appointment;
- Establish an independent internal audit function with responsibility to:
    - examine and evaluate the adequacy and effectiveness of the policies, controls and procedures adopted by the firm to comply with the requirements of the ML Regulations;
    - make recommendations in relation to those policies, controls and procedures; and
    - monitor the firm's compliance with those recommendations.

Regulation 21(3), (4) 2.6 An individual in the firm must be appointed as a nominated officer, whose identity, as well as any subsequent appointment to this position, must be notified to their supervisor. The firm must also notify their supervisor of the name of the member of its board (or equivalent management body) or of its senior management, and of any subsequent appointment to this position, as the officer responsible for the firm's compliance with the ML Regulations. Such notifications must be made within 14 days of the appointment.

Regulation 21(2)(a) 2.7 Screening of relevant employees (for the purposes referred to in paragraph 2.5 above) means an assessment of:

- the skills, knowledge and expertise of the individual to carry out their functions effectively; and
- the conduct and integrity of the individual.

Regulation 21(2)(b) 2.8 A relevant employee is one whose work is –

- relevant to the firm's compliance with any requirement in the ML Regulations; or
- otherwise capable of contributing to the
    - identification or mitigation of the risks of ML/TF to which the firm is subject; or
    - prevention or detection of ML/TF in relation to the firm's business.

Regulation 19(4) 2.9 A firm's policies, controls and procedures must include policies, controls and procedures:

See Revisions Sept 2026 for update to 2.9

- which provide for the identification and scrutiny of
    - complex or unusually large transactions, or an unusual pattern of transactions;
    - transactions which have no apparent economic or legal purpose; and

- any other activity which the firm regards as particularly likely by its nature to be related to money laundering or terrorist financing.

- which specify the undertaking of additional measures, where appropriate, to prevent the use for money laundering or terrorist financing of products or transactions which might favour anonymity;
- which ensure that when new products, new business practices or new technology are adopted by the firm, appropriate measures are taken to assess, and if necessary, mitigate, any money laundering or terrorist financing risks this may cause;
- under which anyone in the firm who knows or suspects (or has reasonable grounds for knowing or suspecting) money laundering or terrorist financing is required to report such knowledge or suspicion to the firm's nominated officer.

Firms should also have in place policies, controls and procedures to assess and mitigate the risks arising from remote booking arrangements.

Regulation 21(8), (9)

2.10 Firms must establish and maintain systems which enable them to respond fully and rapidly to enquiries from financial investigators accredited under s3 of POCA, persons acting on behalf of the Scottish Ministers in their capacity as an enforcement authority under the Act or constables, relating to:

- whether it maintains, or has maintained during the previous five years, a business relationship with any person; and
- the nature of that relationship.

2.11 As well as considering the provisions of the ML Regulations about what internal controls should comprise, it could be helpful to look to the FCA Handbook, which although only applying to FCA-regulated firms, provides helpful commentary on overall systems requirements.

SYSC 3.1.1 R
SYSC 3.1.2 G
SYSC 6.1.1 R
SYSC 6.1.2 R

2.12 FCA-regulated firms are required to have systems and controls appropriate to their business. Such systems and controls will therefore vary depending on the nature and characteristics of the firm, although they must include measures 'for countering the risk that the firm might be used to further financial crime'. This requires a firm to make use of its assessment of the financial crime risks to which it is subject (described more fully in paragraphs 1.2-1.8). Financial crime includes the handling of the proceeds of crime – that is, money laundering or terrorist financing. The nature and extent of systems and controls will vary by firm and depend on a variety of factors, including:

- the nature, scale and complexity of the firm's business;
- the diversity of its operations, including geographical diversity;
- its customer, product and activity profile;
- its distribution channels;
- the volume and size of its transactions; and
- the degree of risk associated with each area of its operation.

SYSC 6.3.1 R
Regulation 19

2.13 An FCA-regulated firm must ensure that these systems and controls:

- enable it to identity, assess, monitor and manage money laundering risk; and
- are comprehensive and proportionate to the nature, scale and complexity of its activities.

These obligations are, in effect, similar to those imposed on all obliged entities under the ML Regulations.

SYSC 6.3.7 G
SYSC 6.3.8 R
SYSC 6.3.9 R

2.14 An FCA-regulated firm's systems and controls (but see paragraph 1.49 for general insurance firms and mortgage intermediaries) are required to cover senior management accountability, including allocation to a director or senior manager of overall responsibility for the establishment and maintenance of effective AML systems and controls and the appointment of a person with adequate seniority and experience as MLRO. The systems and controls should also cover:

- appropriate training on money laundering to ensure that employees are aware of, and understand, their legal and regulatory responsibilities and their role in handling criminal property and money laundering/terrorist financing risk management;
- appropriate provision of regular and timely information to senior management relevant to the management of the firm's criminal property/money laundering/terrorist financing risks;
- appropriate documentation of the firm's risk management policies and risk profile in relation to money laundering, including documentation of the firm's application of those policies; and
- appropriate measures to ensure that money laundering risk is taken into account in the day-to-day operation of the firm, including in relation to:
    - the development of new products;
    - the taking-on of new customers; and
    - changes in the firm's business profile.

2.15 It is important that the firm's policies, controls and procedures are communicated widely throughout the firm, to increase the effectiveness of their implementation.

Outsourcing and non-UK processing

2.16 Many firms outsource certain activities, including some of their systems and controls and/or processing to an agent or outsourcing service provider elsewhere within the UK and to other jurisdictions, and/or to other group companies. Involving other entities in the operation of a firm's systems may give rise to additional risk which must be actively managed. Firms should obtain assurance that outsourcing providers meet the standards or requirements set out in this Guidance.

Regulation 39(7), (8)

2.17 Nothing in the ML Regulations prevents a firm applying CDD measures by means of an agent or an outsourcing service provider (but see paragraphs 5.3.51 to 5.3.53 in Part I, Chapter 5), provided that the arrangements between the firm and the agent or outsourcing service provider provide for the firm to remain liable for any failure to apply such measures.

SYSC 3.1, 3.2.4 G
SYSC 8.1, 13.9

2.18 FCA-regulated firms cannot contract out of their regulatory responsibilities, and therefore remain responsible for systems and controls in relation to the activities outsourced, whether within the UK or to another jurisdiction. In all instances of outsourcing, it is the delegating firm that bears the ultimate responsibility for the duties undertaken in its name. This will include the requirement to ensure that the provider of the outsourced services has in place satisfactory AML/CTF systems, controls and procedures, and that those policies and procedures are kept up to date to reflect changes in UK requirements.

2.19 Where a firm's UK AML/CTF operational activities are undertaken by an outsourced service provider or group companies in other jurisdictions (e.g. call centres abroad, transaction monitoring or CDD processing), those activities must be subject to equivalent AML/CTF policies and procedures that are applicable to the UK firm. Internal reporting procedures must be implemented to ensure that all suspicions relating to UK-related accounts, transactions or activities are reported to the firm's nominated officer in the UK.

2.20 Firms should also be aware of local obligations, in all jurisdictions to which they outsource functions, for the detection and prevention of financial crime. Procedures should be in place to meet local AML/ CTF regulations and reporting requirements. Any conflicts between the UK and local AML/CTF requirements, where meeting local requirements would result in a lower standard than in the UK, should be resolved in favour of the UK requirements.

2.21 In some circumstances, the outsourcing of functions can actually lead to increased risk - for example, outsourcing to businesses in jurisdictions with less stringent AML/CTF requirements than in the UK. All financial services businesses that outsource functions and activities should therefore assess any possible AML/ CTF risk associated with the outsourced functions, record the assessment and monitor the risk on an ongoing basis.

Intragroup and group companies

2.22 UK firms must ensure that all UK AML/CTF and sanctions obligations are complied with where there are UK branches or UK subsidiaries that may have intragroup and external outsourcing arrangements that are relevant to the UK firm's financial crime systems and controls.

2.23 The MLRO/SMF 17 must have due authority to take action where material AML/CTF outsourcing risks arise (intragroup and external).

2.24 Where there are intragroup outsourced activities to other group companies or to headquarters (in cases of a UK branch) firms should have risk-based mechanisms, such as service level agreements to cover, for example:

- Reporting of AML/CTF management information, which could take the form of key performance indicators (KPIs) that may indicate certain ML/TF risks, to monitor compliance with AML/CTF policies and procedures;
- Reporting of AML/CTF management information, which could take the form of key risk indicators (KRIs) that may include details of preventative mitigating controls or the results of defective quality assurance controls;
- Provision of information on AML/CTF training completed by staff of the outsourcing service providers, within or outside the UK;
- Provision of information on the results of compliance monitoring/ testing or relevant audits where risk issues have been identified;
- Escalation protocols to communicate relevant operational events having an impact on the performance of the outsourced activity.

CHAPTER 3

NOMINATED OFFICER/MONEY LAUNDERING REPORTING OFFICER (MLRO)

- **Relevant law/regulation**
  - Regulation 21
  - COCON
  - PRIN, Principle 11
  - APER, Chapters 2 and 4
  - APER, Principles 4 and 7
  - SYSC, Chapter 6
  - SUP, Chapter 10A, 10C
- **Core obligations**
  - Nominated officer to be appointed, who must receive and review internal disclosures
  - Nominated officer is responsible for making external reports
  - FCA approval required for MLRO (who may also be the nominated officer), as it is a designated Senior Management Function (SMF 17)
  - Threshold competence required
  - MLRO should be able to act on his own authority
  - Adequate resources must be devoted to AML/CTF
  - MLRO is responsible for oversight of the firm's AML systems and controls
- **Actions required, to be kept under regular review**
  - Appoint a nominated officer
  - Senior management to ensure the MLRO has:
    - active support of senior management
    - adequate resources
    - independence of action
    - access to information
    - an obligation to produce an annual report
  - MLRO to ensure he has continuing competence
  - MLRO to monitor the effectiveness of systems and controls

General legal and regulatory obligations

Legal obligations

Regulation 21(3) POCA ss337, 338 Terrorism Act ss21A, 21B

3.1 All firms (other than sole traders) carrying out relevant business under the ML Regulations, whether or not the firm is regulated by the FCA, must appoint a nominated officer, who is responsible for receiving disclosures under Part 7 of POCA and Part 3 of the Terrorism Act, deciding whether these should be reported to the NCA, and, if appropriate, making such external reports.

3.2 A sole trader with no employees who knows or suspects, or where there are reasonable grounds to know or suspect, that a customer of his, or the person on whose behalf the customer is acting, is or has been engaged in, or attempting, money laundering or terrorist financing, must make a report promptly to the NCA.

Regulation 21(1)(a)

3.3 Where appropriate with regard to the size and nature of its business, a firm must appoint a member of its board of directors (or equivalent

management body) or of its senior management as the officer responsible for the firm's compliance with the ML Regulations.

Regulatory obligations

SYSC 6.3.9 R
SUP 10C.4.3 R

3.4 In the case of FCA-regulated firms, other than sole traders with no employees and those firms covered by paragraph 3.2, there is a requirement to appoint an MLRO. The responsibilities of the MLRO under SYSC are different from those of the nominated officer under the ML Regulations, POCA or the Terrorism Act, but in many FCA-regulated firms it is likely that the MLRO and the nominated officer will be one and the same person. When discharging different legal and regulatory functions, it is important that the individual is aware which role he is acting in.

SYSC 6.3.9(1) R

3.5 The MLRO is responsible for oversight of the firm's compliance with the FCA's Rules on systems and controls against money laundering.

Regulation 21(8)

3.6 An MLRO should be able to monitor the day-to-day operation of the firm's AML/CTF policies, and respond fully and rapidly to enquiries for information made by the FCA or law enforcement.

PRIN 2.1.1
APER 2.1A.3

3.7 Under FCA Principle 11 of its Principles for Businesses, an FCA-regulated firm must deal with its regulators in an open and cooperative way, and must disclose to the FCA appropriately anything relating to the firm of which the FCA would reasonably expect notice. The MLRO is personally required to deal with the FCA similarly, under its Statement of Principle 4.

SYSC 1.1A.1
SYSC 3.2.6 R

3.8 As noted in paragraph 1.49, general insurance firms and mortgage intermediaries are not covered by the ML Regulations, s 330 of POCA, s 21A of the Terrorism Act, or the provisions of SYSC relating specifically to money laundering. They are, however, regulated by the FCA and may be subject to the disclosure obligations in POCA and the Terrorism Act. They therefore are under no obligation to appoint a nominated officer or an MLRO, or to allocate to a director or senior manager the responsibility for the establishment and maintenance of effective anti-money laundering systems and controls. They are, however, subject to the general requirements of SYSC, and so have an obligation to have appropriate risk management systems and controls in place, including controls to counter the risk that the firm might be used to further financial crime. They are also subject to ss 337 and 338 of POCA and s 19 of the Terrorism Act.

POCA s 332
Terrorism Act
s 19

3.9 For administrative convenience, and to assist their staff fulfil their obligations under POCA or the Terrorism Act, firms who have no legal obligation to do so, may nevertheless choose to appoint a nominated officer. Where they do so, the nominated officer will be subject to the reporting obligations in s 332 of POCA and s 19 of the Terrorism Act.

Standing of the MLRO *

SYSC 6.3.10 G FSMA s59	3.10	The role of MLRO has been designated by the FCA as a controlled/Senior Management function under s 59 of FSMA. As a consequence, any person invited to perform that function must be individually approved by the FCA, on the application of the firm, before performing the function. The FCA expect that the MLRO will be based in the UK.
APER 4.7.9 E APER 2.1A.3	3.11	Failure by the MLRO to discharge the responsibilities imposed on him in SYSC 6.3.9 R is conduct that does not comply with Statement of Principle 7 for Approved Persons, namely that 'an approved person performing an accountable higher management function must take reasonable steps to ensure that the business of the firm for which they are responsible in their accountable function capacity complies with the relevant requirements and standards of the regulatory system'.
SYSC 6.3.9 R SYSC 6.3.10 G	3.12	In FCA-regulated firms, the MLRO is responsible for the oversight of all aspects of the firm's AML/CTF activities and is the focal point for all activity within the firm relating to anti-money laundering. The individual appointed as MLRO must have a sufficient level of seniority within the firm (see paragraph 1.38). As the MLRO is an Approved Person/SMF Manager, their job description should clearly set out the extent of the responsibilities given to them, and their objectives. The MLRO will need to be involved in establishing the basis on which a risk-based approach to the prevention of money laundering/terrorist financing is put into practice.
SYSC 4.4 SYSC 6.3.9(1) R SYSC 6.3.10 G	3.13	Along with the SMF Manager appointed by the Board (see paragraph 1.37), an MLRO will support and co-ordinate senior management focus on managing the money laundering/terrorist financing risk in individual business areas. They will also help ensure that the firm's wider responsibility for forestalling and preventing money laundering/terrorist financing is addressed centrally, allowing a firm-wide view to be taken of the need for monitoring and accountability.
	3.14	As noted in paragraph 1.41, the relationship between the MLRO and the director(s)/senior manager(s) allocated overall responsibility for the establishment and maintenance of the firm's AML/CTF systems is one of the keys to an effective AML/CTF regime. It is important that this relationship is clearly defined and documented, so that each knows the extent of their, and the other's, role and day to day responsibilities.
Regulation 21(1)(a)	3.15	Where the firm is required to appoint a board member or member of its senior management as the officer responsible for the firm's compliance with the ML Regulations, it is important that this individual, the MLRO and the director(s)/senior manager(s) allocated overall responsibility for the establishment and maintenance of the firm's AML/CTF systems (see paragraph 3.14) are all clear as to the responsibilities of each.
SYSC 6.3.9(2) R	3.16	The MLRO must have the authority to act independently in carrying out their responsibilities. The MLRO must be free to have direct access to the FCA and (where they are the nominated officer) appropriate law

*Note: There are updates within paras 3.10 to 3.36 that are awaiting formal HMT approval - until such time, the updates are available under the Revisions tab at https://www.jmlsg.org.uk/revisions/.

enforcement agencies, including the NCA, in order that any suspicious activity may be reported to the right quarter as soon as is practicable. They must be free to liaise with the NCA, on their own authority, on any question of whether to proceed with a transaction in the circumstances.

SYSC 6.3.9(2) R

3.17 Senior management of the firm must ensure that the MLRO has sufficient resources available to them, including appropriate staff and technology. This should include arrangements to apply in their temporary absence.

3.18 Where a firm is part of a group, it may appoint as its MLRO an individual who performs that function for another firm within the group. If a firm chooses this approach, it may wish to permit the MLRO to delegate AML/CTF duties to other suitably qualified individuals within the firm. Similarly, some firms, particularly those with a number of branches or offices in different locations, may wish to permit the MLRO to delegate such duties within the firm. In larger firms, because of their size and complexity, the appointment of one or more permanent Deputy MLROs of suitable seniority may be necessary. In such circumstances, the principal, or group MLRO needs to ensure that roles and responsibilities within the group are clearly defined, so that staff of all business areas know exactly who they must report suspicions to.

SUP 10C.3.13 R

3.19 Where an MLRO is temporarily unavailable, no pre-approval for a deputy will be required for temporary cover of up to 12 weeks in any consecutive 12-month period. For longer periods, however, FCA approval will need to be sought. Rather than appointing a formal deputy, smaller firms may prefer to rely on temporary cover.

3.20 Where AML/CTF tasks are delegated by a firm's MLRO, the FCA will expect the MLRO to take ultimate managerial responsibility.

Internal and external reports

Regulation 19(4)(d) POCA s 330

3.21 A firm must require that anyone in the firm to whom information or other matter comes in the course of business as a result of which they know or suspect, or have reasonable grounds for knowing or suspecting, that a person is engaged in money laundering or terrorist financing complies with Part 7 of POCA or Part 3 of the Terrorism Act (as the case may be). This includes staff having an obligation to make an internal report to the nominated officer as soon as is reasonably practicable after the information or other matter comes to them.

3.22 Any internal report should be considered by the nominated officer, in the light of all other relevant information, to determine whether or not the information contained in the report does give rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion, of money laundering or terrorist financing.

3.23 A firm is expected to use its existing customer information effectively by making such information readily available to its nominated officer.

3.24 In most cases, before deciding to make a report, the nominated officer is likely to need access to the firm's relevant business information. A firm should therefore take reasonable steps to give its nominated officer access to such information. Relevant business information may include details of:

- the financial circumstances of a customer or beneficial owner, or any person on whose behalf the customer has been or is acting;
- the features of the transactions, including, where appropriate, the jurisdiction in which the transaction took place, which the firm entered into with or for the customer (or that person); and
- the underlying CDD information, and copies of the actual source documentation in respect of the customer.

3.25 In addition, the nominated officer may wish:

- to consider the level of identity information held on the customer, and any information on their personal circumstances that might be available to the firm; and
- to review other transaction patterns and volumes through the account or accounts in the same name, the length of the business relationship and identification records held.

Regulation 19(4)(d)
Regulation 21(5)
POCA s 331

3.26 If the nominated officer (or appointed alternate) concludes that the internal report does give rise to knowledge or suspicion of money laundering or terrorist financing, they must make a report to the NCA as soon as is practicable after they make this determination. The nominated officer (or appointed alternate)'s decision in this regard must be their own, and should not be subject to the direction or approval of other parties within the firm.

3.27 Guidance on reviewing internal reports, and reporting as appropriate to the NCA, is set out in Chapter 6.

National and international findings in respect of countries and jurisdictions

3.28 An MLRO should ensure that the firm obtains, and makes appropriate use of, any government or FATF findings concerning the approach to money laundering prevention in particular countries or jurisdictions. This is especially relevant where the approach has been found to be materially deficient by FATF. Reports on the mutual evaluations carried out by the FATF can be found at www.fatf-gafi.org. Other sources of information include IMF and World Bank reports.

3.29 The ML Regulations state that a FATF call for action country is a country named on the list of High-Risk Jurisdictions subject to a Call for Action, as published by FAFT from time to time. This list identifies high-risk jurisdictions with serious strategic deficiencies in the area of anti-money laundering, counter terrorist financing or counter proliferation financing.

3.30 Countries may also be assessed using publicly available indices from, for example, HM Treasury Sanctions[10], FATF high-risk and non-cooperative jurisdictions[11], FATF Mutual Evaluation Reports, Transparency International Corruption Perceptions Index[12], FCO Human Rights Report[13] and Department for International Trade overseas country risk pages[14].

3.31 Firms considering business relations and transactions with individuals and firms – whether direct or through correspondents - located in higher risk jurisdictions, or jurisdictions against which the UK has outstanding advisory notices, should take account of the background against which the assessment, or the specific recommendations contained in the advisory notices, have been made.

3.32 Additionally, the NCA periodically produces intelligence assessments, which are forwarded to the MLROs of the relevant sectors for internal dissemination only. No NCA material is published through an open source.

Monitoring effectiveness of money laundering controls

SYSC 6.3.3 R
SYSC 6.3.9(1) R
SYSC 6.3.10 G

3.33 A firm is required to carry out regular assessments of the adequacy of its systems and controls to ensure that they manage the money laundering risk effectively. Oversight of the implementation of the firm's AML/CTF policies and procedures, including the operation of the risk-based approach, is primarily the responsibility of the MLRO, under delegation from senior management. The MLRO must therefore ensure that appropriate monitoring processes and procedures across the firm are established and maintained.

Regulation 21(1)

3.34 However, where appropriate with regard to the size and nature of its business, a firm must establish an independent internal audit function with responsibility for:

- examining and evaluating the adequacy and effectiveness of the policies, controls and procedures adopted by the firm to comply with the requirements of the ML Regulations;
- making recommendations in relation to those policies, controls and procedures; and
- monitoring the firm's compliance with those recommendations.

3.35 Effectiveness of systems and controls is therefore driven by a combination of features, including:

[10] https://www.gov.uk/government/publications/the-uk-sanctions-list
[11] http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/
[12] https://www.transparency.org/en/cpi/2021
[13] https://www.gov.uk/government/collections/human-rights-and-democracy-reports
[14] https://www.gov.uk/government/collections/overseas-business-risk

- ensuring that policies and procedures reflect current legal and regulatory developments and requirements;
- having appropriate monitoring processes, with timely follow up of findings;
- the adequacy of resources available;
- appropriate monitoring of outsourced compliance arrangements;
- adequately trained staff, who are up to date with current developments;
- having appropriate quality control/internal review processes;
- appropriate management information made available to senior management and those with supervisory responsibilities;
- the work of any internal audit function.

Regulation 20

3.36 The effective operation of group systems and controls in branches and subsidiary undertakings outside the UK will be influenced by the ability of the group to ensure that these can be followed without local restrictions, whether in law or otherwise (see paragraphs 1.60 - 1.62).

Reporting to senior management

SYSC 6.3.7(2) G

3.37 At least annually the senior management of an FCA-regulated firm should commission a report from its MLRO which assesses the operation and effectiveness of the firm's systems and controls in relation to managing money laundering risk.

3.38 In practice, senior management should determine the depth and frequency of information they feel necessary to discharge their responsibilities. The information provided in the FCA Annual Financial Crime Report may provide some of the material required for this purpose. The MLRO may also wish to report to senior management more frequently than annually, as circumstances dictate.

3.39 The firm's senior management should consider the report, and take any necessary action to remedy deficiencies identified in it, in a timely manner.

3.40 The MLRO will wish to bring to the attention of senior management areas where the operation of AML/CTF controls should be improved, and proposals for making appropriate improvements. The progress of any significant remedial programmes will also be reported to senior management.

3.41 In addition, the MLRO should report on the outcome of any relevant quality assurance or internal audit reviews of the firm's AML/CTF processes, as well as the outcome of any review of the firm's risk assessment procedures (see paragraph 4.82).

3.42 Firms will need to use their judgment as to how the MLRO should be required to break down the figures of internal reports in their annual report.

3.43 In December 2006, after discussion with the FCA, JMLSG issued a template suggesting a suitable presentation and content framework for a working paper underpinning the production of the MLRO Annual Report (see further https://www.jmlsg.org.uk/other-material/useful-resources/).

3.44 An MLRO may choose to report in a different format, according to the nature and scope of their firm's business.

3.45 In practice, subject to the approval of the FCA, larger groups might prepare a single consolidated report covering all of its regulated firms. The MLRO of each regulated firm within the group still has a duty to report appropriately to the senior management of his regulated firm.

Reporting to the FCA

3.46 The MLRO is likely to be responsible for the preparation and submission of the Annual Financial Crime Report required by the FCA.

SUP 16.23.4 R
SUP 16.23.2 R

3.47 All firms, other than credit unions and certain firms with limited permissions and total revenues of less than £5 million, must submit an Annual Financial Crime Report to the FCA annually in respect of their financial year ending on its latest accounting reference date.

SUP 16.23.5 R

3.48 If a group includes more than one firm, a single Annual Financial Crime Report may be submitted, and so satisfy the requirements of all firms in the group, where all the firms included in the single report have the same accounting reference date.

SUP 16.23.6 R
SUP 16.23.7 R

3.49 A firm must submit the Annual Financial Crime Report in the form specified in SUP 16 Annex 42AR, using the appropriate online systems accessible from the FCA website (www.fca.org.uk). The Report must be submitted within 60 business days of the firm's accounting reference date.

CHAPTER 4

RISK-BASED APPROACH

➢ **Relevant law/regulation** ▪ Regulations 18, 19(1), 27(8), 28(13), 33, 35 and 36 ▪ SYSC 3.1.2 G, 6.1.1 R, 6.3.1-3, 6.3.6 ➢ **Other authoritative pronouncements which endorse a risk-based approach** ▪ FATF Recommendations 1 and 10 ▪ Basel Paper – *Sound management of risks related to money laundering and financing of terrorism (updated July 2020)* ▪ IAIS Guidance Paper 5 ▪ IOSCO Principles paper
➢ **Core obligations** ▪ Identify and assess the risks of money laundering and terrorist financing to which its business is subject ▪ Appropriate systems and controls must reflect the degree of risk associated with the business and its customers ▪ Determine appropriate CDD measures on a risk-sensitive basis, depending on the type of customer, business relationship, product or transaction ▪ Take into account situations and products which by their nature can present a higher risk of money laundering or terrorist financing; these specifically include correspondent relationships; and business relationships and occasional transactions with PEPs
➢ **Actions required, to be kept under regular review** ▪ Carry out a formal, and regular, money laundering/terrorist financing/proliferation financing risk assessment, including market changes, and changes in products, customers and the wider environment ▪ Ensure internal policies, controls and procedures, including staff awareness, adequately reflect the risk assessment ▪ Ensure customer identification and acceptance procedures reflect the risk characteristics of customers ▪ Ensure arrangements for monitoring systems and controls are robust, and reflect the risk characteristics of customers

Introduction and legal obligations

General

4.1 There are a number of discrete steps in assessing the most cost effective and proportionate way to manage and mitigate the money laundering, terrorist financing and proliferation financing risks faced by the firm. These steps are to:

- identify the money laundering, terrorist financing and proliferation financing risks that are relevant to the firm;
- assess the risks presented by the firm's particular
    - customers and any underlying beneficial owners*;
    - products or services;
    - transactions;
    - delivery channels;
    - geographical areas of operation;

- design and implement controls to manage and mitigate these assessed risks, in the context of the firm's risk appetite;
- monitor and improve the effective operation of these controls; and
- record appropriately what has been done, and why.

** In this Chapter, references to 'customer' should be taken to include beneficial owner, where appropriate.*

4.2 Whatever approach is considered most appropriate to the firm's money laundering/terrorist financing/proliferation financing risk, the broad objective is that the firm should know at the outset of the relationship who its customers (and, where relevant, beneficial owners) are, where they operate, what they do, and their expected level of activity with the firm. The firm then should consider how the profile of the customer's financial behaviour builds up over time, thus allowing the firm to identify transactions or activity that may be suspicious.

Risk Assessment

Regulation 18(1),(2),(3) 18A(1),(2),(3)

4.3 The ML Regulations require firms to take appropriate steps to identify and assess the risks of money laundering, terrorist financing and proliferation financing[1] to which its business is subject, taking into account:

- information on money laundering, terrorist financing and proliferation financing made available to them by the FCA;
- risk factors, including factors relating to their customers, countries or geographic areas in which they operate, products, services, transactions and delivery channels.

In considering what steps are appropriate, firms must take into account the size and nature of its business. Firms that do not offer complex products or services and that have limited or no international exposure may not need an overly complex or sophisticated business risk assessment.

Regulation 18(4),(5),(6) 18A(4),(5),(6)

4.4 The risk assessments carried out must be documented, kept up to date and made available to the FCA on request. The FCA may decide that a documented risk assessment in the case of a particular firm is not required where the specific risks inherent in the sector in which the firm operates are clear and understood.

Regulation 16(2); 16A

4.5 The UK government has published national risk assessments (NRAs) of money laundering, terrorist financing and proliferation financing[2] which provide a backdrop to a firm's assessment of the UK risks inherent in

[1] The Money Laundering and Terrorist Financing (Amendment)(No.2) Regulations 2022 introduced a requirement for proliferation financing risk assessments wef 1 September 2022. A stand-alone PF risk assessment is not required.

[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf; https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2017; https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2020; https://www.gov.uk/government/publications/national-risk-assessment-of-proliferation-financing

its business. Firms should be aware of these publications, and should take account of relevant findings that affect their individual business risk assessment.

Regulation 16A(9)

4.5A The meaning of proliferation financing, as it relates to risk assessment, policies, controls and procedures, is specifically limited to the provision of funds or financial services for use in contravention of a relevant financial sanctions obligation.

Obligation to adopt a risk-based approach

4.6 Senior management of most firms, whatever business they are in, manage the firm's affairs with regard to the risks inherent in the business environment and jurisdictions the firm operates in, those risks inherent in its business and the effectiveness of the controls it has put in place to manage these risks.

4.7 To assist the overall objective to prevent money laundering, terrorist financing and proliferation financing, a risk-based approach:

- recognises that the money laundering/terrorist financing/proliferation financing threat to firms varies across customers, jurisdictions, products and delivery channels;
- allows management to differentiate between their customers in a way that matches the risk in their particular business;
- allows senior management to apply its own approach to the firm's procedures, systems and controls, and arrangements in particular circumstances; and
- helps to produce a more cost-effective system.

Regulation 33(7)
Regulation 37(4)

4.8 A firm therefore uses its assessment of the risks inherent in its business to inform its risk-based approach to the identification and verification of individual customers, which will in turn drive the level and extent of due diligence appropriate to that customer.

4.9 No system of checks will detect and prevent all money laundering, terrorist financing and proliferation financing. A risk-based approach will, however, serve to balance the cost burden placed on individual firms and their customers with a realistic assessment of the threat of the firm being used in connection with money laundering, terrorist financing and proliferation financing. It focuses the effort where it is needed and will have most impact.

4.10 The appropriate approach in any given case is ultimately a question of judgment by senior management, in the context of the risks they determine the firm faces.

Risk assessment – identification and assessment of business risks

Regulation 18(2)(b)

4.11 A firm is required to assess the risks inherent in its business, taking into account risk factors including those relating to its customers, countries

or geographical areas in which it operates, products, services, its transactions and delivery channels.

4.12 Examples of the risks in particular industry sectors are set out in the sectoral guidance in Part II. FATF also publishes papers on the ML/TF/PF risks in various industry sectors, see www.fatf-gafi.org. The UK government has published national risk assessments of money laundering and terrorist financing which provide a backdrop to a firm's assessment of the UK risks inherent in its business. Firms should be aware of these publications, and should take account of relevant findings that affect their individual business risk assessment.

4.13 The risk environment faced by the firm includes the wider context within which the firm operates – whether in terms of the risks posed by the jurisdictions in which it and its customers operate, the relative attractiveness of the firm's products or the nature of the transactions undertaken. Risks are posed not only in relation to the extent to which the firm has, or has not, been able to carry out the appropriate level of CDD in relation to the customer or beneficial owner(s), nor by who the customer or its beneficial owner(s) is (are), but also in relation to the activities undertaken by the customer – whether in the normal course of its business, or through the products used and transactions undertaken.

4.14 The business of many firms, their product and customer base, can be relatively simple, involving few products, with most customers falling into similar categories. In such circumstances, a simple approach, building on the risk the firm's products are assessed to present, may be appropriate for most customers, with the focus being on those customers who fall outside the 'norm'. Other firms 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 AML/CTF procedures. Here, too, the approach for most customers may be relatively straightforward, building on the product risk.

4.15 For firms which operate internationally, or which have customers based or operating abroad, there are additional risk considerations relating to the position of the jurisdictions involved, and their reputation and standing as regards the inherent ML/TF/PF risk, and the effectiveness of their AML/CTF enforcement regime.

4.16 Many governments and authorities carry out ML/TF/PF risk assessments for their jurisdictions, and firms should have regard to these, insofar as they are published and available.

4.17 The ML Regulations state that a FATF call for action country is a country named on the list of High-Risk Jurisdictions subject to a Call for Action, as published by FATF from time to time. This list identifies high-risk jurisdictions with strategic deficiencies in the area of anti-money laundering, counter terrorist financing or counter proliferation financing.

4.18 Countries may also be assessed using publicly available indices from, for example, HM Treasury Sanctions, FATF high-risk and non-cooperative jurisdictions, Transparency International Corruption Perceptions Index and the Department of International Trade (see paragraph 3.30).

SYSC 6.3.6 G

4.19 In identifying its money laundering risk an FCA-regulated firm should consider a range of factors, including

- its customer, product and activity profiles;
- its distribution channels;
- the complexity and volume of its transactions;
- its processes and systems; and
- its operating environment.

4.20 The firm should therefore assess its risks in the context of how it might most likely be involved in money laundering, terrorist financing and proliferation financing. In this respect, senior management should ask themselves a number of questions, for example:

- What risk is posed by the firm's customers?
- What risk is posed by a customer's behaviour?
- How does the way the customer comes to the firm affect the risk?
- What risk is posed by the products/services the customer is using?

4.21 Annex 4-I contains further guidance on considerations firms might take account of in assessing the level of ML/TF/PF risk in different jurisdictions. The concept of an 'equivalent jurisdiction' no longer exists under the ML Regulations.

4.22 When the FCA issues a relevant thematic review report, or updates its *Financial Crime Guide*, as part of its ongoing assessment of ML/TF risks, a firm should consider whether there are any areas of risk or issues of concern which are relevant to the firm's business highlighted within the report. Firms should be aware of the FCA's published enforcement findings in relation to individual firms, and its actions in response to these - this information is available on the FCA website (https://www.fca.org.uk/about/enforcement).

New technologies

Regulation 19(4)(c), 33(6)(b)(v), 19A(4)

4.23 In identifying and assessing the money laundering, terrorist financing and proliferation financing risks, firms must take account of whether new products and new business practices are involved, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. As well as being specifically required in assessing whether there is a high risk of ML/TF/PF in a particular situation, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. Appropriate measures should be taken to manage and mitigate those risks, including where relevant in particular cases the application of enhanced due diligence measures.

A risk-based approach – Design and implement controls to manage and mitigate the risks

Regulation 19(1); 19A(1)

4.24 Once the firm has identified and assessed the risks it faces in respect of money laundering, terrorist financing and proliferation financing, senior management must establish and maintain policies, controls and procedures to mitigate and manage effectively the risks of money laundering, terrorist financing and proliferation financing identified in its risk assessment. These policies, controls and procedures must take account of the size and nature of the firm's business.

4.25 The policies, controls and procedures designed to mitigate assessed ML/TF/PF risks should be appropriate and proportionate to these risks, and should be designed to provide an effective level of mitigation.

Regulation 19(2)(b), 19A(2)(b)

4.26 Firms must obtain approval from their senior management for the policies, controls and procedures that they put in place and for monitoring and enhancing the measures taken, where appropriate.

4.27 A risk-based approach requires the full commitment and support of senior management, and the active co-operation of business units. The risk-based approach needs to be part of the firm's philosophy, and as such reflected in its procedures and controls. There needs to be a clear communication of policies, controls and procedures across the firm, along with robust mechanisms to ensure that they are carried out effectively, weaknesses are identified, and improvements are made wherever necessary.

Regulation 19, 19A, 21
20(1)(b)

4.28 The policies, controls and procedures referred to in paragraph 4.24 must include, but are not limited to:

- risk management practices, customer due diligence, reporting, record-keeping, internal controls, compliance management and employee screening;
- where appropriate with regard to the size and nature of the business, an independent audit function to examine and evaluate the firm's policies, controls and procedures.
- for parent firms, policies on the sharing of information about customers, customer accounts and transactions.

4.29 The nature and extent of AML/CTF/PF controls will depend on a number of factors, including:

- The nature, scale and complexity of the firm's business
- The diversity of the firm's operations, including geographical diversity
- The firm's customer, product and activity profile
- The distribution channels used
- The volume and size of transactions
- The extent to which the firm is dealing directly with the customer or is dealing through intermediaries, third parties, correspondents or non face to face access

- The degree to which the firm outsources the operation of any procedures to other (Group) entities.

4.30 The application of CDD measures is intended to enable a firm to form a reasonable belief that it knows the true identity of each customer and beneficial owner, and, with an appropriate degree of confidence, knows the types of business and transactions the customer is likely to undertake. The firm's procedures should include procedures to:

- Identify and verify the identity of each customer on a timely basis
- Identify and take reasonable measures to verify the identity of any ultimate beneficial owner
- Obtain appropriate additional information to understand the customer's circumstances and business, including the expected nature and level of transactions

4.31 How a risk-based approach is implemented will depend on the firm's operational structure. For example, a firm that operates through multiple business units will need a different approach from one that operates as a single business. Equally, it will also be relevant whether the firm operates through branches or subsidiary undertakings; whether their business is principally face to face or online; whether the firm has a high staff/customer ratio and/or a changing customer base, or a small group of relationship managers and a relatively stable customer base; or whether their customer base is international (especially involving high net worth individuals) or largely domestic.

4.32 Senior management should decide on the appropriate approach in the light of the firm's structure. The firm may adopt an approach that starts at the business area level, or one that starts from business streams. Taking account of any geographical considerations relating to the customer, or the transaction, the firm may start with its customer assessments, and overlay these assessments with the product and delivery channel risks; or it may choose an approach that starts with the product risk, with the overlay being the customer and delivery channel risks.

A risk-based approach – customer risk assessments

General

Regulation 28(12)

4.33 Based on the risk assessment carried out, a firm will determine the level of CDD that should be applied in respect of each customer and beneficial owner. It is likely that there will be a standard level of CDD that will apply to the generality of customer, based on the firm's risk appetite.

4.34 As regards money laundering, terrorist financing and proliferation financing, managing and mitigating the risks will involve measures to verify the customer's identity; collecting additional information about the customer; and monitoring their transactions and activity, to determine whether there are reasonable grounds for knowing or suspecting that money laundering or terrorist financing may be taking

place. Part of the control framework will involve decisions as to whether verification should take place electronically, and the extent to which the firm can use customer verification procedures carried out by other firms. Firms must determine the extent of their CDD measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction.

4.35 To decide on the most appropriate and relevant controls for the firm, senior management should ask themselves what measures the firm can adopt, and to what extent, to manage and mitigate these threats/risks most cost effectively, and in line with the firm's risk appetite. Examples of control procedures include:

- Introducing a customer identification programme that varies the procedures in respect of customers appropriate to their assessed money laundering/terrorist financing/proliferation financing risk;
- Requiring the quality of evidence – whether documentary, electronic or by way of third party assurance - to be of a certain standard;
- Obtaining additional customer information, where this is appropriate to their assessed money laundering/terrorist financing/proliferation financing risk; and
- Monitoring customer transactions/activities.

It is possible to try to assess the extent to which each customer should be subject to each of these checks, but it is the balance of these procedures as appropriate to the risk assessed in the individual customer, or category of customer, to which they belong that is relevant.

4.36 A customer identification programme that is graduated to reflect risk could involve:

- a standard information dataset to be held in respect of all customers;
- a standard verification requirement for all customers;
- more extensive due diligence (more identification checks and/or requiring additional information) on customer acceptance for higher risk customers;
- where appropriate, more limited identity verification measures for specific lower risk customer/product combinations; and
- an approach to monitoring customer activities and transactions that reflects the risk assessed to be presented by the customer, which will identify those transactions or activities that may be unusual or suspicious.

Customer risk assessments

Regulation 18

4.37 Although the ML/TF/PF risks facing the firm fundamentally arise through its customers, the nature of their businesses and their activities, a firm must consider its customer risks in the context of the wider ML/TF/PF environment inherent in the business and jurisdictions in which the firm and its customers operate. Firms should bear in mind that some jurisdictions have close links with other, perhaps higher risk, jurisdictions, and where appropriate and relevant regard should be had to this.

4.38 The risk posed by an individual customer may be assessed differently depending on whether the customer operates, or is based, in a jurisdiction with a reputation for ML/TF/PF, or in one which has a reputation for strong AML/CTF enforcement, or whether a customer is established in a FATF call for action country (see 5.5.11). Whether, and to what extent, the customer has contact or business relationships with other parts of the firm, its business or wider group can also be relevant.

4.39 In reaching an appropriate level of satisfaction as to whether the ML/TF/PF risk posed by the customer is acceptable and able to be managed, requesting more and more identification is not always the right answer – it is sometimes better to reach a full and documented understanding of what the customer does, and the transactions it is likely to undertake. Some business lines carry an inherently higher risk of being used for ML/TF/PF purposes than others.

Regulation 31(1) 4.40 However, as stated in paragraph 5.2.6, if a firm cannot satisfy itself as to the identity of a customer or the beneficial owner who is not the customer; verify that identity; or obtain sufficient information on the nature and intended purpose of the business relationship, it must not enter into a new business relationship and must terminate an existing one.

4.41 While a risk assessment should always be performed at the inception of the customer relationship (although see paragraph 4.48 below), for some customers a comprehensive risk profile may only become evident once the customer has begun transacting through an account, making the monitoring of transactions and on-going reviews a fundamental component of a reasonably designed RBA. A firm may also have to adjust its risk assessment of a particular customer based on information received from a competent authority.

4.42 Some other firms, however, often (but not exclusively) those dealing in wholesale markets, may offer a more 'bespoke' service to customers, many of whom are already subject to extensive due diligence by lawyers and accountants for reasons other than AML/CTF/PF. In such cases, the business of identifying the customer will be more complex, but will take account of the considerable additional information that already exists in relation to the prospective customer.

General principles – use of risk categories and factors

SYSC 6.3.6 G 4.43 In order to be able to implement a reasonable RBA, firms should identify criteria to assess potential money laundering risks. Identification of the money laundering or terrorist financing risks, to the extent that such terrorist financing risk can be identified, of customers or categories of customers, and transactions will allow firms to design and implement proportionate measures and controls to mitigate these risks.

4.44 Money laundering and terrorist financing risks may be measured using a number of factors. Application of risk categories to customers/situations can then provide a strategy for managing potential risks by enabling firms to subject customers to proportionate controls

and oversight. The key risk criteria are: country or geographic risk; customer risk; and product/services risk. The weight given to these criteria (individually or in combination) in assessing the overall risk of potential money laundering may vary from one institution to another, depending on their respective circumstances. Consequently, firms have to make their own determination as to the risk weights. Parameters set by law or regulation may limit a firm's discretion.

Regulation 33(7), 37(4)

4.45 Annex 4-II contains a fuller list of illustrative risk factors a firm may address when considering the ML/TF/PF risk posed by customer situations.

Regulation 28(13)

4.46 When assessing the ML/TF/PF risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channel risks, a firm should take into account risk variables relating to those risk categories. These variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures. Examples of such variables include:

- The purpose of an account or relationship
- The level of assets to be deposited by a customer or the size of transactions undertaken
- The regularity or duration of the business relationship

4.47 When assessing risk, firms should consider all relevant risk factors before determining what is the overall risk category and the appropriate level of mitigation to be applied.

4.48 A risk assessment will often result in a stylised categorisation of risk: e.g., high/medium/low. Criteria will be attached to each category to assist in allocating customers and products to risk categories, in order to determine the different treatments of identification, verification, additional customer information and monitoring for each category, in a way that minimises complexity.

Weighting of risk factors

4.49 When weighting risk factors, firms should make an informed judgment about the relevance of different risk factors in the context of a particular customer relationship or occasional transaction. This often results in firms allocating different 'scores' to different factors – for example, firms may decide that a customer's personal links to a jurisdiction associated with higher ML/TF/PF risk is less relevant in light of the features of the product they seek.

4.50 Ultimately, the weight given to each of these factors is likely to vary from product to product and customer to customer (or category of customer) and from one firm to another. When weighting factors, firms should ensure that:

- Weighting is not unduly influenced by just one factor;
- Economic or profit considerations do not influence the risk rating;
- Weighting does not lead to a situation where it is impossible for any business to be classified as high risk;

- Situations identified by national legislation or risk assessments as always presenting a high money laundering risk cannot be over-ruled by the firm's weighting; and
- Firms are able to override any automatically generated risk scores where necessary. The rationale for the decision to override such scores should be documented appropriately.

4.51 Where a firm uses automated systems, purchased from an external provider, to allocate overall risk scores to categorise business relationships or occasional transactions, it should understand how such systems work and how it combines risk factors to achieve an overall risk score. A firm must always be able to satisfy itself that the scores allocated reflect the firm's understanding of ML/TF/PF risk, and it should be able to demonstrate this to the FCA if necessary.

4.52 When the FCA issues a relevant thematic review report, or updates its *Financial Crime Guide*, as part of its ongoing assessment of ML/TF risks, a firm should consider whether there are any areas of risk or issues of concern which are relevant to the firm's business highlighted within the report. Firms should be aware of the FCA's published enforcement findings in relation to individual firms, and its actions in response to these; this information is available on the FCA website (https://www.fca.org.uk/about/enforcement).

Lower risk/simplified due diligence

4.53 Many customers, by their nature or through what is already known about them by the firm, carry a lower money laundering or terrorist financing risk. These might include:

- Customers who are employment-based or with a regular source of income from a known source which supports the activity being undertaken; (this applies equally to pensioners or benefit recipients, or to those whose income originates from their partners' employment);
- Customers with a long-term and active business relationship with the firm; and
- Customers represented by those whose appointment is subject to court approval or ratification (such as executors).

Regulation 37(1)

4.54 There are other circumstances where the risk of money laundering or terrorist financing may be lower. In such circumstances, and provided there has been an adequate analysis of the risk by the country or by the firm, including taking into account risk factors in Regulation 37(3), the firm may (if permitted by local law or regulation) apply reduced CDD measures. (See Part I, paragraphs 5.4.1ff for additional guidance on simplified due diligence.)]

4.55 Annex 4-II contains a fuller list of illustrative risk factors a firm may address when considering the ML/TF/PF risk posed by customer situations.

4.56 Having a lower money laundering or terrorist financing risk for identification and verification purposes does not automatically mean

that the same customer is lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.

4.57 Firms should not, however, judge the level of risk solely on the nature of the customer or the product. Where, in a particular customer/product combination, *either or both* the customer and the product are considered to carry a higher risk of money laundering or terrorist financing, the overall risk of the customer should be considered carefully. Firms need to be aware that allowing a higher risk customer to acquire a lower risk product or service on the basis of a verification standard that is appropriate to that lower risk product or service, can lead to a requirement for further verification requirements, particularly if the customer wishes subsequently to acquire a higher risk product or service.

4.58 Further considerations to be borne in mind in carrying out a risk assessment are set out in the sectoral guidance in Part II.

Higher risk/enhanced due diligence

4.59 When assessing the ML/TF/PF risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, potentially higher risk situations may be influenced by:

- Customer risk factors
- Country or geographic risk factors
- Product, service, transaction or delivery channel risk factors

Regulation 33(1), 4.60 Where higher risks are identified, firms are required to take enhanced measures to manage and mitigate the risks. Politically Exposed Persons and Correspondent relationships have been specifically identified by the authorities as higher risk, as well as business relationships with customers established in a FATF call for action country or relevant transactions where either of the parties is established in a FATF call for action country. Specific guidance on enhanced due diligence in these cases is given in section 5.5.

4.61 Where a customer is assessed as carrying a higher risk, then depending on the product sought, it will be necessary to seek additional information in respect of the customer, to be better able to judge whether or not the higher risk that the customer is perceived to present is likely to materialise. Such additional information may include an understanding of where the customer's funds and wealth have come from. Guidance on the types of additional information that may be sought is set out in section 5.5.

4.62 Where the risks of ML/TF/PF are higher, firms must conduct enhanced due diligence measures consistent with the risks identified.

Regulation 33(4)

(a) In particular, they must:

- as far as reasonably possible, examine the background and purpose of the transaction; and

- increase the degree and nature of monitoring of the business relationship, in order to determine whether these transactions or activities appear unusual or suspicious.

Regulation 33(5)

(b) Examples of other EDD measures that, depending on the requirements of the case, could be applied for higher risk business relationships include:

- Obtaining, and where appropriate verifying, additional information on the customer and updating more regularly the identification of the customer and any beneficial owner
- Obtaining additional information on the intended nature of the business relationship
- Obtaining information on the source of funds or source of wealth of the customer
- Obtaining information on the reasons for intended or performed transactions
- Obtaining the approval of senior management to commence or continue the business relationship
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards

4.63 Annex 4-II contains a fuller list of illustrative risk factors a firm may address when considering the ML/TF/PF risk posed by customer situations.

Regulation 33(1)(f), (4)

4.64 Where EDD measures are applied, firms must as far as reasonably possible examine the background and purpose of all unusually complex or unusually large transactions, unusual patterns of transactions and transactions which have no apparent economic or legal purpose. They must also increase the degree and nature of monitoring of the business relationship in which such transactions are made to determine whether those transactions or that relationship appear to be suspicious.

4.65 In the case of some situations assessed as high risk, or which are outside the firm's risk appetite, the firm may wish not to take on the customer, or may wish to exit from the relationship. This may be the case in relation to particular types of customer, or in relation to customers from, or transactions to or through, particular high-risk countries or geographic areas, or in relation to a combination of other risk factors.

4.66 Although jurisdictions may be subject to economic sanctions, there may be some situations where for humanitarian or other reasons a firm may, under licence, take on or continue with the customer or the business or transaction in, to, or through such high-risk jurisdictions.

4.67 The firm must decide, on the basis of its assessment of the risks posed by different customer/product combinations, on the level of verification that should be applied at each level of risk presented by the customer. Consideration should be given to all the information a firm gathers about a customer, as part of the normal business and vetting processes.

Consideration of the overall information held may alter the risk profile of the customer.

4.68 Identifying a customer as carrying a higher risk of money laundering or terrorist financing does not automatically mean that he is a money launderer, or a financier of terrorism. Similarly, identifying a customer as carrying a low risk of money laundering or terrorist financing does not mean that the customer is not. Staff therefore need to be vigilant in using their experience and common sense in applying the firm's risk-based criteria and rules (see Chapter 7 – Staff awareness, training and alertness).

4.69 When the FCA issues a relevant thematic review report, or updates its *Financial Crime Guide*, as part of its ongoing review of its controls to manage and mitigate its ML/TF risks, a firm should consider how its systems, controls and procedures appear in relation to the self-assessment questions set out in the report. Firms should be aware of the FCA's published enforcement findings in relation to individual firms, and its actions in response to these - this information is available at https://www.fca.org.uk/about/enforcement.

A risk-based approach – Monitor and improve the effective operation of the firm's controls

Regulation 19(2)(b)
SYSC 6.3.8 R

4.70 The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities.

4.71 Independent testing of, and reporting on, the development and effective operation of the firm's RBA should be conducted by, for example, an internal audit function (where one is established), external auditors, specialist consultants or other qualified parties who are not involved in the implementation or operation of the firm's AML/CTF compliance programme.

SYSC 6.3.3 R

4.72 The firm will need to have some means of assessing that its risk mitigation procedures and controls are working effectively, or, if they are not, where they need to be improved. Its policies, controls and procedures will need to be kept under regular review. Aspects the firm will need to consider include:

- appropriate procedures to identify changes in customer characteristics, which come to light in the normal course of business;
- reviewing ways in which different products and services may be used for money laundering/terrorist financing purposes, and how these ways may change, supported by typologies/law enforcement feedback, etc;
- adequacy of staff training and awareness;
- monitoring compliance arrangements (such as internal audit/quality assurance processes or external review);
- where appropriate, the establishment of an internal audit function;

- the balance between technology-based and people-based systems;
- capturing appropriate management information;
- upward reporting and accountability;
- effectiveness of liaison with other parts of the firm; and
- effectiveness of the liaison with regulatory and law enforcement agencies.

4.73 When the FCA issues a relevant thematic review report, or updates its *Financial Crime Guide*, as part of its monitoring of the performance of its ML/TF/PF controls, a firm should consider whether any of the examples of poor practice have any resonance within the firm. Firms should be aware of the FCA's published enforcement findings in relation to individual firms, and its actions in response to these - this information is available at https://www.fca.org.uk/about/enforcement.

A risk-based approach – Record appropriately what has been done and why

SYSC 6.3.3 R
Regulation 18(4)

4.74 Firms must document their risk assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide appropriate risk assessment information to competent authorities.

4.75 Annex 4-III contains illustrative examples of systems and controls a firm might have in place in order to keep its risk assessments up to date.

4.76 The responses to consideration of the issues set out above, or to similar issues, will enable the firm to tailor its policies and procedures on the prevention of money laundering and terrorist financing. Documentation of those responses should enable the firm to demonstrate to its regulator and/or to a court:

- how it assesses the threats/risks of being used in connection with money laundering, terrorist financing and proliferation financing;
- how it agrees and implements the appropriate systems and procedures, including due diligence requirements, in the light of its risk assessment;
- how it monitors and, as necessary, improves the effectiveness of its systems and procedures; and
- the arrangements for reporting to senior management on the operation of its control processes.

4.77 In addition, on a case-by-case basis, firms should document the rationale for any additional due diligence measures it has undertaken (or any it has waived) compared to its standard approach, in view of its risk assessment of a particular customer.

Risk management is dynamic

SYSC 6.3.3 R

4.78 Risk management generally is a continuous process, carried out on a dynamic basis. A money laundering/terrorist financing/proliferation financing risk assessment is not a one-time exercise. Firms must therefore ensure that their risk management processes for managing money laundering, terrorist financing and proliferation financing risks are kept under regular review.

4.79 There is a need to monitor the environment within which the firm operates. Success in preventing ML/TF/PF in one area of operation or business will tend to drive criminals to migrate to another area, business, or product stream. Periodic assessment should therefore be made of activity in the firm's market place. If evidence suggests that displacement is happening, or if customer behaviour is changing, the firm should be considering what it should be doing differently to take account of these changes.

4.80 In a stable business change may occur slowly - most businesses are evolutionary. Customers' activities change (without always notifying the firm) and the firm's products and services – and the way these are offered or sold to customers – change. The products/transactions attacked by prospective money launderers, terrorist financiers and proliferation financiers will also vary as perceptions of their relative vulnerability change.

4.81 There is, however, a balance to be achieved between responding promptly to environmental changes, and maintaining stable systems and procedures.

4.82 A firm should therefore keep its risk assessment(s) up to date. An annual, formal reassessment might be too often in most cases, but still appropriate for a dynamic, growing business. It is recommended that a firm revisit its assessment at least annually, even if it decides that there is no case for revision. Firms should include details of the assessment, and any resulting changes, in the MLRO's annual report (see paragraphs 3.37 to 3.45).

Annex 4-I

CONSIDERATIONS IN ASSESSING THE LEVEL OF ML/TF RISK IN DIFFERENT JURISDICTIONS

1. This Annex is designed to assist firms by setting out how they might approach their assessment of other jurisdictions, to determine their level of ML/TF risk. The Annex discusses jurisdictions where there may be a presumption of low risk, and those where such a presumption may not be appropriate without further investigation. It then discusses issues that a firm should consider in all cases when coming to a judgment on the level of ML/TF risk implicit in any particular jurisdiction.

Implications of an assessment as low risk

2. Assessment of a jurisdiction as low risk only allows for some easement of the level of due diligence carried out – it is not a complete exemption from the application of CDD measures in respect of customer identification. It does not exempt the firm from carrying out ongoing monitoring of the business relationship with the customer, nor from the need for such other procedures (such as monitoring) as may be necessary to enable a firm to fulfil its responsibilities under the Proceeds of Crime Act 2002.
3. Although the judgment on the risk level is one to be made by each firm in the light of the particular circumstances, senior management is accountable for this judgment – either to its regulator, or, if necessary, to a court. It is therefore important that the reasons for concluding that a particular jurisdiction is low risk (other than those in respect of which a presumption of low risk may be made) are documented at the time the decision is made, and that it is made on relevant and up to date data or information.

Categories of country

(a) *EU/EEA member states*

4. When identifying lower risk jurisdictions, FATF encourages firms to take into consideration country risk factors:

   - Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems.
   - Countries identified by credible sources as having a low level of corruption or other criminal activity.

   In making a risk assessment, countries or financial institutions could, when appropriate, also take into account possible variations in money laundering and terrorist financing risk between different regions or areas within a country.

5. All Member States of the EU are required to enact legislation and financial

sector procedures in accordance with the EU Fourth Money Laundering Directive. The directive implements the revised 2012 FATF standards.

All EEA countries have undertaken to implement the fourth money laundering directive and all are members of FATF or the relevant FATF style regional body (for Europe, this is MONEYVAL).

6. Given the commitment to implement the Fourth Money Laundering Directive, firms may initially presume EU and EEA member states to be low risk; significant variations may however exist in the precise measures that have been taken to transpose the money laundering directive (and its predecessors) into national laws and regulations. Moreover, the effective implementation of the standards will also vary. Where firms have substantive information which indicates that a presumption of low risk cannot be sustained, either in general or for particular products, they will need to consider whether their procedures should be enhanced to take account of this information.

7. All FATF members, including members of FATF style regional bodies, undertake to implement the FATF anti-money laundering and counter-terrorism Recommendations as part of their membership obligations.

8. However, unlike the transposition of the money laundering directive by EU Member States, implementation cannot be mandatory, and all members will approach their obligations in different ways, and under different timetables.

9. Information on the effectiveness of implementation in these jurisdictions may be obtained through scrutiny of Mutual Evaluation reports, which are published on the FATF website, as well as through the FATF public statement, compliance statement and advisory notices issued by HM Treasury.

10. A majority of countries and territories do not fall within the lists of countries that can be presumed to be low risk. This does not necessarily mean that the AML/CTF legislation, and standards of due diligence, in those countries are lower than those in other jurisdictions assessed as low risk. However, standards vary significantly, and firms will need to carry out their own assessment of particular countries. In addition to a firm's own knowledge and experience of the country concerned, particular attention should be paid to any FATF-style or IMF/World Bank evaluations that have been undertaken.

11. As a result of due diligence carried out, therefore, for the purposes of determining those jurisdictions which, in the firm’s judgment, are low risk, firms may rely, for the purposes of carrying out CDD measures, on other regulated firms situated in such a jurisdiction.

Factors to be taken into account when assessing other jurisdictions

14. Factors include:

- Geographical risk factors
- Membership of groups that only admit those meeting a certain benchmark
- Contextual factors – political stability; level of (endemic) corruption etc
- Evidence of relevant (public) criticism of a jurisdiction, including HMT/FATF advisory notices
- Independent and public assessment of the jurisdiction's overall AML regime
- Need for any assessment to be recent
- Implementation standards (including quality and effectiveness of supervision)
- Incidence of trade with the jurisdiction – need to be proportionate especially where very small

Geographical risk factors

15. Geographical risk factors include:

- countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to counter money laundering or terrorist financing;
- countries identified by credible sources as having significant levels of corruption or other criminal activity, such as terrorism, money laundering, and the production and supply of illicit drugs;
- countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;
- countries providing funding or support for terrorism;
- countries that have organisations operating within their territory which have been designated—
    - by the government of the United Kingdom as proscribed organisations under Schedule 2 to the Terrorism Act 2000, or
    - by other countries, international organisations or the European Union as terrorist organisations;

Firms should bear in mind that the presence of one or more risk factors may not always indicate that there is a high risk of money laundering or terrorist financing in a particular situation.

Membership of an international or regional 'group'

16. There are a number of international and regional 'groups' of jurisdictions that admit to membership only those jurisdictions that have demonstrated a commitment to the fight against money laundering and terrorist financing, and which have an appropriate legal and regulatory regime to back up this commitment.

Contextual factors

17. Such factors as the political stability of a jurisdiction, and where it stands in tables of corruption are relevant to whether it is likely that a jurisdiction will be low risk. It will, however, seldom be easy for firms to make their own assessments of such matters, and it is likely that they will have

to rely on external agencies for such evidence – whether prepared for general consumption, or specifically for the firm. Where the firm looks to publicly available evidence, it will be important that it has some knowledge of the criteria that were used in making the assessment; the firm cannot rely solely on the fact that such a list has been independently prepared, even if by a respected third party agency.

Evidence of relevant (public) criticism

18. The FATF from time to time issues statements on its concerns about the lack of comprehensive AML/CTF/CPF systems in a number of jurisdictions. When constructing their internal procedures, therefore, financial sector firms should have regard to the need for additional monitoring procedures for transactions from any country that is listed on these statements of concern. Additional monitoring procedures will also be required in respect of correspondent relationships with financial institutions from such countries.

19. Other, commercial agencies also produce reports and lists of jurisdictions, entities and individuals that are involved, or that are alleged to be involved, in activities that cast doubt on their integrity in the AML/CTF area. Such reports lists can provide some useful and relevant evidence – which may or may not be conclusive – on whether or not a particular jurisdiction is likely to be low risk.

Mutual evaluation reports

20. Particular attention should be paid to assessments that have been undertaken by standard setting bodies such as FATF, and by international financial institutions such as the IMF.

FATF

21. FATF member countries monitor their own progress in the fight against money laundering and terrorist financing through regular mutual evaluation by their peers. In 1998, FATF extended the concept of mutual evaluation beyond its own membership through its endorsement of FATF-style mutual evaluation programmes of a number of regional groups which contain non-FATF members. The groups undertaking FATF-style mutual evaluations are

    - the Group of International Finance Centre Supervisors (GIFCA) see www.groupgifcs.org
    - the Caribbean Financial Action Task Force (CFATF) see www.cfatf.org
    - the Asia/Pacific Group on Money Laundering (APG) see www.apgml.org
    - MONEYVAL, covering the Council of Europe countries which are not members of FATF see www.coe.int/Moneyval
    - the Financial Action Task Force on Money Laundering of Latin America (GAFILAT) see www.gafisud.org
    - the Middle East and North Africa Financial Action Task Force (MENAFATF) see www.menafatf.org
    - the Eurasian Group (EAG) see www.eurasiangroup.org,
    - the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) see www.esaamlg.org
    - the Intergovernmental Action Group against Money-Laundering in West Africa (GIABA) see www.giaba.org
    - Task Force on Money Laundering in Central Africa (GABAC) see https://gabac.org

22. Firms should bear in mind that mutual evaluation reports are at a 'point in time', and should be interpreted as such. Although follow up actions are usually reviewed after two years, there can be quite long intervals between evaluation reports in respect of a particular jurisdiction. Even at the point an evaluation is carried out there can be changes in train to the jurisdiction's AML/CTF

regime, but these will not be reflected in the evaluation report. There can also be subsequent changes to the regime (whether to respond to criticisms by the evaluators or otherwise) which firms should seek to understand and to factor into their assessment of whether the jurisdiction is low risk.

23. In assessing the conclusions of a mutual evaluation report, firms may find it difficult to give appropriate weighting to findings and conclusions in respect of the jurisdiction's compliance with particular Recommendations. For the purposes of assessing level of risk, compliance (or otherwise) with certain Recommendations may have more relevance than others. The extent to which a jurisdiction complies with the following Recommendations may be particularly relevant:

Legal framework:
Recommendations 1, 3, 4 and 5
Measures to be taken by firms:
Recommendations 9, 10, 11, 17 and 20,
Supervisory regime:
Recommendations 26, 27 and 35
International co-operation:
Recommendations 2 and 40

24. Summaries of FATF and FATF-style evaluations are published in FATF Annual Reports and can be accessed at www.fatf-gafi.org. However, mutual evaluation reports prepared by some FATF-style regional bodies may not be carried out fully to FATF standards, and firms should bear this in mind if a decision on whether a jurisdiction is low risk is based on such reports.

IMF/World Bank

25. As part of their financial stability assessments of countries and territories, the IMF and the World Bank have agreed with FATF a detailed methodology for assessing compliance with AML/CTF standards, using the FATF Recommendations as the base. A number of countries have already undergone IMF/World Bank assessments in addition to those carried out by FATF, and some of the results can be accessed at www.imf.org. Where IMF/World Bank assessments relate to FATF members, the assessments are formally adopted by the FATF and appear on the FATF website.

Implementation standards (including effectiveness of supervision)

26. Information on the extent and quality of supervision of AML/CTF standards may be obtained from the extent to which a jurisdiction complies with Recommendations 17, 23, 29 and 30.

Incidence of trade with the jurisdiction

27. In respect of any particular jurisdiction, the level and extent of due diligence that needs to be carried out in making a judgment on the level of risk will be influenced by the volume and size of the firm's business with that jurisdiction in relation to the firm's overall business.

UK prohibition notices and advisory notices

Prohibition notices

28. Under certain circumstances, HM Treasury may, pursuant to the Counter-terrorism Act 2008, Schedule 7, issue directions to a firm in relation to customer due diligence; ongoing monitoring; systematic reporting; and limiting or ceasing business. Details of any such HM Treasury directions will be found at www.hm-treasury.gov.uk.

Advisory notices

HM Treasury

29. HM Treasury issues advisory notices in which it expresses the UK's full support of the work of the FATF on jurisdictions of concern. The HM Treasury advisory notice is available at https://www.gov.uk/government/publications/money-laundering-and-terrorist-financing-controls-in-overseas-jurisdictions-advisory-notice.

30. The FATF issues periodic announcements about its concerns regarding the lack of comprehensive AML/CTF systems in various jurisdictions.

31. The FATF maintains two lists that identify countries with strategic deficiencies in the areas of anti-money laundering, counter terrorist financing or counter proliferation financing:

    1. High-risk Jurisdictions Subject to a Call for Action.

    2. Jurisdictions under Increased Monitoring.

32. The FATF also maintains a statement *Improving Global AML/CTF Compliance: On-going Process*, which lists jurisdictions identified as having strategic AML/CTF deficiencies for which they have developed an action plan with the FATF. While the situations differ among jurisdictions, each has provided a written high-level political commitment to address the identified deficiencies. The FATF will closely monitor the implementation of these action plans and encourages its members to consider the information set out in the statement.

33. The latest versions of these FATF documents are available at http://www.fatf-gafi.org.

34. In the UK, the ML Regulations determine that a FATF call for action country is a country named on the list of High-Risk Jurisdictions subject to a Call for Action per 31.1 above.

FCA

34. The FCA expect firms they supervise for money laundering purposes to consider the impact of these documents on their policies and procedures.

ANNEX 4-II

ILLUSTRATIVE RISK FACTORS RELATING TO CUSTOMER SITUATIONS

Note: These are risk factors that may be relevant for consideration during the course of risk assessments but do not automatically indicate a higher risk.

I. CUSTOMER RISK FACTORS

A. Business or professional activity

Risk factors that may be relevant when considering the risk associated with a customer's or their beneficial owners' business or professional activity include:

• Does the customer or beneficial owner have links to sectors that are associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, arms trade and defence, extractive industries and public procurement?

• Does the customer or beneficial owner have links to sectors that are associated with higher ML, TF or PF risk, for example certain Money Service Businesses, casinos or dealers in precious metals of the defence industry?

• Does the customer or beneficial owner have links to sectors that involve significant amounts of cash?

• Where the customer is a legal person, what is the purpose of their establishment? For example, what is the nature of their business?

• Does the customer have political connections, for example, are they a Politically Exposed Person (PEP), or is their beneficial owner a PEP? Does the customer or beneficial owner have any other relevant links to a PEP, for example, are any of the customer's directors PEPs and if so, do these PEPs exercise significant control over the customer or beneficial owner? In what jurisdiction is the PEP, their business or a business they are connected with, located?*

• Does the customer or beneficial owner hold another public position that might enable them to abuse public office for private gain? For example, are they senior or regional public figures with the ability to influence the awarding of contracts, decision-making members of high profile sporting bodies or individuals that are known to influence the government and other senior decision-makers?

• Is the customer a legal person subject to enforceable disclosure requirements that ensure that reliable information about the customer's beneficial owner is publicly available, for example public companies listed on stock exchanges that make such disclosure a condition for listing?

• Is the customer a credit or financial institution from a jurisdiction with an effective AML/CTF regime and is it supervised for compliance with local AML/CTF obligations? Is there evidence that the customer has been subject to supervisory sanctions or enforcement for failure to comply with AML/CTF obligations or wider conduct requirements in recent years?

---

* Domestic PEPs have an inherently lower risk (ML Reg 35(3A))

• Is the customer a public administration or enterprise from a jurisdiction with low levels of corruption?

• Is the customer's or their beneficial owner's background consistent with what the firm knows about their former, current or planned business activity, their business' turnover, the source of funds and the customer's or beneficial owner's source of wealth?

• Is the customer a beneficiary of a life insurance policy (that the firm has become aware of) in situations where there may be an increased risk, for example complex products with potential multiple investment accounts or those that allow for early surrender and have a surrender value, or beneficiaries with no obvious links to the policy holder?

• Is the customer a third country national who is applying for residence rights in or citizenship of an EEA state in exchange for transfers of capital, purchase of property, government bonds, or investment in corporate entities in that EEA state?

B. Reputation

The following risk factors may be relevant when considering the risk associated with a customer's or their beneficial owners' reputation**:**

• Are there any adverse media reports or other relevant information sources about the customer? For example, are there any allegations of criminality or terrorism against the customer or their beneficial owners? If so, are these credible? Firms should determine the credibility of allegations on the basis of the quality and independence of the source data and the persistence of reporting of these allegations, among others. The absence of criminal convictions alone may not be sufficient to dismiss allegations of wrongdoing.

• Has the customer, beneficial owner or anyone publicly known to be closely associated with them had their assets frozen due to administrative or criminal proceedings or allegations of terrorism, terrorist financing, or proliferation financing? Does the firm have reasonable grounds to suspect that the customer or beneficial owner or anyone publicly known to be associated with them has, at some point in the past, been subject to such an asset freeze?

• Does the firm know if the customer or beneficial owner has been subject to a suspicious activity report in the past?

• Does the firm have any in-house information about the customer's or their beneficial owner's integrity, obtained, for example, in the course of a long-standing business relationship?

C. Nature and behaviour

The following risk factors may be relevant when considering the risk associated with a customer's or their beneficial owners' nature and behaviour (not all of these risk factors will be apparent at the outset, but may emerge only once a business relationship has been established):

• Does the customer have legitimate reasons for being unable to provide robust evidence of their identity, perhaps because they are an asylum seeker?

• Does the firm have any doubts about the veracity or accuracy of the customer's or beneficial owner's identity?

• Are there indications that the customer might seek to avoid the establishment of a business relationship? For example, does the customer look to carry out one or several one-off transactions where the establishment of a business relationship might make more economic sense?

• Is the customer's ownership and control structure transparent and does it make sense?If the customer's ownership and control structure is complex or opaque, is there an obvious commercial or lawful rationale?

• Does the customer issue bearer shares or have nominee shareholders?

• Is the customer a legal person or arrangement that could be used as an asset holding vehicle?

• Is there a sound reason for changes in the customer's ownership and control structure?

• Does the customer request transactions that are unusually complex, unusually or unexpectedly large or have an unusual or unexpected pattern without apparent economic or lawful purpose or a sound commercial rationale? Are there grounds to suspect that the customer is trying to evade certain thresholds?

• Does the customer request unnecessary or unreasonable levels of secrecy? For example, is the customer reluctant to share CDD information, or do they appear to disguise the true nature of their business?

• Can the customer's or beneficial owner's source of wealth or source of funds be easily explained, for example through their occupation, inheritance or investments?

• Does the customer use their products and services as expected when the business relationship was first established?

• Where the customer is a non-resident, could their needs be better serviced elsewhere?Is there a sound economic or lawful rationale for the customer requesting the type of financial service sought?

• Is the customer a non-profit organisation whose activities expose it to particularly high risks of abuse for terrorist financing purposes?

II. COUNTRIES AND GEOGRAPHIC AREAS FACTORS

When identifying the risk associated with countries and geographic areas, firms should consider the risk related to:

a) the jurisdiction in which the customer or beneficial owner is based;

b) the jurisdictions which are the customer´s or beneficial owner's main place of business; and

c) the jurisdiction to which the customer or beneficial owner has relevant personal links.

Annex 4-I sets out further guidance on considerations firms might take account of in assessing the level of ML/TF/PF risk in different jurisdictions.

III. PRODUCTS, SERVICES AND TRANSACTIONS RISK FACTORS

When identifying the risk associated with their products, services or transactions, firms should consider the risk related to:

a) the level of transparency, or opaqueness, the product, service or transaction afford;

b) the complexity of the product, service or transaction; and

c) the value or size of the product, service or transaction.

Risk factors that may be relevant when considering the risk associated with a product, service or transaction's transparency include:

• To what extent do products or services facilitate or allow anonymity or opaqueness of customer, ownership or beneficiary structures, for example pooled accounts, bearer shares, fiduciary deposits, offshore and certain trusts, or legal entities like foundations that are structured in a way to take advantage of anonymity and dealings with shell companies or companies with nominee shareholders that could be abused for illicit purposes?

• To what extent is it possible for a third party that is not part of the business relationship to give instructions, *e.g.* certain correspondent banking relationships?

Risk factors that may be relevant when considering the risk associated with a product, service or transaction's complexity include:

• To what extent is the transaction complex and involves multiple parties or multiple jurisdictions, for example certain trade finance transactions? Are transactions straightforward, for example regular payments into a pension fund?

• To what extent do products or services allow payments from third parties or accept overpayments where this is not normally foreseen? Where third party payments are foreseen, does the firm know the third party's identity, for example a state benefit authority or a guarantor? Or are products and services funded exclusively by fund transfers from the customer's own account at another financial institution that is subject to AML/CTF standards and oversight that are comparable to those required under the UK regime?

• Does the firm understand the risks associated with its new or innovative product or service, in particular where this involves the use of new technologies or payment methods?

Risk factors that may be relevant when considering the risk associated with a product, service or transaction's value or size include:

• To what extent are products or services cash intensive, such as many payment services but also certain current accounts?

• To what extent do products or services facilitate or encourage high value transactions?Are there any caps on transaction values or levels of premium that could limit the use of the product or service for money laundering or terrorist financing purposes?

• Is there a transaction related to oil, arms, precious metals, tobacco products, cultural artefacts, ivory and other items related to protected species, and other items of archaeological, historical, cultural and religious significance, or of rare scientific value, where the ML/TF risk is raised? See below.

Firms should consider all relevant information at their disposal concerning ML/TF risks arising from transactions listed in ML Regulation 33 (6)(b)(vii) and consider their exposure to potential high-risk transactions involving these items, as identified through undertaking risk based CDD measures on their customers.

"Transaction" involves two parties who are making or benefiting from the transaction, or executing it (the customer and the firm), and includes a firm facilitating a transaction between two third parties.

A risk-based approach should be adopted in the interpretation of "related to". Where such a transaction is identified, firms should consider the closeness of the relationship or link between the item and the transaction, as well as between the transaction and the customer and/or firm.

Transactions should be considered on a risk basis in all instances and the below are not exhaustive examples of scope:

Oil: Transactions made to and/or from parties in the oil production process, including the sale of oil to exploration companies and refiners. Firms should consider terrorist financing methodologies. Retail customers purchasing refined oil products from petrol retailers should not be included. See also FATF Reports.[16]

Arms: Transactions such as those relating to a trade in live firearms or customers involved in the arms trade should be considered.

Precious metals: Transactions involving large-medium scale industrial miners to/from PEPs should be considered, as well as those made by refineries to their suppliers and wholesalers or vice versa. EDD should be considered on transactions involving gold recyclers and jewellers on a risk basis. See FATF's 2015 Report (https://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-risks-vulnerabilities-associated-with-gold.pdf).

Tobacco Products: Transactions involving wholesalers and their suppliers rather than retail sale of tobacco to the public should be considered, as well as identified risks such as "boot legging". See FATF's 2012 Tobacco Report https://www.fatf-gafi.org/media/fatf/documents/reports/Illicit%20Tobacco%20Trade.pdf).

Cultural artefacts or other items of archaeological, historical, cultural or religious significance or of rare scientific value: Firms should adopt definitions of these items considering Annex 1 of the EU's 2019 Regulation on the Import of Cultural Goods and consider the ML/TF risks identified in the EU's

[16] https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf; http://www.fatf-gafi.org/media/fatf/documents/reports/Specific%20Risk%20Factors%20in%20the%20Laundering%20of%20Proceeds%20of%20Corruption.pdf

2019 Supra National Risk Assessment. [17] This includes the looting and trafficking of antiquities and other artefacts.

Ivory or other items related to protected species: Firms should consider the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) definitions of ivory and other protected species. EDD should be performed on transactions involves CITES items on a risk basis of potential illegal wildlife trafficking (IWT). IWT can mean the domestic or international trade of CITES species in contravention of national or international laws.

Specific considerations could include:

- In/outbound transactions involving zoos, pet stores involved in the sales of animals, safari companies, hunting reserves, timber importers. Large deposits/withdrawals from government officials who work in environment or other related government departments that have oversight of government stockpiles of seized ivory, rhino horn, timber, or those working in forestry agencies, wildlife management authorities, or CITES Management Authorities.
- Transactions involving Asian nationals operating import/export, international trading, or transport companies in Africa and suspected of transporting CITES products.

Examples of transactions involving traders who may sell CITES products indirectly, and are not subject to EDD include: cosmetic retailers who may sell products containing fragments of orchid or cacti; food retailers who may sell products containing caviar extract; musical instrument manufacturers who may sell products containing rosewood or ivory.

IV. DELIVERY CHANNEL RISK FACTORS

When identifying the risk associated with the way the customer obtains the products or services they require, firms should consider the risk related to:

a) the extent to which the business relationship is conducted on a non-face to face basis without appropriate controls in place; and

b) any introducers or intermediaries the firm might use and the nature of their relationship to the firm.

When assessing the risk associated with the way the customer obtains the product or services, firms should consider a number of factors including:

• Is the customer physically present for identification purposes? If they are not, has the firm used a reliable form of non-face to face CDD? Has it taken steps to prevent impersonation or identity fraud? Has the firm used an electronic identification process that is secure from fraud and misuse and capable of providing an appropriate level of assurance?

• Has the customer been introduced from other parts of the same financial group and if so, to what extent can the firm rely on this introduction as reassurance that the customer will not expose the firm to excessive ML/TF/PF risk? What has the firm done to satisfy itself that the group entity applies CDD measures to UK standards?

[17] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0001.01.ENG; https://ec.europa.eu/info/files/supranational-risk-assessment-money-laundering-and-terrorist-financing-risks-affecting-union_en

• Has the customer been introduced from a third party, for example a bank that is not part of the same group, and is the third party a financial institution or is their main business activity unrelated to financial service provision? What has the firm done to be satisfied that:

i. the third party applies CDD measures and keeps records to UK standards and that it is supervised for compliance with comparable AML/CTF obligations in line with UK requirements?

ii. the third party will provide, immediately upon request, relevant copies of identification and verification data, among others in line with UK requirements? and

iii. the quality of the third party's CDD measures is such that it can be relied upon?

• Has the customer been introduced through a tied agent, i.e. without direct firm contact? To what extent can the firm be satisfied that the agent has obtained enough information so that the firm knows its customer and the level of risk associated with the business relationship?

• If independent or tied agents are used, to what extent are they involved on an ongoing basis in the conduct of business? How does this affect the firm's knowledge of the customer and ongoing risk management?

• Where a firm uses an intermediary, are they:

i. a regulated person subject to AML obligations that are consistent with those of the UK regime?

ii. subject to effective AML supervision? Are there any indications that the intermediary's level of compliance with applicable AML legislation or regulation is inadequate, for example because the intermediary has been sanctioned for breaches of AML/CTF obligations?

iii. based in a jurisdiction associated with higher ML/TF/PF risk? Where a third party is based in a FATF call for action country, firms must not rely on that intermediary. However, reliance may be possible provided that the intermediary is a branch or majority-owned subsidiary undertaking of another firm established outside the UK, and the firm is confident that the intermediary fully complies with group wide policies, controls and procedures in line with UK requirements.

Note: With effect from 1 September 2023, firms must take appropriate steps to identify and assess the risks of proliferation financing to which its business is subject, and establish and maintain policies, controls and procedures to mitigate and manage these risks (The Money Laundering and Terrorist Financing (Amendment)(No.2) Regulations 2022 Reg 18A. See also Part II Sector 15 Annex 15-V.

ANNEX 4-III

CONSIDERATIONS IN KEEPING RISK ASSESSMENTS UP TO DATE

Firms should keep their assessment of ML/TF/PF risk associated with individual business relationships and occasional transactions, as well as the underlying factors, under review to ensure their assessment of ML/TF/PF risk remains up to date and relevant. Firms should assess information obtained as part of their ongoing monitoring of the business relationship and consider whether this affects the risk assessment.

Firms should also ensure that they have systems and controls in place to identify emerging ML/TF/PF risks and that they can assess and, where appropriate, incorporate these in their business-wide and individual risk assessments in a timely manner.

Examples of systems and controls firms should put in place to identify emerging risks include:

- processes to ensure internal information is reviewed regularly to identify trends and emerging issues, both in relation to individual business relationships and the firm's business;

- processes to ensure the firm regularly reviews relevant information sources. This should involve, in particular:

  i. regularly reviewing media reports that are relevant to the sectors or jurisdictions the firm is active in;

  ii. regularly reviewing law enforcement alerts and reports;

  iii ensuring that the firm becomes aware of changes to terror alerts and sanctions regimes as soon as they occur, for example by regularly reviewing terror alerts an looking for sanctions regime updates; and

  iv. regularly reviewing thematic reviews and similar publications issued by competent authorities.

- processes to capture and reviewing information on risks relating to new products;

- engagement with other industry representatives and competent authorities (such as round tables, conferences and training) and processes to feed back any findings to relevant staff; and

- establishing a culture of information sharing within the firm and strong company ethics.

Examples of systems and controls firms should put in place to ensure their individual and business-wide risk assessment remains up to date include:

- setting a date at which the next risk assessment update takes place, *e.g.* on the 1 March every year, to ensure new or emerging risks are included in the risk assessment. Where the firm is aware that a new risk has emerged, or an existing one has increased, this should be reflected in the risk assessment as soon as possible; and

- carefully recording issues throughout the year that could have a bearing on the risk assessment, such as internal suspicious transaction reports, compliance failures and intelligence from front office staff.

Like the original risk assessments, any update of a risk assessment and adjustment of accompanying CDD measures should be proportionate and commensurate with the ML/TF/PF risk.

CHAPTER 5

CUSTOMER DUE DILIGENCE

- **Relevant UK law/regulation**
  - Regulations 4-6, 27-38
  - POCA ss 330 – 331, 334(2), 342
  - Terrorism Act
  - Counter-terrorism Act 2008, Schedule 7
  - Financial sanctions legislation
- **Customers that may not be dealt with**
  - UN Sanctions resolutions 1267 (1999), 1373 (2001), 1333 (2002), 1390 (2002) and 1617 (2005) *(For updates see https://www.un.org/securitycouncil/sanctions/information)*
  - EC Regulation 2580/2001, 881/2002 (as amended), 423/2007 and 1110/2008
  - EU Regulation 2016/1686
  - Terrorism Act, 2000, Sch 2
  - Terrorism (United Nations Measures) Orders 2006 and 2009
  - Al-Qa'ida and Taliban (United Nations Measures) Order 2006
  - HM Treasury Sanctions Lists
- **Regulatory regime**
  - SYSC 6.1.1 R, 6.3.7(5) G
  - FCA Financial Crime Guide
  - FCA PEPs guidance
- **Other material pointing to good practice**
  - FATF Recommendations
  - FATF Guidance on the risk-based approach: High level principles and procedures
  - Basel paper – *Sound management of risks related to money laundering and financing of terrorism*
  - IAIS Guidance Paper 5
  - IOSCO Principles paper
  - ESA Risk Factor Guidelines

- **Core obligations**
  - Must carry out prescribed CDD measures for all customers not covered by exemptions
  - Must have systems to deal with identification issues in relation to those who cannot produce the standard evidence
  - Must take a risk-based approach when applying enhanced due diligence to take account of the greater potential for money laundering in higher risk cases, specifically in respect of PEPs and correspondent relationships
  - Some persons/entities must not be dealt with
  - Must have specific policies in relation to the financially (and socially) excluded
  - If satisfactory evidence of identity is not obtained, the business relationship must not proceed further
  - Must have some system for keeping customer information up to date

5.1 Meaning of customer due diligence measures and ongoing monitoring

5.1.1 The ML Regulations 2017 (as amended) specify CDD measures that are required to be carried out, and the timing, as well as actions required if CDD measures are not carried out. The Regulations then describe circumstances in which limited CDD measures are permitted (referred to as 'Simplified Due Diligence'), and those customers and circumstances where enhanced

due diligence is required. Provision for reliance on other regulated firms in the carrying out of CDD measures are then set out.

5.1.2 Schedule 7 to the Counter-terrorism Act 2008 gives HM Treasury power to require firms, in particular circumstances, to carry out enhanced CDD and monitoring. Details of any such HM Treasury directions will be found at www.hm-treasury.gov.uk.

5.1.3 This chapter therefore gives guidance on the following:

- The meaning of CDD measures (5.1.5 – 5.1.15)
- Timing of, and non-compliance with, CDD measures (5.2.1 – 5.2.13)
- Application of CDD measures (section 5.3)
- Simplified due diligence (section 5.4)
- Enhanced due diligence (section 5.5)
- Reliance on third parties and multipartite relationships (section 5.6)
- Monitoring customer activity (section 5.7)

Regulation 28(12),(16)

5.1.4 Firms must determine the extent of their CDD measures and ongoing monitoring on a risk-sensitive basis, depending on the type of customer, business relationship, product or transaction. They must be able to demonstrate to their supervisory authority that the extent of their CDD measures and monitoring is appropriate in view of the risks of money laundering and terrorist financing.

What is customer due diligence?

Regulation 28(1), (2)

5.1.5 The CDD measures that must be carried out involve:

(a) identifying the customer, and verifying his identity (see paragraphs 5.3.2ff**);**
(b) identifying the beneficial owner, where relevant, and verifying his identity (see paragraphs 5.3.8ff)**;** and
(c) assessing, and where appropriate obtaining information on, the purpose and intended nature of the business relationship or transaction (see paragraphs 5.3.23ff**)**.

Regulation 28(4)(c), (5), (3A)

5.1.6 Where the customer or beneficial owner is a legal person (other than a company listed on a regulated market), trust, company, foundation or similar legal arrangement, firms must take reasonable measures to understand the ownership and control structure of that legal person, trust, company, foundation or legal arrangement.

5.1.7 Working out who is a beneficial owner may not be a straightforward matter. Different rules apply to different forms of entity (see paragraphs 5.3.8ff).

Regulations 33-38

5.1.8 For some business relationships, determined by the firm to present a low degree of risk of ML/TF, simplified due diligence (SDD) may be applied; in the case of higher risk situations, and specifically in relation to PEPs or correspondent relationships with third country respondents, enhanced due diligence (EDD) measures must be applied on a risk sensitive basis.

- for guidance on applying SDD see section 5.4
- for guidance on applying EDD see section 5.5

What is ongoing monitoring?

Regulation 28(11)

5.1.9 Firms must conduct ongoing monitoring of the business relationship with their customers (section 5.7), including the scrutiny of transactions undertaken throughout the course of the relationship and keeping CDD information up to date. This is a separate, but related, obligation from the requirement to apply CDD measures.

Why is it necessary to apply CDD measures and conduct ongoing monitoring?

Regulations 27, 28
POCA, ss 327-334
Terrorism Act s 21A

5.1.10 The CDD and monitoring obligations on firms under legislation and regulation are designed to make it more difficult for the financial services industry to be used for money laundering or terrorist financing.

5.1.11 Firms also need to know who their customers are to guard against fraud, including impersonation fraud, and the risk of committing offences under POCA and the Terrorism Act, relating to money laundering and terrorist financing.

Criminal Finances Act

5.1.12 Tax evasion is a predicate offence leading to money laundering. Failing to report knowledge or suspicions relating to such an activity is an offence committed by a firm.

5.1.13 Firms therefore need to carry out customer due diligence, and monitoring, for two broad reasons:

- to help the firm, at the time due diligence is carried out, to be reasonably satisfied that customers are who they say they are, to know whether they are acting on behalf of another, and that there is no legal barrier (e.g. government sanctions) to providing them with the product or service requested; and
- to enable the firm to assist law enforcement, by providing available information on customers or activities being investigated.

5.1.14 It may often be appropriate for the firm to know rather more about the customer than his identity: it will, for example, often need to be aware of the nature of the customer's business or activities in order to assess the extent to which his transactions and activity undertaken with or through the firm is consistent with that business.

Other material, pointing to good practice

5.1.15 FATF, the Basel Committee, IAIS and IOSCO have issued recommendations on the steps that should be taken to identify customers. FATF has also published guidance on high level principles and procedures on the risk-based approach. The Basel Committee's recommendations comprise a set of guidelines on the *Sound management of risks relating to money laundering and financing of terrorism*. Although the Basel paper is addressed to banks, the IAIS Guidance Paper 5 to insurance entities, and IOSCO's Principles paper to the securities industry, their principles are worth considering by providers of other forms of financial services. These recommendations are available at: www.fatf-gafi.org; www.bis.org; www.iaisweb.org; www.iosco.org. Where relevant, firms are encouraged to use these websites to keep up to date with developing industry guidance

from these bodies. The private sector Wolfsberg Group has also issued relevant material, see www.wolfsberg-principles.com.

5.2 Timing of, and non-compliance with, CDD measures

Regulation 27(1) 5.2.1 A firm must apply CDD measures when it does any of the following:

(a) establishes a business relationship;
(b) carries out an occasional transaction;
(c) suspects money laundering or terrorist financing; or
(d) doubts the veracity of documents or information previously obtained for the purpose of identification or verification.

Timing of verification

Regulation 30(2) 5.2.2 **General rule**: The verification of the identity of the customer and, where applicable, the beneficial owner, must, subject to the exceptions referred to below, take place before the establishment of a business relationship or the carrying out of a transaction.

Regulation 30(3) 5.2.3 **Exception if necessary not to interrupt normal business and there is little risk:** In any other case, verification of the identity of the customer, and where there is one, the beneficial owner, may be completed during the establishment of a business relationship if

(a) this is necessary not to interrupt the normal conduct of business and
(b) there is little risk of money laundering or terrorist financing occurring

provided that the verification is completed as soon as practicable after contact is first established.

Regulation 30(4),(5) 5.2.4 **Exception when opening an account:** The verification of the identity of a customer (or beneficial owner, if there is one) opening an account may take place after the account (including an account which permits transactions in transferable securities) has been opened, provided that there are adequate safeguards in place to ensure that no transactions are carried out by or on behalf of the customer before verification has been completed.

See Revisions Sept 2026
Insertion of 5.2.4A

Regulation 30(6),(7) 5.2.5 **Other exceptions:** Where a firm is required to apply CDD measures in the case of a trust, a legal entity (other than a body corporate) or a legal arrangement (other than a trust), and the beneficiaries of that trust, entity or arrangement are designated as a class, or by reference to particular characteristics, the firm must establish and verify the identity of the beneficiary before –

- any payment is made to the beneficiary, or
- the beneficiary exercises its vested rights in the trust, entity or legal arrangement.

Requirement to cease transactions, etc

Regulation 31(1)

5.2.6 Where a firm is unable to apply CDD measures in relation to a customer, the firm

(a) must not carry out a transaction through a bank account with or on behalf of the customer;
(b) must not establish a business relationship or carry out a transaction with the customer otherwise than through a bank account;
(c) must terminate any existing business relationship with the customer;
(d) must consider whether it ought to be making a report to the NCA, in accordance with its obligations under POCA and the Terrorism Act.

5.2.7 Firms should always consider whether an inability to apply CDD measures is caused by the customer not possessing the 'right' documents or information. In this case, the firm should consider whether there are any other ways of being reasonably satisfied as to the customer's identity. In either case, the firm should consider whether there are any circumstances which give grounds for making a report.

Regulation 31(1), (2)

5.2.8 If the firm concludes that the circumstances do give reasonable grounds for knowledge or suspicion of money laundering or terrorist financing, a report must be made to the NCA (see Chapter 6). The firm must then retain the funds until consent has been given to return the funds to the source from which they came.

Regulation 31(2)

5.2.9 If the firm concludes that there are no grounds for making a report, it will need to decide on the appropriate course of action. This may be to retain the funds while it seeks other ways of being reasonably satisfied as to the customer's identity, or to return the funds to the source from which they came. Returning the funds in such a circumstance is part of the process of terminating the relationship; it is closing the account, rather than carrying out a transaction with the customer through a bank account.

Electronic transfer of funds

EC Regulation 2015/847

5.2.10 To implement FATF Recommendation 16, the EU adopted Regulation 2015/847, which came into force on 26 June 2017, and is directly applicable in all member states. The Regulation requires that payment services providers (PSPs) must include certain information in electronic funds transfers and ensure that the information is verified. The core requirement is that the payer's name, address and account number, and the name and payment account number of the payee, are included in the transfer, but there are a number of permitted exemptions, concessions and variations. For guidance on how to meet the obligations under the Regulation, see Part III, Specialist Guidance 1: *Wire transfers*.

5.2.11 The Regulation includes (among others) the following definitions:

- 'Payer' means a person that holds a payment account and allows a transfer of funds from that payment account, or where there is no payment account, that gives a transfer of funds order.
- 'Payee' means a person that is the intended recipient of the transfer of funds

- 'Payment service provider' means a natural or legal person (as defined) providing transfer of funds services.
- 'Intermediary payment service provider' means a payment service provider that is not the payment service provider of the payer or of the payee and that receives and transmits a transfer of funds on behalf of the payment service provider of the payer or of the payee or of another intermediate payment service provider.

5.2.12 Accordingly, a financial sector business needs to consider which role it is fulfilling when it is involved in a payment chain. For example, a bank or building society effecting an electronic funds transfer on the direct instructions of a customer to the debit of that customer's account will clearly be a PSP whether it undertakes the payment itself (when it must provide its customer's details as the payer), or via an intermediary PSP. In the latter case it must provide the required information on its customer and payee to the intermediary PSP including when it inputs the payment through an electronic banking product supplied by the intermediary PSP.

5.2.13 In other circumstances when a financial sector business, whether independent of the PSP or a specialist function within the same group, passes the transaction through an account in its own name, it may reasonably consider itself under the above definitions as the payer, rather than the PSP, even though the transaction relates ultimately to a customer, e.g., mortgages, documentary credits, insurance claims, financial markets trades. In these cases, if XYZ is the name of the financial sector business initiating the transfer as a customer of the PSP, XYZ can input its own name if using an electronic banking product. There is nothing in the Regulation to prevent including the name of the underlying client elsewhere in the transfer, if XYZ wishes to do so.

5.3 Application of CDD measures

Regulation 28(1)

5.3.1 Applying CDD measures involves several steps. The firm is required to verify the identity of customers and, where applicable, beneficial owners. The purpose and intended nature of the business relationship must also be assessed, and if appropriate, information on this obtained.

Identification and verification of the customer

Regulation 28(2)(a)

5.3.2 The firm *identifies* the customer by obtaining a range of information about him. The *verification* of the identity consists of the firm verifying some of this information against documents or information obtained from a reliable source which is independent of the customer.

5.3.3 The term ‘customer’ is not defined in the ML Regulations, and its meaning has to be inferred from the definitions of ‘business relationship’ and ‘occasional transaction’, the context in which it is used in the ML Regulations, and its everyday dictionary meaning. It should be noted that for AML/CTF purposes, a ‘customer’ may be wider than the FCA Glossary definition of ‘customer’.

5.3.4 In general, the customer will be the party, or parties, with whom the business relationship is established, or for whom the transaction is carried

out. Where, however, there are several parties to a transaction, not all will necessarily be customers. Further, more specific, guidance for relevant sectors is given in Part II. Section 5.6 is also relevant in this context.

Regulation 4

5.3.5 A "business relationship" is defined in the ML Regulations as a business, professional or commercial relationship between a firm and a customer, which is connected to the business of the firm, and is expected by the firm at the time when contact is established to have an element of duration. A relationship need not involve the firm in an actual transaction; giving advice may often constitute establishing a business relationship.

Regulation 3(1), 27(1), (2)

5.3.6 An "occasional transaction" for CDD purposes means:

- a transfer of funds within the meaning of article 3.9[18] of the funds transfer regulation exceeding €1,000; or
- a transaction carried out other than in the course of a business relationship (e.g., a single foreign currency transaction, or an isolated instruction to purchase shares), amounting to €15,000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked.

5.3.7 The factors linking transactions to assess whether there is a business relationship are inherent in the characteristics of the transactions – for example, where several payments are made to the same recipient from one or more sources over a short period of time, or where a customer regularly transfers funds to one or more sources. For lower-risk situations that do not otherwise give rise to a business relationship, a three-month period for linking transactions might be appropriate, assuming this is not a regular occurrence.

Identification and verification of a beneficial owner

Regulation 6(9)

5.3.8 A beneficial owner is normally an individual who ultimately owns or controls the customer or on whose behalf a transaction is being conducted. In respect of private individuals, the customer themself is the beneficial owner, unless there are features of the transaction, or surrounding circumstances, that indicate otherwise. Therefore, there is no requirement on firms to make proactive searches for beneficial owners in such cases, but

---

[18] 'transfer of funds' means any transaction at least partially carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider, irrespective of whether the payer and the payee are the same person and irrespective of whether the payment service provider of the payer and that of the payee are one and the same, including:

(a) a credit transfer as defined in point (1) of Article 2 of Regulation (EU) No 260/2012;

(b) a direct debit as defined in point (2) of Article 2 of Regulation (EU) No 260/2012;

(c) a money remittance as defined in point (13) of Article 4 of Directive 2007/64/EC, whether national or cross border;

(d) a transfer carried out using a payment card, an electronic money instrument, or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics.

they should make appropriate enquiries where it appears that the customer is not acting on their own behalf.

Regulation 5(1), (3)

5.3.9 The ML Regulations define beneficial owners as individuals either owning or controlling more than 25% of body corporates or partnerships or otherwise owning or controlling the customer. These individuals must be identified, and reasonable measures must be taken to verify their identities. See also 5.3.170.

Regulation 6(1)

5.3.10 In relation to a trust, the ML Regulations define the beneficial owner as each of:

- the settlor;
- the trustees;
- the beneficiaries, or where the individuals benefiting from the trust have not been determined, the class of persons in whose main interest the trust is set up, or operates;
- any individual who has control over the trust.

Regulation 6(3)

5.3.11 In relation to a foundation or other legal arrangement similar to a trust, the beneficial owners are those who hold equivalent or similar positions to those set out in paragraph 5.3.10.

Regulation 6(7), (8)

5.3.12 In relation to a legal entity or legal arrangement which does not fall within 5.3.8-5.3.10, the beneficial owners are:

- any individual who benefits from the property of the entity or arrangement;
- where the individuals who benefit from the entity or arrangement have yet to be identified, the class of persons in whose main interest the entity or arrangement is set up or operates;
- any individual who exercises control over the property of the entity or arrangement.

Where an individual is the beneficial owner of a body corporate which benefits from or exercises control over the property of the entity or arrangement, the individual is to be regarded as benefiting from or exercising control over the property of the entity or arrangement.

5.3.13 Where an individual is required to be *identified* as a beneficial owner in the circumstances outlined in paragraph 5.3.8, where a customer who is a private individual is fronting for another individual who is the beneficial owner, the firm should obtain the same information about that beneficial owner as it would for a customer. For identifying beneficial owners of customers other than private individuals see paragraphs 5.3.126 onwards.

Regulation 28(2)(a), (b), (4)(b), (18)

5.3.14 The *verification* requirements under the ML Regulations are, however, different as between a customer and a beneficial owner. The identity of a customer or beneficial owner must be verified on the basis of documents or information obtained from a reliable source which is independent of the customer. For these purposes, documents issued or made available by an official body are to be regarded as being independent of a person even if they are provided or made available to the firm by or on behalf of that person. The obligation to verify the identity of a beneficial owner, however, is for the firm to take reasonable measures so that it is satisfied

that it knows who the beneficial owner is. It is up to each firm to consider whether it is appropriate, in light of the money laundering or terrorist financing risk associated with the business relationship, to make use of records of beneficial owners in the public domain, ask their customers for relevant data, require evidence of the beneficial owner's identity on the basis of documents or information obtained from a reliable source which is independent of the customer, or obtain the information in some other way.

5.3.15 In low-risk situations, therefore, it may be reasonable for the firm to confirm the beneficial owner's identity based on information supplied by the customer. This could include information provided by the customer (including trustees or other representatives whose identities have been verified) as to their identity, and confirmation that they are known to the customer. While this may be provided orally or in writing, any information received orally should be recorded in written form by the firm.

Regulation 6(1)(c)(d)

5.3.16 In some trusts and similar arrangements, instead of being an individual, the beneficial owner may be a class of persons who may benefit from the trust (see paragraphs 5.3.258ff). Where only a class of persons is required to be identified, it is sufficient for the firm to ascertain and name the scope of the class. It is not necessary to identify every individual member of the class.

Existing customers

Regulations 27(8), 29(7)

5.3.17 Firms must apply CDD measures at appropriate times to its existing customers on a risk-sensitive basis. Firms must also apply CDD measures to any anonymous accounts, passbooks or anonymous safe-deposit boxes before they are used. The obligation to report suspicions of money laundering, or terrorist financing, however, applies in respect of *all* the firm's customers, as does the UK financial sanctions regime (see paragraphs 5.3.54-5.3.61).

Regulation 27(8)(za)(zb)

Firms must apply CDD measures when they have any legal duty (e.g. ML Regulation 28(3A)) to contact an existing customer to review any information relating to the beneficial ownership of the customer.

Firms must also apply CDD measures when they have to contact an existing customer in order to fulfil any duty under the International Tax Compliance Regulations 2015 (e.g. FATCA, CRS, DAC2).

Firms should consider whether information received as a result of any of these obligations, contains changes that require CDD measures to be applied on a risk-based approach.

Regulation 27(9)

5.3.18 As risk dictates, therefore, firms must take steps to ensure that they hold appropriate information to demonstrate that they are satisfied that they know all their customers. Where the identity of an existing customer has already been verified to a previously applicable standard then, in the absence of circumstances indicating the contrary, the risk is likely to be low. A range of trigger events, such as an existing customer applying to open a new account or establish a new relationship, might prompt a firm to seek appropriate evidence.

5.3.19 Firms that do not seriously address risks (including the risk that they have not confirmed the identity of existing customers) are exposing themselves to the possibility of action for breach of the FCA Rules, or of the ML Regulations.

5.3.20 A firm may hold considerable information in respect of a customer of some years' standing. In some cases the issue may be more one of collating and assessing information already held than approaching customers for more identification data or information.

Acquisition of one financial services firm, or a portfolio of customers, by another

5.3.21 When a firm acquires the business and customers of another firm, either as a whole, or as a portfolio, it is not necessary for the identity of all existing customers to be re-verified, provided that:

- all underlying customer records are acquired with the business; **or**
- a warranty is given by the acquired firm, or by the vendor where a portfolio of customers or business has been acquired, that the identities of its customers have been verified.

It is, however, important that the acquiring firm's due diligence enquiries include some sample testing in order to confirm that the customer identification procedures previously followed by the acquired firm (or by the vendor, in relation to a portfolio) have been carried out in accordance with UK requirements.

5.3.22 In the event that:

- the sample testing of the customer identification procedures previously undertaken shows that these have not been carried out to an appropriate standard; or
- the procedures cannot be checked; or
- the customer records are not accessible by the acquiring firm,

verification of identity will need to be undertaken as soon as is practicable for all transferred customers who are not existing verified customers of the transferee, in line with the acquiring firm's risk-based approach, and the requirements for existing customers opening new accounts.

Nature and purpose of proposed business relationship

Regulation 28(2)(c) 5.3.23 A firm must understand the purpose and intended nature of the business relationship or transaction to assess whether the proposed business relationship is in line with the firm's expectation and to provide the firm with a meaningful basis for ongoing monitoring. In some instances this will be self-evident, but in many cases the firm may have to obtain information in this regard. Whether, and to what extent, the customer has contact or business relationships with other parts of the firm, its business or wider group can also be relevant, especially for higher risk customers. The customer may have different risk profiles in different parts of the business or group.

5.3.24 Depending on the firm's risk assessment of the situation, carried out in accordance with the guidance set out in Chapter 4, information that might be relevant may include some or all of the following:

- nature and details of the business/occupation/employment;
- record of changes of address;
- the expected source and origin of the funds to be used in the relationship;
- the origin of the initial and ongoing source(s) of wealth and funds (particularly within a private banking or wealth management relationship);
- copies of recent and current financial statements;
- the various relationships between signatories and with underlying beneficial owners;
- the anticipated level and nature of the activity that is to be undertaken through the relationship.

5.3.25 Having a lower money laundering and/or terrorist financing risk for identification and verification purposes does not automatically mean that the same customer is lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.

5.3.26 When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels risk, firms should take into account risk variables relating to those risk categories (see Annex 4-II). These variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting on the appropriate level of CDD measures. Examples of such variables include:

- the purpose of an account or relationship
- the level of assets to be deposited by a customer or the size of transactions undertaken
- the regularity or duration of the business relationship

Keeping information up to date

Regulation 28(11)(b)

5.3.27 Documents or information obtained for the purposes of applying CDD measures, held about customers, must be kept up to date. Once the identity of a customer has been satisfactorily verified, there is no obligation to re-verify identity (unless doubts arise as to the veracity or adequacy of the evidence previously obtained for the purposes of customer identification); as risk dictates, however, firms must take steps to ensure that they hold appropriate up-to-date information on their customers. A range of trigger events, such as an existing customer applying to open a new account or establish a new relationship, might prompt a firm to seek appropriate evidence.

5.3.28 Although keeping customer information up-to-date is required under the ML Regulations, this is also a requirement of the Data Protection Act in respect of personal data.

Characteristics and evidence of identity

5.3.29 The identity of an individual has a number of principal aspects: i.e., their given name (which of course may change), supported by date of birth. Knowledge of an individual's residential address is also central to being reasonably satisfied that the customer is who they say they are, perhaps especially for customers with more common names. Other facts about an individual accumulate over time: e.g., family circumstances and addresses, employment and business career, contacts with the authorities or with other financial sector firms, physical appearance.

5.3.30 The identity of a customer who is not a private individual is a combination of its constitution, its business, and its legal form and its ownership and control structure.

Evidence of identity

Regulation 28(2)(a)(b), (18)

5.3.31 The ML Regulations require that customer due diligence must be carried out on the basis of documents or information obtained from a reliable source which is independent of the customer. It is therefore important that the evidence used to verify identity meet this test, both at on-boarding stage and subsequently when due diligence is revised/updated.

5.3.32 Evidence of identity can be obtained in a number of forms. In respect of individuals, much weight is placed on so-called 'identity documents', such as passports and photocard driving licences, 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 confirmation, including, in appropriate circumstances, written assurances from persons or organisations that have dealt with the customer for some time.

Regulation 28(19)

5.3.33 An increasing amount of data on individuals is held electronically/digitally, in various forms, and by various organisations. Evidence of identity can also be obtained by means of a digital identification process. Like documents, sources of electronic information about individuals can, of course, vary in integrity and in reliability and independence in terms of their technology and content, therefore firms should be satisfied that any process from which such information is obtained is secure from fraud and misuse and capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact that person. Firms should therefore document steps taken in this regard.

Regulation 28(12)

5.3.34 How much identity information or evidence to ask for, the balance between asking for documents and using electronic sources or digital identification, and what to verify, in order to be reasonably satisfied as to a customer's identity, and to guard against impersonation, are matters for the judgment of the firm, which must be exercised on a risk-based approach, as set out in Chapter 4, taking into account factors such as:

- the nature of the product or service sought by the customer (and any other products or services to which they can migrate without further identity verification);

- the nature and length of any existing or previous relationship between the customer and the firm;
- the nature and extent of any assurances from other regulated firms that may be relied on; and
- whether the customer is physically present.

5.3.35 An appropriate record of the steps taken, and copies of, or references to, the evidence obtained to identify the customer must be kept.

Documentary evidence

5.3.36 Documentation purporting to offer evidence of identity may emanate from a number of sources. These documents differ in their integrity, reliability and independence. Some are issued after due diligence on an individual's identity has been undertaken; others are issued on request, without any such checks being carried out. There is a broad hierarchy of documents:

- certain documents issued by government departments and agencies, or by a court; then
- certain documents issued by other public sector bodies or local authorities; then
- certain documents issued by regulated firms in the financial services sector; then
- those issued by other firms subject to the ML Regulations, then
- those issued by other organisations.

5.3.37 In their procedures, therefore, firms will in many situations need to be prepared to accept a range of documents.

5.3.38 Firms should recognise that some documents are more easily forged or counterfeited than others. If suspicions are raised in relation to any document offered, firms should take whatever practical and proportionate steps are available to establish whether the document offered has been reported as lost or stolen.

Electronic evidence

5.3.39 Firms may choose to use electronic/digital identity checks where this is possible, either on their own or in conjunction with documentary evidence.

5.3.40 Some electronic sources evidencing identity can be created by commercial organisations from a range of other existing electronic material, without any requirement that the source meet particular verifiable performance or other standards in doing so. Others may be established against specific transparent criteria, and be subject to independent verification and assessment of their processes against these criteria, both initially and on an ongoing basis.

5.3.41 Firms should understand the basis upon which any particular source is established and whether, and if so how, its compliance with specific criteria, and performance are monitored.

5.3.42 Electronic data sources can provide a wide range of confirmatory material without directly involving the customer, although the customer's permission may be required for the firm to have access to a particular source. Some sources focus on using primary identity documents, sometimes using biometric data. Others accumulate corroborative information which in principle is separately available elsewhere. Some sources are independent of the customer, whilst others are under their 'control' in the sense that their approval is required for information to be included. Where the user is required to give their approval, consideration should be given to the possibility that the user may prevent certain information being accessed to conceal certain facts.

5.3.43 Given the increasing prevalence of social media data, firms may consider it appropriate, in some circumstances, to take such information into account as corroboration for, or supplementary to, their CDD measures. However, firms should have regard to the risks inherent in the reliability of this data, as well have regard to using such information responsibly under privacy and data protection laws.

5.3.44 In using an electronic source or digital identity to verify a customer's identity, firms should ensure that they are able to demonstrate that they have both verified that the customer (or beneficial owner) exists, and satisfied themselves that the applicant seeking the business relationship is, in fact, that customer (or beneficial owner). The use of biometric information is one way of achieving the latter confirmation, as is the use of private information or codes that incontrovertibly link the potential customer (or beneficial owner) to the electronic/digital identity information.

5.3.45 Firms should recognise that some electronic sources may be more easily tampered with, in the sense of their data being able to be amended informally and unofficially, than others. If suspicions are raised in relation to the integrity of any electronic information obtained, firms should take whatever practical and proportionate steps are available to establish whether these suspicions are substantiated, and if so, whether the relevant source should be used.

Nature of electronic checks

5.3.46 A number of commercial organisations which access many data sources are accessible online by firms, and may provide firms with a composite and comprehensive level of electronic verification through a single interface. Such organisations use databases of both positive and negative information, and many also access high-risk alerts that utilise specific data sources to identify high-risk conditions, for example, known identity frauds or inclusion on a PEPs or sanctions list, or known criminality. Some of these sources are, however, only available to closed user groups.

5.3.47 Positive information (relating to full name, current address, date of birth) can prove that an individual exists, but some can offer a higher degree of confidence than others. Some electronic sources or digital identity schemes specify criteria-driven levels of assurance or scored levels of verification that are established through the accumulation of specific pieces of identity information.

5.3.48 Such information should include data from more robust sources - where an individual has to prove their identity, or address, in some way in order to be included, as opposed to others where no such proof is required. The information maintained should be kept up to date, and the organisation's verification – or re-verification - of different aspects of it should not be older than an agreed period.

5.3.49 Negative information includes lists of individuals known to have committed fraud, including identity fraud, and registers of deceased persons. Checking against such information may be necessary to mitigate against impersonation fraud in line with the firm's risk-based approach.

5.3.50 For an electronic/digital check to provide satisfactory evidence of identity on its own, it must use data from multiple sources, and across time, or incorporate qualitative checks that assess the strength of the information supplied, or be done through an organisation which meets the criteria in paragraphs 5.3.51-5.3.52. An electronic check that accesses data from a single source (e.g., a single check against the Electoral Register, or at a single point in time), is not normally enough on its own to verify identity, although it may be sufficient where, for example, the source has been issued by a government authority and contains cryptographic security features.

Criteria for use of a provider of electronic verification of identity, digital identity or trust service

5.3.51 Some commercial organisations providing digital identities or electronic or digital identity verification are free-standing and set their own operating criteria, whilst others may be part of an association or arrangement which, in order to admit organisations to 'membership' require them to demonstrate that they meet certain published criteria – for example, in relation to data sources used, or recency of information - and carry out some form of checks on continuing compliance.

Regulation 28(19)

5.3.52 Before using an organisation for digital identities, electronic or digital identity verification, or trust services, firms should be satisfied that information supplied by the provider is considered to be sufficiently extensive, reliable, accurate, independent of the customer, and capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact that person. This judgment may be assisted by considering whether the provider meets the following criteria:

- it is recognised, through registration with the Information Commissioner's Office (or national equivalent for EEA/EU registered organisations), to store personal data;
- it is accredited or certified to offer the identity verification service through a governmental or industry process that involves meeting minimum published standards;
- it uses a range of multiple, positive information sources, including other activity history where appropriate, that can be called upon to link an applicant to both current and previous circumstances;
- it accesses negative information sources, such as databases relating to identity fraud and deceased persons;
- it accesses a wide range of alert data sources;

- its published standards, or those of the scheme under which it is accredited or certified, require its verified data or information to be kept up to date, or maintained within defined periods of re-verification;
- arrangements exist whereby the identity provider's continuing compliance with the minimum published standards is assessed; and
- it has transparent processes that enable the firm to know what checks were carried out, what the results of these checks were, and what they mean in terms of how much certainty they give as to the identity of the subject.
- it keeps sufficient records of information used to provide its services.

5.3.53 In addition, an organisation should have processes that allow the enquirer to capture and store the information they used to verify an identity, and/or return a level of assurance that can be stored by the enquirer as evidence of the organisations' verification processes.

Persons firms should not accept as customers

Persons and entities subject to financial sanctions

5.3.54 The United Nations and United Kingdom are able to designate persons and entities as being subject to financial sanctions, in accordance with relevant legislation. Such sanctions normally include a comprehensive freeze of funds and economic resources, together with a prohibition on making funds or economic resources available to the designated target. The UK Sanctions List includes all designated individuals, entities and specified ships that are subject to sanctions in the UK.

See: https://www.gov.uk/government/publications/the-uk-sanctions-list

5.3.55 The obligations under the UK financial sanctions regime apply to all firms, and not just to banks. The UK Sanctions List includes all the names of designated persons under UN and UK sanctions regimes which have effect in the UK. Firms will not normally have any obligation under UK law to have regard to lists issued by other organisations or authorities in other countries, although a firm doing business in other countries will need to be aware of the scope and focus of relevant financial sanctions regimes in those countries. Other websites may contain useful background information, but the purpose of the UK Sanctions List is to draw together in one place all the names of designated persons for the various sanctions regimes effective in the UK. All firms to whom this guidance applies, therefore, whether or not they are FCA-regulated or subject to the ML Regulations, will need either:

- for manual checking: to register with the HM Treasury update service (directly or via a third party, such as a trade association); or
- if checking is automated: to ensure that relevant software includes checks against the relevant list and that this list is up to date.

5.3.56 *Intentionally left blank.*

5.3.57 OFSI may also be contacted direct to provide guidance and to assist with any concerns regarding the implementation of financial sanctions:

Office of Financial Sanctions Implementation
HM Treasury
1 Horse Guards Road
LONDON SW1A 2HQ
Tel: +44 (0) 20 7270 5454
Email: ofsi@hmtreasury.gov.uk

5.3.58 To reduce the risk of breaching obligations under financial sanctions regimes, firms are likely to focus their resources on areas of their business that carry a greater likelihood of involvement with targets, or their agents. Within this approach, firms are likely to focus their prevention and detection procedures on direct customer relationships, and then have appropriate regard to other parties involved.

5.3.59 Firms need to have some means of monitoring payment instructions to ensure that proposed payments to targets or their agents are not made. The majority of payments made by many firms will, however, be to other regulated firms, rather than to individuals or entities that may be targets.

5.3.60 Where a firm freezes funds under financial sanctions legislation, or where it has suspicions of terrorist financing, it must make a report to OFSI, and/or to the NCA. Guidance on such reporting is given in paragraphs 6.33 to 6.42.

CTA 2008, Schedule 7

5.3.61 Under certain circumstances, HM Treasury may issue directions to a firm in relation to customer due diligence; ongoing monitoring; systematic reporting; and limiting or ceasing business. Details of any such HM Treasury directions will be found at www.hm-treasury.gov.uk.

5.3.62 Trade sanctions can be imposed by governments or other international authorities, and these can have financial implications. Where the proposed trade deal also involves a person or entity which is subject to an asset freeze, a firm will need a licence from OFSI to deal with the funds or economic resources of the designated individual, as well as the export licence from the Department for International Trade. Firms which operate internationally should be aware of such sanctions, and should consider whether these affect their operations; if so, they should decide whether they have any implications for the firm's procedures. Further information and links can be found at: https://www.gov.uk/guidance/uk-sanctions.

Illegal immigrants

s40 (1), (2)

5.3.63 Under the Immigration Act 2014, a bank or building society must not open a current account for a person who is in the UK but does not have leave to enter or remain in the UK. These immigration checks must also be carried out on existing personal current accounts on a quarterly basis and Home Office notified of a disqualified person's account or application for an account [19].

[19] See The Immigration Act 2014 (Current Accounts)(Compliance & c) Regulations 2016 s2

s 40 (3)

5.3.64 Confirmation that a person is not entitled to enter or remain in the UK can be obtained through carrying out a check with a specified[20] anti-fraud organisation or a specified data matching authority.

5.3.65 Normal CDD measures must still be applied to the customer once his immigration status has been checked. Where a current account is refused, the person must be informed it is for reasons of immigration status.

Shell banks and anonymous accounts

Regulation 34 (2), (3), (4)(b)

5.3.66 Firms must not enter into, or continue, a correspondent relationship with a shell bank. Firms must take appropriate measures to ensure that it does not enter into or continue a correspondent relationship with a bank that is known to allow its accounts to be used by a shell bank. A shell bank is an entity incorporated in a jurisdiction where it has no physical presence involving meaningful decision-making and management, and which is not part of a financial conglomerate.

Regulation 29(6), (7)

5.3.67 Firms carrying on business in the UK must not set up an anonymous account, an anonymous passbook, or an anonymous safe-deposit box for any new or existing customer. All firms carrying on business in the UK must apply CDD measures to all existing anonymous accounts, passbooks and safe-deposit boxes before such accounts, passbooks or safe-deposit boxes are used in any way.

5.3.68 Firms should pay special attention to any money laundering or terrorist financing threat that may arise from products or transactions that may favour anonymity and take measures, if needed, to prevent their use for money laundering or terrorist financing purposes.

Private individuals

General

5.3.69 Paragraphs 5.3.71 to 5.3.91 refer to the standard identification requirement for customers who are private individuals; paragraphs 5.3.92 to 5.3.125 provide further guidance on steps that may be applied as part of a risk-based approach.

5.3.70 Depending on the circumstances relating to the customer, the product and the nature and purpose of the proposed relationship, firms may also need to apply the following guidance to identifying, and verifying the identity of, beneficial owners, and to other relevant individuals associated with the relationship or transaction (but see paragraphs 5.3.8 to 5.3.16).

Obtain standard evidence

Identification

[20] See The Immigration Act 2014 (Specified Anti-fraud Organisation) Order 2014 SI 2014/1798

5.3.71 The firm should obtain the following information in relation to the private individual:

- full name
- residential address
- date of birth

Verification

Regulation 28(18)(b)

5.3.72 Verification of the information obtained must be based on reliable sources, independent of the customer – which might either be a document or documents produced by the customer, or electronically by the firm, or by a combination of both. Documents issued or made available by an official body are regarded as independent of the customer, even if they are provided or made available to the firm by the customer. Where business is conducted face-to-face, firms should see originals of any documents involved in the verification. Customers should be discouraged from sending original valuable documents by post.

A – DOCUMENTARY EVIDENCE

5.3.73 If documentary evidence of an individual's identity is to provide a high level of confidence, it will typically have been issued by a government department or agency, or by a court or local authority that has checked the existence and characteristics of the persons concerned. In cases where such documentary evidence of identity may not be available to an individual, other evidence of identity may give the firm reasonable confidence in the customer's identity, although the firm should weigh these against the risks involved.

5.3.74 Documentary evidence complementing identity should normally only be accepted if it originates from a public sector body or another regulated financial services firm, or is supplemented by knowledge that the firm has of the person or entity, which it has documented.

5.3.75 If identity is to be verified from documents, this should be based on:

Either a government-issued document which incorporates:

- the customer's full name and photograph, and
    - **either** his residential address
    - **or** his date of birth.

Government-issued documents with a photograph include:

- Valid passport
- Valid photocard driving licence (full or provisional)
- National Identity card
- Firearms certificate or shotgun licence
- Identity card issued by the Electoral Office for Northern Ireland

or a government, court or local authority-issued document (without a photograph) which incorporates the customer's full name, ***supported by*** a second document, either government-issued, or issued by a judicial authority, a public sector body or authority, a regulated utility company, or another FCA-regulated firm in the UK financial services sector, which incorporates:

- the customer's full name and
  - **either** his residential address
  - **or** his date of birth

Government-issued documents without a photograph include:

- Valid (old style) full UK driving licence
- Recent evidence of entitlement to a state or local authority-funded benefit (including housing benefit and council tax benefit), tax credit, pension, educational or other grant
- Instrument of a court appointment (such as liquidator, or grant of probate)
- Current council tax demand letter, or statement

5.3.76 Examples of other documents to support a customer's identity include current bank statements, or credit/debit card statements, issued by a regulated financial sector firm in the UK, or utility bills. If the document is from the internet, a pdf version may be more reliable (but see paragraph 5.3.45). Consideration should be given to an increased risk of forgery or counterfeiting of paper documents as customer statements can potentially be indistinguishable from originals. Where a member of the firm's staff has visited the customer at his home address, a record of this visit may constitute evidence corroborating that the individual lives at this address (i.e. equivalent to a second document).

5.3.77 In practical terms, this means that, for face-to-face verification, production of a valid passport or photocard driving licence (so long as the photograph is in date[21]) should enable most individuals to meet the identification requirement for AML/CTF purposes. The firm's risk-based procedures may dictate additional checks for the management of credit and fraud risk, or may restrict the use of certain options, e.g., restricting the acceptability of National Identity Cards in face-to-face business in the UK to cards issued only by EEA member states and Switzerland. For customers who cannot provide the standard evidence, other documents may be appropriate (see paragraphs 5.3.108 to 5.3.125).

5.3.78 Some consideration should be given as to whether the documents relied upon are forgeries or counterfeits. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity. Examples of sources of information include CIFAS, the Fraud Advisory Panel and the Serious Fraud Office. Commercial software is also

[21] It should be noted that as well as a general expiry date for UK driving licences, the photograph has a separate expiry date (10 years from first issue). Northern Ireland driving licences have a single expiry date, which is ten years from date of issue.

available that checks the algorithms used to generate passport numbers. This can be used to check the validity of passports of any country that issues machine-readable passports.

B – ELECTRONIC EVIDENCE AND DIGITAL IDENTITY

5.3.79 When using an electronic source or digital identity to verify a customer's identity, firms should ensure that they are able to demonstrate that they have both verified that the customer exists, and satisfied themselves that the individual seeking the business relationship is, in fact, that customer (or beneficial owner).

5.3.80 Electronic verification may be carried out by the firm either direct, using as its basis the customer's full name, address and date of birth, or through an organisation which has been considered per the criteria in paragraphs 5.3.51 and 5.3.52.

5.3.81 For verification purposes, a firm may approach an electronic source ot digital identity provider of its own choosing, or the potential customer may elect to offer the firm access to an electronic/digital source that they have already registered with, and which has already accumulated verified evidence of identity, and which has been considered per the criteria in paragraphs 5.3.51 and 5.3.52.

5.3.82 Some digital identity or electronic sources service providers focus on using primary identity documents, sometimes using biometric data. Other electronic sources accumulate corroborative information which in principle is separately available elsewhere. Some information is independent of the customer, whilst other is under their 'control' in the sense that their approval is required for information to be included.

5.3.83 As well as requiring an organisation used for electronic verification or digital identity to be considered per the criteria set out in paragraphs 5.3.51 and 5.3.52, it is important that the process of electronic verification meets an appropriate level of assurance before it can be judged to satisfy the firm's legal obligation.

5.3.84 Commercial organisations that provide electronic verification of identity or digital identity use various methods of displaying results - for example, by the number of documents checked, or through scoring mechanisms. Some organisations confirm that a given, predetermined 'level' of assurance or scored level of verification has been reached. Firms should ensure that they understand the basis of the system they use, in order to be satisfied that the sources of the underlying data reflect the guidance in paragraphs 5.3.46-5.3.50, and cumulatively meet an appropriate level of confirmation in relation to the risk assessed in the relationship.

C – MITIGATION OF IMPERSONATION RISK

5.3.85 Whilst some types of financial transaction have traditionally been conducted on a non-face-to-face basis, other types of transaction and relationships are increasingly undertaken in this way: e.g., internet and telephone banking, online share dealing.

5.3.86 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:

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

5.3.87 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 customer is typically not physically present - such as in many wholesale markets, or when purchasing some types of collective investments - which would not in itself increase the risk attaching to the transaction or activity. A firm should take account of such cases in developing their systems and procedures.

5.3.88 Additional measures would also include assessing the possibility that the customer is deliberately avoiding face-to-face contact. It is therefore important to be clear on the appropriate approach in these circumstances.

5.3.89 Where identity is verified electronically, copy documents are used, or the customer is not physically present (*), a firm should apply an additional verification check to manage the risk of impersonation fraud by directly linking the customer to the claimed identity. In this regard, firms should consider:

- verifying with the customer additional aspects of their identity which are held electronically; or
- utilising biometric data (including facial recognition (**) and liveness checks where appropriate); or
- requesting the applicant to confirm a secret code, or biometric factor – such codes, digital verification or other secret data may be set up within the identity, or may be supplied to a verified mobile phone, or through a verified bank account, on a one-time basis, or
- following the guidance in paragraph 5.3.90.

5.3.90 The additional verification check may consist of robust anti-fraud checks that the firm routinely undertakes as part of its existing procedures, or may include:

- requiring the first payment to be carried out through an account in the customer's name with a UK or EU regulated credit institution, or an assessed low risk jurisdiction;

(*) With appropriate controls in place non face-to-face may not pose higher risk
(**) For example, via a UK government certified digital identity service provider (IDSP)

- verifying additional aspects of the customer's identity (see paragraph 5.3.29);

- telephone contact with the customer prior to opening the account on a home or business number which has been verified (electronically or otherwise), or a "welcome call" to the customer before transactions are permitted, using it to verify additional aspects of personal identity information that have been previously provided during the setting up of the account;

- communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to them, which, in full or in part, is required to be returned completed or acknowledged without alteration);

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

- other card or account activation procedures;

- requiring copy documents to be certified by an appropriate person.

5.3.91 The source(s) of information used to verify that an individual exists may be different from those sources used to verify that the potential customer is in fact that individual.

Other considerations

5.3.92 The standard identification requirement (for documentary or electronic approaches) is likely to be sufficient for most situations. If, however, the customer, and/or the product or delivery channel, is assessed to present a higher money laundering or terrorist financing risk – whether because of the nature of the customer, or their business, or its location, or because of the product features available – the firm will need to decide whether it should require additional identity information to be provided, and/or whether to verify additional aspects of identity.

5.3.93 Where the result of the standard verification check gives rise to concern or uncertainty over identity, or other risk considerations apply, so the number of matches that will be required to be reasonably satisfied as to the individual's identity will increase.

5.3.94 For higher risk customers, the need to have additional information needs to be balanced against the possibility of instituting enhanced monitoring (see sections 5.5 and 5.7).

See Revisions Sept 2026
Insertion 5.3.94A

Executors and personal representatives

Regulation 6(6)

5.3.95 In the case of an estate of a deceased person in the course of administration, the beneficial owner is

- in England and Wales and Northern Ireland, the executor, original or by representation, or administrator for the time being of a deceased person; and
- in Scotland, the executor for the purposes of the Executors (Scotland) Act 1900[22].

In circumstances where an account is opened or taken over by executors or administrators for the purpose of winding up the estate of a deceased person, firms may accept the court documents granting probate or letters of administration as evidence of authority of those personal representatives. Lawyers, probate practitioners and accountants acting in the course of their business as regulated firms, who are note named as executors/administrators, can be verified by reference to their practising certificates, or to an appropriate professional register. 22A

5.3.96 When a customer's account is taken over by their personal representatives, firms may find the Framework for authorising people wanting to operate a bank account for someone else'[23] agreed between the Office of the Public Guardian, UKF, Building Societies Association, the Law Society in England and Wales and others a useful source of practical advice.

Court of Protection orders and court-appointed deputies

2005, c 9
SI 2007/1253

5.3.97 Under the Mental Capacity Act 2005 (and related Regulations), the Court of Protection will be able to make an order concerning a single decision in cases where a one-off decision is required regarding someone who lacks capacity. The Court can also appoint a deputy or deputies (previously referred to as receivers) where it is satisfied that a series of decisions needs to be made for a person who lacks capacity.

MLRs 28.10

5.3.97A When the Court of Protection (or equivalent in Scotland and Northern Ireland) appoints a deputy, such as a local authority/NHS trust or professional deputy (e.g. a firm of solicitors), that deputy is acting on behalf of the customer. Firms should verify the deputy's identity and their authority to act on the customer's behalf.

The deputy may nominate an authorised officer (such as a professional carer) to access or to close an account. A firm may, under its risk-based approach and as an anti-fraud check, take appropriate and proportionate measures to verify the identity of the authorised officer and to verify their authority to act. Firms should focus due diligence on the authorised officer in their professional capacity (e.g. business address should be recorded not residential address), rather than in their personal capacity, unless considered relevant.

Firms should take account of FCA guidance on achieving good outcomes for customers with characteristics of vulnerability.

5.3.98 Firms may accept the court documents appointing the deputy, or concerning a single act, as evidence of authority of the person appointed.

---

[22] 1900 c.55. Sections 6 and 7 were amended by the Succession (Scotland) Act 1964 (c.41)

22A Schedule 4 Legal Services Act provides a list of the regulators of lawyers that licence probate activities delivered by the authorised persons that they regulate

[23] http://www.mentalhealthlaw.co.uk/media/Banking_guidance_for_banks_3-4-13.pdf

Attorneys

5.3.99 When a person deals with assets under a power of attorney, that person is also a customer of the firm. Consequently, the identity of holders of powers of attorney should be verified, in addition to that of the donor. In the case of a joint and several power of attorney, the identity of the person acting separately may be verified on its own, without the need to verify the identity of all persons when they are not acting jointly.

See Revisions Sept 2026 5.3.99

When a person holds a power of attorney in a professional capacity (such as a solicitor), firms should focus due diligence on that person in their professional capacity, rather than in their personal capacity, unless considered relevant.

5.3.100 Other than where the donor or grantor of a power of attorney is an existing customer of the firm, their identity must be verified. In many cases, these customers may not possess the standard identity documents referred to in paragraphs 5.3.75ff, and firms may have to accept some of the documents referred to in paragraph 5.3.115. There may also be cases where the donor or granter is not able to perform face-to-face identification (e.g. disabled, home bound, remote location, sever loss of mental capacity); due consideration should be given to the individual's circumstances in such cases.

5.3.101 New Enduring Powers of Attorney are no longer able to be entered into, but where one has already been registered with the Office of the Public Guardian, the firm will know that the donor has lost, or is losing, capacity. A Lasting Power of Attorney cannot be used until it has been registered, but, subject to any restrictions, this may be done at any time, including while the donor is still able to manage their affairs. Therefore, the firm will not necessarily know whether the donor has lost capacity.

Source of funds as evidence

5.3.102 Under certain conditions, where the money laundering or terrorist financing risk in a product is considered to be at its lowest, a payment drawn on an account with a UK or EU regulated credit institution, or with one from an assessed low risk jurisdiction, and which is in the sole or joint name of the customer, may satisfy the standard identification requirement. Whilst the payment may be made between accounts with regulated firms or by cheque or debit card, the accepting firm must be able to confirm that the payment (by whatever method) is from a bank or building society account in the sole or joint name(s) of the customer. Part II, Sector 7: *Life assurance, and life-related pensions and investment products,* has an exception to this in respect of direct debits.

5.3.103 Whilst it is immaterial whether the transaction is effected remotely or face-to-face, each type of relationship or transaction that is entered into must be considered before determining that it is appropriate to rely on this method of verification. Firms will need to be able to demonstrate why they considered it to be reasonable to have regard to the source of funds as evidence in a particular instance. Part II, Sector 3: *Electronic Money* includes guidance on accepting the funding instrument used to load a purse as a form of initial verification in low risk situations, subject to compensating monitoring controls and turnover limits, and establishing that the customer has rightful control over the instrument.

5.3.104 One of the restrictions that will apply to a product that qualifies for using the source of funds as evidence will be an inability to make payments direct to, or to receive payments direct from, third parties. If, subsequent to using the source of funds to verify the customer's identity, the firm decides to allow such a payment or receipt to proceed, it should verify the identity of the third party. A further restriction would be that cash withdrawals should not be permitted, other than by the customers themselves, on a face-to-face basis where identity can be confirmed.

5.3.105 If a firm proposing to rely on the source of funds has reasonable grounds for believing that the identity of the customer has not been verified by the firm on which the payment has been drawn, it should not permit the source of funds to be used as evidence, and should verify the customer's identity in line with the appropriate standard requirement.

5.3.106 If a firm has reason to suspect the motives behind a particular transaction, or believes that the business is being structured to avoid the standard

identification requirement, it should not permit the use of the source of funds as evidence to identify the customer.

5.3.107 Part II, Sector 8: *Non-life providers of investment fund products* provides additional guidance to investment fund managers in respect of customers whose identity may not need to be verified until the time of redemption.

Customers who cannot provide the standard evidence

5.3.108 Some customers may not be able to produce identification information equivalent to the standard. Such cases may include, for example, some low-income customers in rented accommodation, customers with a legal, mental or physical inability to manage their affairs, individuals dependent on the care of others, dependant spouses/partners or minors, students, refugees and asylum seekers, migrant workers and prisoners. The firm will therefore need an approach that compensates for the difficulties that such customers may face in providing the standard evidence of identity.

SYSC 6.3.7 (5) G Financial Inclusion Task Force, December 2010

5.3.109 The FCA Rules adopt a broad view of financial exclusion, in terms of ensuring that, where people cannot reasonably be expected to produce standard evidence of identity, they are not unreasonably denied access to financial services. The term is sometimes used in a narrower sense, for example, the Financial Inclusion Task Force refers to those who, for specific reasons, do not have access to mainstream banking or financial services - that is, those at the lower end of income distribution who are socially/financially disadvantaged and in receipt of benefits, or those who chose not to seek access to financial products because they believed that they will be refused.

5.3.110 Firms offering financial services directed at the financially aware may wish to consider whether any apparent inability to produce standard levels of identification evidence is consistent with the targeted market for these products.

5.3.111 As a first step, before concluding that a customer cannot produce evidence of identity, firms will have established that the guidance on initial identity checks for private individuals set out in paragraphs 5.3.71 to 5.3.107 cannot reasonably be applied in view of the circumstances of the relevant customer.

5.3.112 The guidance at paragraph 5.3.75 does not require that in all cases a customer's address should be verified – the standard verification is verification of name and a choice between verifying address or date of birth. Providing the standard evidence of address can be a particular difficulty for many new arrivals to the UK, and firms should have regard to this fact in deciding whether, in particular cases, to insist on address verification, and if so, how this might be satisfied.

5.3.113 Guidance on verifying the identity of most categories of customers who cannot provide the standard evidence is given in Part II, Sector 1: *Retail banking*. Guidance on cases with more general application is given in paragraphs 5.3.115 to 5.3.125.

5.3.114 Where a firm concludes that an individual customer cannot reasonably meet the standard identification requirement, and that the provisions in Part II, Sector 1: *Retail banking*, Annex 1-I, cannot be met, it may accept as

identification evidence a letter or statement from an appropriate person who knows the individual, that indicates that the person is who he says he is.

Persons without standard documents, in care homes, or in receipt of pension

5.3.115 An entitlement letter from the DWP, or a letter from the DWP confirming that the person is in receipt of a pension, could provide evidence of identity. If this is not available, or is inappropriate, a letter from an appropriate person, for example, the matron of a care home, may provide the necessary evidence.

Those without the capacity to manage their financial affairs

5.3.116 Guidance on dealing with customers who lack, or are losing, capacity to manage their affairs, covering Powers of Attorney; Court of Protection Orders; and Appointeeship, are set out in a BBA leaflet, "Guidance for people wanting to manage a bank account for someone else" available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/515055/Guidance-for-people-wanting-to-manage-a-bank-account-for-someone-else.pdf (see also paragraphs 5.3.97 – 5.3.101). Although this leaflet is directed at banks, its contents have more general application.

Gender reassignment

5.3.117 A firm should satisfy itself (for example, on the basis of documentary medical evidence) that the gender transfer of a customer is genuine (as with a change of name). Such cases usually involve transferring a credit history to a reassigned gender. This involves data protection, not money laundering issues. The consent of the person involved is necessary.

Students and young people

5.3.118 When opening accounts for students or other young people, the standard identification requirement should be followed as far as possible (see paragraphs 5.3.71 – 5.3.107). In practice, it is likely that many students, and other young people, will have a passport, and possibly a driving licence. Where the standard requirement would not be relevant, however, or where the customer cannot satisfactorily meet this, other evidence could be obtained by obtaining appropriate confirmation(s) from the applicant's workplace, school, college, university or care institution (see https://www.gov.uk/government/collections/sponsorship-information-for-employers-and-educators and Part II, Sector 1: *Retail banking*, Annex 1-I). Any confirmatory letter should be on appropriately headed notepaper; in assessing the strength of such confirmation, firms should have regard to the period of existence of the educational or other institution involved, and whether it is subject to some form of regulatory oversight. UCAS also maintain a database of students who have confirmed places at a University/Higher Education establishment, which is accessible on subscription (see www.ucasmedia.com/).

5.3.119 All international students undergo rigorous checks by the immigration services at home and abroad in order to be satisfied as to their identity and

bona fides before they are given leave to enter or remain in the UK as a student or prospective student. Applicants must meet the requirements of the Student Immigration Rules and must provide documentation which demonstrates that they intend to study, and have been accepted, on a course of study at a bona fide institution. This includes the provision of a course admission letter from the education institution. If they cannot provide the documents they will not be given leave to enter or remain in the UK.

5.3.120 Often, a business relationship in respect of a minor will be established by a family member or guardian. In cases where the adult opening the account or establishing the relationship does not already have an existing relationship with the firm, the identity of that adult should be verified and, in addition, the firm should see one of the following documents (or similar documents issued in other jurisdictions) in the name of the child:

- birth certificate
- passport
- NHS Medical Card
- Child benefit documentation
- Child Tax Credit documentation
- National Insurance Card (for those aged 16 and over)

Financially excluded

5.3.121 Further guidance on verifying the identity of financially excluded persons is given in Part II, Sector 1: *Retail banking,* paragraphs 1.38 – 1.41. A proportionate and risk-based approach will be needed to determine whether the evidence available gives reasonable confidence as to the identity of a customer.

5.3.122 Where a firm has concluded that it should treat a customer as financially excluded for the purposes of customer identification, and the customer is identified by means other than standard evidence, the reasons for doing so should be documented.

5.3.123 The "financially excluded" are not a homogeneous category of uniform risk, and firms should consider the risk presented in any particular case. Some financially excluded persons may represent a higher risk of money laundering regardless of whether they provide standard or non-standard tokens to confirm their identity, e.g. a passport holder who qualifies only for a basic account on credit grounds. Firms may wish to consider whether enhanced due diligence (see section 5.5) or monitoring (see section 5.7) of the size and expected volume of transactions would be useful in respect of some financially excluded categories, based on the firm's own experience of their operation.

5.3.124 In other cases, where the available evidence of identity is limited, and the firm judges that the individual cannot reasonably be expected to provide more, but that the business relationship should nevertheless go ahead, it should consider instituting enhanced monitoring arrangements over the customer's transactions and activity (see section 5.7). In addition, the firm should consider whether restrictions should be placed on the customer's ability to migrate to other, higher risk products or services.

5.3.125 Where an applicant produces non-standard or incomplete documentation, staff should not cite the ML Regulations (or other regulation relating to the prevention of money laundering and/or terrorist financing) as an excuse for not opening an account without giving proper consideration to the evidence available, referring up the line for advice as necessary. It may be that at the conclusion of that process a considered judgment may properly be made that the evidence available does not provide a sufficient level of confidence that the applicant is who they claim to be, in which event a decision not to open the account would be fully justified. Firms should bear in mind that the ML Regulations are not explicit as to what is and is not acceptable evidence of identity.

Customers other than private individuals

5.3.126 Depending on the nature of the entity, a relationship or transaction with a customer who is not a private individual may be entered into in the customer's own name, or in that of specific individuals or other entities on its behalf. Beneficial ownership may, however, 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.

Regulation 28(3A)

Where the customer is a legal person, company, trust, foundation, or similar legal arrangement, reasonable measures must be taken to understand the ownership and control structure of the entity.

Regulation 28(4)

5.3.127 In deciding who the beneficial owner is in relation to a customer who is not a private individual, the firm's objective must be to know who has ownership or 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. Verifying the identity of the beneficial owner(s) will be carried out on a risk-based approach, following the guidance in paragraphs 5.3.8 to 5.3.16, and will take account of the number of individuals, the nature and distribution of their interests in the entity and the nature and extent of any business, contractual or family relationship between them.

5.3.128 Firms also have obligations under the UK financial sanctions regime (see Part III: *Compliance with the UK financial sanctions regime)* which require the collection of information in relation to trustees, directors or equivalent. In determining the information to be collected, therefore, firms should take account of their information needs in relation to sanctions compliance.

5.3.129 Certain other information about the entity should be obtained as a standard requirement. Thereafter, on the basis of the money laundering/terrorist financing risk assessed in the customer/product/delivery channel combination, a firm should decide the extent to which the identity of the entity should be verified. The firm should also decide what additional information in respect of the entity and, potentially, some of the individuals behind it, should be obtained (see section 5.5).

Regulation 30A(1), (1A), (2), (2A)

5.3.129A Firms must obtain an excerpt of the register of the company, unregistered company, the limited liability partnership, an eligible Scottish partnership, an in-scope trust, or registrable overseas entity before establishing a business relationship. The excerpt may be obtained from the customer, Companies House, or a third-party provider. In the case of in-scope trusts, an excerpt from the Trust Registration Service (TRS) must be obtained via the agent or trustee of the trust, and an excerpt of the Register of Overseas Entities (ROE) must be obtained for registrable overseas entity customers. See also 5.3.129C.

Firms must also obtain an excerpt as listed above whilst carrying out CDD and ongoing monitoring of a business relationship once established. Firms should apply a risk-based approach to obtaining up-to-date excerpts. For example, when it becomes aware that the beneficial ownership information it holds is outdated or has changed, or that an overseas entity has become registrable (*).

Regulation 30(2B), 3, Schedule 3AZA

5.3.129B If the firm finds a material discrepancy between information relating to the beneficial ownership of the company which it collects as above, and information which becomes available to it whilst conducting CDD (including during onboarding and ongoing monitoring), the material discrepancy must be reported to Companies House, or to HMRC if it relates to a trust.

Beneficial ownership in this context (excluding trusts and overseas entities), means a person of significant control (PSC) per the information held in the PSC register and not as defined in the ML Regulations. Information on the PSC register may thus differ from other beneficial ownership information and not necessarily be inaccurate. Discrepancies that result solely from differences between the definition of PSCA and 'beneficial owner' in the ML Regulations are not material and therefore not reportable. Beneficial ownership in the case of trusts means trustees, settlors, beneficiaries, protectors, or other individuals that exercise control over the trust (see 5.3.261). Beneficial ownership in the case of overseas entities means registrable beneficial owners, not PSCs.

Identifying a discrepancy does not in itself trigger the reporting obligation, as discrepancies must be material to be reportable (**). For example, a material discrepancy would arise when there is a missing or different person (legal or natural) recorded, as compared between information in the PSC register, ROE or TRS and the beneficial ownership information obtained when conducting CDD.

A discrepancy itself does not necessarily prohibit the onboarding of the customer, nor require the firm to exit the relationship. The nature and relevance of the discrepancy should however be assessed by firms with their CDD process and risk-based approach, in considering whether there are reasonable grounds for suspicion of money laundering/terrorist financing.

A discrepancy report is not a substitute for a suspicious activity report (SAR) and the requirement to submit a SAR where appropriate remains.

(*) This could occur when the nature and purpose of the business relationship changes - the firm may start providing products/services to facilitate the purchase, sale or transfer of UK land or property.
(**) See MLRs Schedule 3AZA.

Material discrepancies should be considered with an overarching requirement of proportionality and reasonableness, taking into account the ML/TF risk that the firm has determined is posed by the customer, and the reasonable justification provided for the discrepancy.

Firms should consider whether the material discrepancy is indicative of being linked to ML/TF or concealing details of the business of the customer, which could be a potential indicator for suspicion of ML/TF. When doing so, firms need not consider whether any such concealment is deliberate or not. Discrepancies arising from administrative or clerical errors, or due to chronological factors affecting timely updates of the registers are unlikely to constitute concealment and therefore are unlikely to be reportable.

The material discrepancy report should be made as soon as reasonable possible when discovered (*).

For further guidance (including circumstances where Companies House considers firms do not need to make a report) see: https://www.gov.uk/guidance/report-a-discrepancy-about-a-beneficial-owner-on-the-psc-register-by-an-obliged-entity.

For further guidance on discrepancy reporting for in-scope trusts (including what HMRC considers a material discrepancy) see: https://www.gov.uk/hmrc-internal-manuals/trust-registration-service-manual/trsm70030.

5.3.129C Excerpts should only be those of the legal entity or trust that is the firm's customer, and not other undertakings, legal entities or trusts within the customer's ownership and control structure, unless the firm has a direct business relationship with them.

Excerpts of registers need only be obtained if the firm's customer is registered or registrable. This may be determined through the ordinary course of business and the application of existing CDD measures (**).

The ROE only needs to be checked and excerpts of the ROE obtained when the nature and purpose of the business relationship involves or changes to mean the firm is providing products/services to facilitate the purchase, sale or transfer of UK land or property, subject to a risk-based approach and consideration of proportionality.

There are exemptions to registration (in respect of the TRS and ROE) and firms can apply a risk-based approach in this determination. Depending on the firm's assessment of risk, this could include obtaining attestation from the customer in lower risk scenarios, or obtaining independent professional advice in circumstances assessed as posing a higher ML/TF risk (***).

If a firm determines that a customer is registrable but has not registered, it is a material discrepancy and must be reported.

If a firm is reasonably satisfied that an unregistered trust is not required to register, it does not need to make a report but should document its decision.

(*) For trusts, firms may wish to resolve discrepancies with the customer and only make a report if unresolved within a reasonable time period.
(**) Overseas entities must be registered with ROE to purchase, sell or transfer UK land or property. UK and non-UK trusts liable for UK tax must register with TRS.
(***) See also HMRC guidance: https://www.gov.uk/hmrc-internal-manuals/trust-registration-service-manual/trsm23000.

Regulation 27(9)(c) and 33(1)(g)

5.3.130 Where an entity is known to be linked to a PEP (as a result of the PEP being a beneficial owner of the entity), or to a jurisdiction assessed as carrying a higher money laundering/terrorist financing risk, it is likely that this will put the entity into a higher risk category, and that enhanced due diligence measures should therefore be applied (see sections 5.5 and 5.7).

5.3.131 Many entities, both in the UK and elsewhere, operate internet websites, which contain information about the entity. Firms should bear in mind that this information, although helpful in providing much of the material that a firm might need in relation to the company, its directors and business, is not independently verified before being made publicly available in this way.

Space intentionally left blank

5.3.132 This section provides guidance on verifying the identity of a range of non-personal entities, as follows:

- Regulated financial services firms subject to the ML Regulations (or equivalent) (paragraphs 5.3.133 to 5.3.138)
- Other firms subject to the ML Regulations (or equivalent) (paragraphs 5.3.139 to 5.3.142)
- Corporate customers (other than regulated firms) (paragraphs 5.3.143 to 5.3.176)
- Partnerships and unincorporated businesses (paragraphs 5.3.177 to 5.3.191)
- Public sector bodies, governments, state-owned companies and supranationals (paragraphs 5.3.192 to 5.3.203)
- Sovereign Wealth Funds (paragraphs 5.3.204-5.3.227)
- Pension schemes (paragraphs 5.3.228 to 5.3.237)
- Charities, church bodies and places of worship (paragraphs 5.3.238 to 5.3.257)
- Other trusts and foundations (paragraphs 5.3.258 to 5.3.282)
- Clubs and societies (paragraphs 5.3.283 to 5.3.293)

Regulated financial services firms subject to the ML Regulations (or equivalent)

Regulation 37(3)(a)

5.3.133 In determining whether a business relationship presents a low degree of risk of ML/TF, and therefore the extent to which it is appropriate to apply SDD measures, a firm must take into account, inter alia, whether the customer is a credit institution or a financial institution which is subject to the requirements in the ML Regulations.

Regulation 37(3)

5.3.134 In their determination of the low degree of risk, firms must also take into account whether the country where the customer is resident, established or registered, or in which it operates, is the UK or an assessed low risk jurisdiction.

Regulation 37(1)

5.3.135 If the firm determines that the situation in relation to another regulated financial services firm presents a low degree of ML/TF risk, simplified due diligence may be applied (see section 5.4).

5.3.136 When applying SDD measures firms must continue to comply with the requirements of Regulation 28 of the ML Regulations although the extent, timing or type of measures undertaken may be adjusted to reflect its determination per 5.3.135.

5.3.137 Firms should:

- record the steps they have taken to check the status of the other regulated firm.
- take appropriate steps to be reasonably satisfied that the person they are dealing with is properly authorised by the customer.
- document the rationale for the decision to apply SDD.

5.3.138 Firms must continue to monitor business relationships and transactions to detect unusual or suspicious transactions.

Group Companies

5.3.138A Where a firm establishes a business relationship or carries out an occasional transaction with another regulated firm in the same group as itself, the level of CDD to be applied should be determined on a risk-based approach. Where the group company is subject to the ML Regulations or equivalent, the firm may apply simplified due diligence measures (see Chapter 5.4).

5.3.138B Where the group company is subject to group wide policies and procedures (that are equivalent to UK MLRs) and is based in a non-equivalent or FATF call for action country, the extent of the CDD/EDD measures to be applied could include consideration of factors such as the nature of activities undertaken with that group company and the risks posed by those activities (see Part II for details of sector specific risks and due diligence requirements).

Other firms that are subject to the ML Regulations (or equivalent)

5.3.139 Customers which are subject to the ML Regulations or equivalent, but which are not regulated in the UK or an assessed low risk jurisdiction as a financial services business, should be treated, for AML/CTF purposes, according to their legal form: for example, as private companies, in accordance with the guidance set out in paragraphs 5.3.163 to 5.3.176; or if partnerships, by confirming their regulated status through reference to the current membership directory of the relevant professional association (for example, law society or accountancy body). However, when professional individuals are acting in their personal capacity, for example, as trustees, their identity should normally be verified as for any other private individual.

5.3.140 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer.

5.3.141 Some consideration should be given as to whether documents relied upon are forgeries or counterfeits. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

Regulation 37(5)(6)

5.3.142 Firms that are subject to the ML Regulations, and, which hold client money in pooled accounts (whether in a bank account or through a securities holding), are in principle obliged to verify the identities of their clients. Financial services firms with which such client accounts are held are, however, permitted to apply SDD measures to the holders of such funds, provided that:

See Revisions 2026 5.3.142

- the business relationship with the holder of the pooled account presents a low risk of ML/TF;
- the information on the identity of the persons on whose behalf monies are held in the pooled account is available, on request, to the firm;
- if the holder of the pooled account is in a third country, the holder is subject to the requirements in national legislation implementing the fourth money laundering directive, and is supervised for compliance with these requirements.

As a practical matter, firms may reasonably apply a similar approach to such client accounts which only contain the funds of a single beneficial owner. Firms should also be satisfied that the customer applies robust and risk-sensitive CDD measures to their own clients and their clients' beneficial owners. It may be appropriate for firms to take risk-sensitive measures to assess the adequacy of its customer's CDD policies and procedures, for example by liaising directly with the customer or by sample-testing the customer's ability to provide CDD information upon request.
See also Annex 5-V.

5.3.142A Part II Sector 22 (paras 22.72-22.74) provides further information on the relationship between a cryptoasset provider or custodian wallet provider when they become a client of another firm that is subject to the ML Regulations.

Corporate customers (other than regulated firms)

5.3.143 Corporate customers may be publicly accountable in several ways. Some public companies are listed on stock exchanges or other regulated markets, and are subject to market regulation and to a high level of public disclosure in relation to their ownership and business activities. Other public companies are unlisted, but are still subject to a high level of disclosure through public filing obligations. Private companies are not generally subject to the same level of disclosure, although they may often have public filing obligations. In their verification processes, firms should take account of the availability of public information in respect of different types of company.

Regulation 43

5.3.144 Most UK body corporates have obligations to maintain up-to-date information on people with significant influence and control over them and file this information at Companies House. This is known as the central register of people with significant control (PSC register), and is accessible online without charge. When a UK body corporate enters into or has an existing business relationship with a firm, where the firm is required to apply CDD measures, the corporate must on request provide the firm with:

- information identifying
  - its name, registered number, registered office and principal place of business;
  - its board of directors or members of the equivalent management body if no board
  - its senior management
  - the law to which it is subject
  - its legal and beneficial owners;
- its articles of association or other governing documents.

UK body corporates must inform the firm with which they have a business relationship of any change to the above information within 14 days of becoming aware of the change.

These requirements do not apply to corporates as defined per 5.3.156.

Guidance on the requirements to maintain PSC registers is available at https://www.gov.uk/government/publications/guidance-to-the-people-with-significant-control-requirements-for-companies-and-limited-liability-partnerships.

5.3.145 The structure, ownership, purpose and activities of the great majority of corporates will be clear and understandable. Corporate customers can use complex ownership structures, which can increase the steps that need to be taken to be reasonably satisfied as to their identities; this does not necessarily indicate money laundering or terrorist financing. The use of complex structures without an obvious legitimate commercial purpose may, however, give rise to concern and increase the risk of money laundering or terrorist financing.

Regulation 28(4)(c)

5.3.146 Control over companies may be exercised through a direct shareholding or through intermediate holding companies. Control may also rest with those who have power to manage funds or transactions without requiring specific authority to do so, and who would be in a position to override internal procedures and control mechanisms. Firms should make an evaluation of the effective distribution of control in each case. What constitutes control for this purpose will depend on the nature of the company, the distribution of shareholdings, and the nature and extent of any business or family connections between the beneficial owners. (More specific guidance on beneficial ownership is given in Part II, Sector 13: *Private equity*, paragraphs 13.49-13.54, which may be of more general interest.)

Regulation 28(2)(b), (4)(c)

5.3.147 To the extent consistent with the risk assessment carried out in accordance with the guidance in Chapter 4, the firm must take reasonable measures to understand the company's legal form and ownership and control structure, and must obtain sufficient additional information on the nature of the company's business, and the reasons for seeking the product or service.

Regulation 5(1)

5.3.148 In the case of a body corporate, other than a company listed on a regulated market, the beneficial owner includes any individual who:

- ultimately owns or controls (whether through direct or indirect ownership or control, including through bearer share holdings or by other means) more than 25% of the shares or voting rights in the body corporate; or
- exercises control over the management of the body corporate; or
- otherwise exercises significant influence or control over the body corporate.

For example, if no individual owns or controls more than 25% of the shares or voting rights in the body, firms should use judgment in determining whether an individual owning or controlling a lower percentage exercises effective control. Guidance on the meaning of other forms of significant influence and control is available for companies:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/621687/psc-statutory-guidance-companies.pdf ; Limited Liability Partnerships: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/523122/Draft_statutory_guidance_LLPs.pdf ; and Eligible Scottish Partnerships: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/621569/170622_Eligible_Scot_P_GUI_June_2017.pdf

5.3.149 Directors of a body corporate do not fall under the definition of beneficial owner in their capacity of director. However, a director may as an individual or legal person also hold an ownership interest in the body, or fall into one of the other categories of exercising significant influence or control over the body.

5.3.150 Paragraphs 5.3.151 – 5.3.154 refer to the standard evidence for corporate customers, and paragraphs 5.3.155 – 5.3.162 provide further supplementary guidance on steps that may be applied as part of a risk-based approach.

Obtain standard evidence

Regulation 28(3)(a)

5.3.151 The firm must obtain and verify the following information in relation to the corporate concerned:

- full name
- registered number
- registered office in country of incorporation
- principal business address (if different from the registered office)

and, additionally, for private or unlisted companies:

- names of individuals who own or control over 25% of its shares or voting rights
- names of any individual(s) who otherwise exercise control over the management of the company

Regulation 30A

Firms must obtain proof of registration or an excerpt of the register of the corporate before establishing a business relationship.

Regulation 28(3)

5.3.152 The firm must take reasonable steps to determine and verify:

(a) the law to which the corporate is subject;
(b) its constitution (whether set out in its articles of association or other governing documents);
(c) names of its directors and the senior persons responsible for its operations.

The firm should verify the information set out in paragraph 5.3.151, and in (a)-(c) above, from appropriate sources, such as:

- confirmation of the company's listing on a regulated market
- a search of the relevant company registry
- a copy of the company's Certificate of Incorporation

5.3.153 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer.

5.3.154 Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

Companies listed on regulated markets

5.3.155 Corporate customers whose securities are admitted to trading on a UK regulated market or an EU regulated market within the EEA, or a regulated financial market outside the EEA whose securities are admitted to equivalent trading disclosure obligations are generally accountable.

Regulation 28(5)

5.3.156 Where the firm has satisfied itself that the customer is:

- a company which is listed on a regulated market (within the meaning of MiFID) in the UK, EU regulated market within the EEA, or on a non-EEA market that is subject to specified disclosure obligations; or
- a majority-owned and consolidated subsidiary of such a listed company

the obligation to identify, and to verify the identity of, beneficial owners, and the obligation to take reasonable steps to determine and verify the information at 5.3.152 (a)-(c) does not apply (see section 5.4).

Regulation 3(1)

5.3.157 Specified disclosure obligations are disclosure requirements consistent with specified articles of:

- Prospectus requirements [Reg 1129/2017]
- Disclosure Guidance and Transparency Rules [FCA Handbook]
- The Market Abuse Regulation [Reg 596/2014]

Regulations 3(1) and 37(3)(a)(iv)

5.3.158 If a regulated market is located within the UK, is an EU regulated market within the EEA, or on a non-EEA market that is subject to specified disclosure obligations, there is no requirement to undertake checks on the market itself. Firms should, however, record the steps they have taken to ascertain the status of the market. If the market is outside the EEA, but is one which subjects companies whose securities are admitted to trading to disclosure obligations which are contained in international standards and are equivalent to the specified disclosure obligations, similar treatment is permitted. For companies listed outside the EEA on markets which do not meet the requirements set out in paragraph 5.3.157, the standard verification requirement for private and unlisted companies should be applied.

5.3.159 ESMA maintains a list of regulated markets within the EU at https://registers.esma.europa.eu/publication/searchRegister?core=esma_registers_upreg.

Other publicly listed or quoted companies

5.3.160 Companies that are listed on a regulated market that is not equivalent and thus where in principle an obligation to verify beneficial owners remains, are still subject to some degree of accountability and transparency. As part of their risk-based approach, therefore, firms may have regard to the listing conditions that apply in the relevant jurisdiction and the level of transparency and accountability to which the company is subject in determining customer risk, including whether SDD may be applied (see Part III Section 3).

5.3.161 Firms should note that AIM is not a regulated market under MiFID. However, due diligence requirements at admission and ongoing disclosure requirements on AIM are broadly similar to those of regulated markets. A firm may, therefore, under its risk-based approach, regard the due diligence

process for admission to AIM as giving equivalent comfort as to the identity of the company under consideration.

5.3.162 In applying the risk-based approach, firms may take into account the potentially lower risk presented by companies whose shares are traded as this makes them less likely to be established for money laundering purposes. However, the firm should, for markets that allow listed companies to have dominant shareholders (especially where they are also directors), ensure that such cases are examined more closely.

Private and unlisted companies

5.3.163 Unlike publicly quoted companies, the activities of private or unlisted companies are often carried out for the profit/benefit of a small and defined group of individuals or entities. Such firms are also subject to a lower level of public disclosure than public companies. In general, however, the structure, ownership, purposes and activities of many private companies will be clear and understandable. Information from the central PSC register will also be available.

Regulation 33(1)(g)

5.3.164 Where private companies are well known, reputable organisations, with long histories in their industries and substantial public information about them, the standard evidence may well be sufficient to meet the firm's obligations. Where a higher risk of money laundering is associated with the business relationship, however, EDD (and enhanced monitoring) must be applied.

5.3.165 In the UK, a company registry search (or enquiry of the Charities Commission in the case of a Charitable Incorporated Organisation) will confirm that the applicant company has not been, or is not in the process of being, dissolved, struck off or wound up. In the case of non-UK companies, firms should make similar search enquiries of the registry in the country of incorporation of the applicant for business.

5.3.166 Standards of control over the issue of documentation from company registries vary between different countries. Attention should be paid to the jurisdiction the documents originate from and the background against which they are produced.

5.3.167 Whenever faced with less transparency, less of an industry profile, or less independent means of verification of the client entity, firms should consider the money laundering or terrorist financing risk presented by the entity, and therefore the extent to which, in addition to the standard evidence, they should verify the identities of other shareholders and/or controllers. It is important to know and understand any associations the entity may have with other jurisdictions (headquarters, operating facilities, branches, subsidiaries, etc) and the individuals who may influence its operations (political connections, etc). A visit to the place of business may be helpful to confirm the existence and activities of the entity.

5.3.168 Firms may find the sectoral guidance in Part II helpful in understanding some of the business relationships that may exist between the customer and other entities in particular business areas.

Directors

5.3.169 Following the firm's assessment of the money laundering or terrorist financing risk presented by the company, it may decide to verify the identity of one or more directors, as appropriate, in accordance with the guidance for private individuals (paragraphs 5.3.71 to 5.3.125). In that event, verification is likely to be appropriate for those who have authority to operate an account or to give the firm instructions concerning the use or transfer of funds or assets, but might be waived for other directors. Firms may, of course, already be required to identify a particular director as a beneficial owner if the director owns or controls more than 25% of the company's shares or voting rights (see paragraph 5.3.148).

Beneficial owners

Regulation 5
Regulation 28(4), (9)
Regulation 28(3A); 28(8)(b)

5.3.170 As part of the standard evidence, the firm will know the names of all individual beneficial owners owning or controlling more than 25% of the company's shares or voting rights, (even where these interests are held indirectly) or who otherwise exercise control over the management of the company. This forms part of their understanding of the ownership and control structure of the entity. If there is an obligation to identify, but no beneficial owner has been identified, or the firm is not satisfied that the individual identified is the beneficial owner, the firm must take reasonable measures to verify the identity of the senior person in the body corporate responsible for managing it (see also paragraphs 5.3.8 to 5.3.16), and record all actions in doing so, as well as difficulties encountered, where applicable. Firms do not satisfy their obligations to verify the identity of beneficial owners by relying only on information contained in a PSC register.

Where there is no reasonable expectation of certain corporate customers, such as supranational organisations, wholly state-owned entities, certain multilateral financial institutions, government agencies and sovereign wealth funds, having a beneficial owner, firms do not need to verify the identity of the senior person but must nevertheless document the steps taken and record the rationale for their conclusions.

Signatories

5.3.171 For operational purposes, the firm is likely to have a list of those authorised to give instructions for the movement of funds or assets, along with an appropriate instrument authorising one or more directors (or equivalent) to give the firm such instructions. The identities of individual signatories need only be verified on a risk-based approach.

Other considerations

5.3.172 Unless their customer's securities are admitted to trading in a regulated market (see 5.3.156), firms are required to verify the identity of beneficial owners of corporate customers that are subject to statutory licensing and regulation of their industry (for example, energy, telecommunications).

Under its risk-based approach, however, a firm may feel that, provided that it is confirmed by a reliable source, independent of the customer, imposition of regulatory obligations on such a firm gives an equivalent level of confidence in the company's public accountability. Therefore, evidence that the corporate customer is subject to the licensing and prudential regulatory regime of a statutory regulator within the UK (e.g., OFGEM, OFWAT, OFCOM or an EEA equivalent), should satisfy the firm's obligation to verify the identity of such a customer.

Regulation 33(1)(g)

5.3.173 The standard evidence is likely to be sufficient for most corporate customers. If, however, the customer, or the product or delivery channel, is assessed to present a higher money laundering or terrorist financing risk – whether because of the nature of the customer, its business or its location, or because of the product features available – the firm must, on a risk-sensitive basis, apply EDD measures. For example, the firm will need to decide whether it should require additional identity information to be provided and/or verified (see sections 5.6 and 5.7).

5.3.174 Higher risk corporate customers may also be, among others, smaller and more opaque entities, with little or no industry profile and those in less transparent jurisdictions, taking account of issues such as their size, industry profile, industry risk.

Bearer shares

5.3.175 Extra care must be taken in the case of companies with capital in the form of bearer shares, because in such cases it is often difficult to identify the beneficial owner(s). Companies that issue bearer shares are frequently incorporated in high-risk jurisdictions. Firms should adopt procedures to establish the identities of the holders and material beneficial owners of such shares and to ensure that they are notified whenever there is a change of holder and/or beneficial owner.

5.3.176 As a minimum, these procedures should require a firm to obtain an undertaking in writing from the beneficial owner which states that immediate notification will be given to the firm if the shares are transferred to another party. Depending on its risk assessment of the client, the firm may consider it appropriate to have this undertaking certified by an accountant, lawyer or equivalent, or even to require that the shares be held by a named custodian, with an undertaking from that custodian that the firm will be notified of any changes to records relating to these shares and the custodian.

Partnerships and unincorporated bodies

5.3.177 Partnerships and unincorporated businesses, although principally operated by individuals, or groups of individuals, are different from private individuals in that there is an underlying business. This business is likely to have a different money laundering or terrorist financing risk profile from that of an individual.

Regulation 5(3)

5.3.178 The beneficial owner of a partnership (other than a limited liability partnership) is any individual who ultimately is entitled to or controls

(whether the entitlement or control is direct or indirect) more than a 25% share of the capital or profits of the partnership, or more than 25% of the voting rights in the partnership, or who otherwise exercise ultimate control over the management of the partnership.

For example, if no individual owns or controls more than 25% of the capital or profits of the partnership, or of the voting rights in the partnership, firms should use judgement in determining whether an individual owning or controlling a lower percentage exercises effective control.

Obtain standard evidence

5.3.179 The firm should obtain the following standard evidence in relation to the partnership or unincorporated association:

- full name
- business address
- names of all partners/principals who exercise control over the management of the partnership
- names of individuals who own or control over 25% of its capital or profit, or of its voting rights

5.3.180 Given the wide range of partnerships and unincorporated businesses, in terms of size, reputation and numbers of partners/principals, firms need to make an assessment of where a particular partnership or business lies on the associated risk spectrum.

5.3.181 The firm's obligation is to verify the identity of the customer using evidence from a reliable source, independent of the customer. Where partnerships or unincorporated businesses are well known, reputable organisations, with long histories in their industries, and with substantial public information about them and their principals and controllers, confirmation of the customer's membership of a relevant professional or trade association is likely to be able to provide such reliable and independent evidence. This does not obviate the need to verify the identity of the partnership's beneficial owners.

5.3.182 As part of the standard evidence, the firm will know the names of all individual beneficial owners owning or controlling more than 25% of the partnership's capital or profit, or its voting rights or who otherwise exercise control over the management of the partnership. The firm must take reasonable measures to verify the identity of those individuals (see paragraphs 5.3.8 to 5.3.16).

5.3.183 Intentionally left blank.

5.3.184 For identification purposes, Scottish partnerships and limited liability partnerships should be treated as corporate customers. For limited partnerships, the identity of general partners should be verified whilst other partners should be treated as beneficial owners.

5.3.185 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer.

5.3.186 Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

Other considerations

5.3.187 Most partnerships and unincorporated businesses are smaller, less transparent, and less well known entities, and are not subject to the same accountability requirements as, for example, companies listed on a regulated market.

5.3.188 Where the money laundering or terrorist financing risk is considered to be at its lowest, the firm may be able to use the source of funds as evidence of the customer's identity. The guidance in paragraphs 5.3.102 to 5.3.106 should be followed. This does not obviate the need to verify the identity of beneficial owners, where these exist.

5.3.189 Whenever faced with less transparency, less of an industry profile, or less independent means of verification of the client entity, firms should consider the money laundering or terrorist financing risk presented by the entity, and therefore the extent to which, in addition to the standard evidence, additional precautions should be taken.

5.3.190 It is important to know and understand any associations the entity may have with other jurisdictions (headquarters, operating facilities, branches, subsidiaries, etc) and the individuals who may influence its operations (political connections, etc). A visit to the place of business may be helpful to confirm the existence and activities of the business.

Principals and owners

5.3.191 Following its assessment of the money laundering or terrorist financing risk presented by the entity, the firm may decide to verify the identity of one or more of the partners/owners as customers. In that event, verification requirements are likely to be appropriate for partners/owners who have authority to operate an account or to give the firm instructions concerning the use or transfer of funds or assets; other partners/owners must be verified as beneficial owners, following the guidance in paragraphs 5.3.8 to 5.3.16.

Public sector bodies, governments, state-owned companies and supranationals (other than sovereign wealth funds)

Regulation 37(3)

5.3.192 In respect of customers which are UK or overseas governments (based in jurisdictions that the firm has determined as low risk), (or their representatives), supranational organisations, government departments,

state-owned companies or local authorities, the approach to identification and verification may be tailored to the circumstances of the customer, reflecting the firm's determination of the level of ML/TF risk presented. Where the firm determines that the business relationship presents a low degree of risk of ML/TF, SDD measures may be applied. Public sector bodies include state supported schools, colleges, universities and NHS trusts.

5.3.193 Bodies engaged in public administration are different from state-owned bodies which conduct business. The nature of the business relationship established with firms in the financial sector will therefore differ. Public administration involves a different revenue/payment stream from that of most businesses, and may be funded from government sources, or from some other form of public revenues. State-owned businesses, on the other hand, may engage in a wide range of activities, some of which might involve higher risk factors, leading to a different level of CDD being appropriate. Such entities may be partly publicly funded or may derive some or all of their revenues from trading activities.

Obtain standard evidence

5.3.194 Firms should obtain the following information about customers who are public sector bodies, governments, state-owned companies and supranationals:

- Full name of the entity
- Nature and status of the entity (e.g., overseas government, treaty organisation)
- Address of the entity
- Name of the home state authority
- Names of directors (or equivalent)

5.3.195 Firms should take appropriate steps to understand the ownership of the customer, and the nature of its relationship with its home state authority.

5.3.196 Firms should, where appropriate, verify the identities of the directors (or equivalent) who have authority to give the firm instructions concerning the use or transfer of funds or assets.

5.3.197 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer.

Signatories

5.3.198 For operational purposes, the firm is likely to have a list of those authorised to give instructions for the movement of funds or assets, along with an appropriate instrument authorising one or more directors (or equivalent) to give the firm such instructions. The identities of individual signatories need only be verified on a risk-based approach.

Schools, colleges and universities

5.3.199 State supported schools, colleges and universities should be treated as public sector bodies, in accordance with the guidance set out in paragraphs

5.3.192 to 5.3.198. The UK Border Agency maintains a register of sponsors www.bia.homeoffice.gov.uk/employers/points/ which may assist firms in verifying the existence of such customers. The register of sponsors lists all organisations that the UK Border Agency has approved to employ migrants or sponsor migrant students.

5.3.200 For independent schools and colleges, firms should refer to the guidance given at paragraph 5.3.253.

Other considerations

5.3.201 The firm's assessment of the money laundering or terrorist financing risk presented by such customers should aim to identify higher risk countries or jurisdictions.

5.3.202 The guidance in paragraphs 5.3.192 to 5.3.200 should be applied to overseas entities, as appropriate to the firm's assessment of the risk that such entities present.

5.3.203 Many governmental, supranational and state-owned organisations will be managed and controlled by individuals who may qualify as PEPs (see paragraphs 5.5.13 to 5.5.23). Firms need to be aware of the increased likelihood of the existence of such individuals in the case of such customers, and deal with them appropriately, having regard to the extent of any risk that the funds of such entities may be used for improper purposes.

Sovereign wealth funds

5.3.204 Sovereign Wealth Funds (SWFs) are defined[24] as special purpose investment funds or arrangements, owned by the general (i.e., national) government. Created by the general government for macroeconomic purposes, SWFs hold, manage, or administer assets to achieve financial objectives, and employ a set of investment strategies which include investing in foreign financial assets.

5.3.205 Typically, SWFs are established from balance of payments surpluses, proceeds raised from privatisations or revenues from natural resources exports. They are managed to meet specific investment objectives, perhaps for a specific future need. Increasingly in recent years, SWFs have looked to employ third party institutions to assist in the management their assets.

5.3.206 Notwithstanding the different forms that SWFs can take, a large proportion of them are participants in the International Forum of Sovereign Wealth Funds (IFSWF).

5.3.207 The IFSWG was established in April 2009 (succeeding the previous International Working Group) to develop a common set of voluntary principles ("the Santiago Principles") in order to promote a clearer understanding of SWFs through better transparency of their governance and operation. A list of the IFSWF's member funds, and the counties in which

[24] International Forum of Sovereign Wealth Funds *www.ifswf.org*

they are established, can be found at Appendix II to the Santiago Principles at: http://www.ifswf.org/santiago-principles. Further countries, plus the OECD and the World Bank, participate as permanent observers. The International Monetary Fund provides both a co-chair of the IFSWF and its secretariat.

5.3.208 A general concern exists that SWFs are capable of being used to meet political, rather than purely financial objectives, by acquiring controlling interests in strategically important industries or destabilising economies. For this reason, understanding the nature of purpose of the SWF and the relationship or transaction is a key AML/CTF control and important to the reputation of the firm. Firms should be alert to activities that might give rise to an asset freezing order where UK interests are at stake.

5.3.209 The firm should consider the international reputation of the country and/or SWF concerned (see the Transparency International website www.transparency.org for some helpful resources), before entering into a relationship with the fund. Moreover, financial sanctions may be in force against a country that operates an SWF and must be observed irrespective of whether or not the country is a member of the IWG.

5.3.210 SWFs are unlikely to qualify for simplified due diligence.

Nature and legal form

5.3.211 SWFs are constituted in a variety of ways. Usually, however, they take one of the following forms:

- pool of assets managed by the Ministry of Finance or Central Bank;
- government-owned corporation;
- independent corporation established by statute

This means that CDD must be tailored according to the nature of the SWF. A fundamental feature, however, is that the beneficial owner of a SWF is the government concerned.

Obtain standard evidence

5.3.212 The standard evidence outlined below is founded on an SWF's participation in the IFSWF and the close involvement with that body of the OECD, IMF and World Bank. Without the comfort of IFSWF membership, the firm should undertake normal identity verification measures according to the legal form of the SWF.

5.3.213 The following information should be obtained about the identity of the SWF and its officers:

- Full name of the SWF
- Address of the SWF
- Name of the national government
- Names of directors/ trustees (or equivalent)

5.3.214 The objectives in terms of identification are to establish that the SWF exists, that it is owned and controlled by a government and that the individuals

with whom the firm has contact in connection with establishing the relationship are bona fide representatives of the fund.

5.3.215 For the purposes of establishing that an SWF exists, reference should normally be made to Appendix II to the Santiago Principles (see paragraph 5.3.207), to confirm that it is represented on the IFSWF as a full or observer member. Additional steps will be required if the fund is not an IFSWF member.

5.3.216 Firms should, where appropriate, verify the identities of the directors (or equivalent) who have authority to give the firm instructions concerning the use or transfer of funds or assets and take steps to be reasonably satisfied that the person(s) the firm is dealing with is properly authorised by the SWF.

5.3.217 To supplement the measures described in paragraph 5.3.216 and assist with the verification of the individuals that represent the fund, a copy of the constitutional documentation should be obtained, including evidence of its establishment or appointment as an SWF and the authority of those individuals to bind the fund or appoint others to do so. Information in the public domain from reputable and independent sources (e.g., news items, international conference programmes etc.) may also be used as additional evidence of an individual's connection with the fund.

5.3.218 For operational purposes, the firm is likely to have a list of those authorised to give instructions for the movement of funds or assets, along with an appropriate instrument authorising one or more directors (or equivalent) to give the firm such instructions. The identities of individual signatories need only be verified on a risk-based approach. Particular care should be exercised if there is a change of government to ensure that the firm is clear as to the individuals authorised to act for the SWF.

Beneficial ownership

5.3.219 SWFs are created to manage the wealth or financial resources at national level so there will be no natural person that has any beneficial interest. The constitutional documents should make this clear.

Nature and purpose

5.3.220 Given the concern that surrounds SWFs (see paragraph 5.3.216), and the fact that those who control them, and perhaps the firm's mandate, are likely in many cases to be PEPs, the firm needs to consider the nature and purpose of various aspects, including:

- the purpose of the SWF
- the purpose of the relationship with the firm
- whether any PEPs are beneficial owners of the SWF, and any heightened ML/TF risk that arises; and
- on an ongoing basis, the reasons for withdrawals from the portfolio

Regulation 33(1)(g) 5.3.221 Each firm's processes should take into account any PEP beneficial ownership of an SWF, and, on a risk-assessed basis, require a person from

senior management and independent from the officer sponsoring the relationship to approve the establishment of the relationship. For higher risk relationships, the firm's compliance (or MLRO) function should also satisfy itself that the risks are acceptable.

5.3.222 The purpose of the SWF should be evident from its constitutional documentation and elsewhere. Note that one of Santiago Principles (GAPP 2) is that the purpose of the fund should be clearly defined and publicly disclosed.

5.3.223 The reasons for using the firm's services need to be understood. For example, investment management mandates are likely to be similar to other institutional mandates and should be questioned if they are unusually focused towards particular sectors, having regard (if appropriate) to the fact that the firm may be managing a specific tranche of the overall fund.

5.3.224 Given the specific nature of SWFs, attention should be given to withdrawals to ensure that the reasons are consistent with the legitimate objectives of the fund and that any payment instructions are appropriate in that context. If the firm has suspicions concerning the motives of the fund, it should make a Suspicious Activity Report to the NCA.

5.3.225 Monitoring should be conducted to identify changes to the objectives of the fund and its status in relation to the IFSWF.

Other considerations

5.3.226 When formulating a risk-based approach to SWFs, and particularly when considering those based in countries with higher levels of corruption, firms should take into account the fact that some IFSWF member funds may not have fully implemented the Santiago Principles and that observers will not necessarily implement them at all and should factor such variations into their additional enquiries.

5.3.227 If a country is not a member of the IFSWF or does not subscribe to the Santiago Principles, it may be more difficult to obtain information about its constitution and objectives. In these circumstances, the firm must determine what further information, if any, it requires, bearing in mind the need to apply a risk-based approach. For example, the firm should understand there may be increased risk that the origins of the fund are corrupt or the funds' purpose constitutes a potential threat in connection with terrorism or economic manipulation.

Pension schemes

5.3.228 UK pension schemes can take a number of legal forms. Some may be companies limited by guarantee; some may take the form of trusts; others may be unincorporated associations. Many register with HMRC in order to achieve tax-exempt status. Most have to register with the Pensions Regulator. Generally, evidence of registration with HMRC and/or the Pensions Regulator (as relevant on a case-by-case basis) will be sufficient to meet identification and verification obligations in respect of most UK pension schemes. HMRC do not issue approval letters. However, if the

firm has any concerns, on application and with the relevant authority, HMRC can be asked to provide documentary confirmation regarding the existence of the scheme. Due to confidentiality restrictions, the Pensions Regulator is unlikely to confirm that a particular pension scheme is registered with them unless the firm is able to provide the scheme's authority for them to provide this information.

Regulation 37(3)(b)(iii)

5.3.229 In determining whether a business relationship presents a low degree of risk of ML/TF, and therefore the extent to which it is appropriate to apply SDD measures, a firm must take into account, inter alia, whether the customer/product is a pension, superannuation or similar scheme which provides retirement benefits for employees, where contributions are made by an employer or by way of deduction from an employee's wages and the scheme rules do not permit the assignment of a member's interest under the scheme. If the firm determines that the situation presents a low degree of ML/TF risk, simplified due diligence may be applied (see section 5.4).

5.3.230 For such a scheme, therefore, the firm need only satisfy itself that the customer qualifies for simplified due diligence in this way.

Regulation 6(4)(b)(ii)

5.3.231 For a scheme that takes the form of a trust, an individual does not qualify as a beneficial owner through having control solely as a result of discretion delegated to him under s 34 of the Pensions Act 1995.

Obtain standard evidence

5.3.232 Where a pension scheme does not meet the criteria in paragraph 5.3.229, and therefore the firm is not able to determine that simplified due diligence measures may be applied, but has HMRC or Pensions Regulator registration, a firm's identification and verification obligations may be met by confirming the scheme's registration, as described in paragraph 5.3.228.

5.3.233 Where a firm is unable to confirm the scheme's HMRC or Pension Regulator registration, a pension scheme should be treated for AML/CTF purposes according to its legal form and standard evidence obtained. In such circumstances and when a pension scheme is structured as a trust, Regulations 44 and 45(2)(b) of the ML Regulations make it clear that where not all members of the class of beneficiaries have been determined, trustees of such pension schemes need only maintain accurate and up-to-date written records of the class of beneficiaries of the pension scheme (rather than of individual beneficiaries).

Signatories

5.3.234 For operational purposes, the firm is likely to have a list of those authorised to give instructions for the movement of funds or assets, along with an appropriate instrument authorising one or more directors (or equivalent) to give the firm such instructions. The identities of individual signatories need only be verified on a risk-based approach.

Other considerations

5.3.235 Following a risk-based approach, the identity of the principal employer may need to be verified in accordance with the guidance given for companies in paragraphs 5.3.143 to 5.3.176 and the source of funding

recorded to ensure that a complete audit trail exists if the employer is wound up.

Payment of benefits

5.3.236 Any payment of benefits by, or on behalf of, the trustees of an occupational pension scheme will not require verification of identity of the recipient. (The transaction will either not be relevant financial business or will be within the scope of the exemption for policies of insurance in respect of occupational pension schemes.)

5.3.237 Where individual members of an occupational pension scheme are to be given personal investment advice, their identities must be verified. However, where the identity of the trustees and principal employer have been satisfactorily verified (and the information is still current), it may be appropriate for the employer to provide confirmation of identities of individual employees.

Charities, church bodies and places of worship

5.3.238 Charities have their status because of their purposes, and can take a number of legal forms. Some may be companies limited by guarantee, a Charitable Incorporated Organisation under the Charities Commission, or incorporated by Royal Charter or by Act of Parliament; some may take the form of trusts; others may be unincorporated associations.

5.3.239 If the charity is an incorporated entity (or otherwise has legal personality), firms should verify its identity following the guidance in paragraphs 5.3.143ff. The charity itself is the firm's customer, for practical purposes represented by the trustees who give instruction to the firm.

Regulation 6(1)

5.3.240 If the charity takes the form of a trust, it has no legal personality and its trustees have control and management over its affairs. In relation to a trust, the ML Regulations define the settlor (where one exists) and trustees as beneficial owners. Where there are a large number of trustees the firm may take a risk-based approach to determining on how many, and which, in respect of whom the firm should carry out full CDD measures. (see paragraphs 5.3.258ff.)

5.3.241 If the charity takes the form of an unincorporated association, it also has no legal personality. Its officers, or members of its governing body, are then the firm's customers, on whom the firm must carry out full CDD measures. (see paragraphs 5.3.283ff.)

5.3.242 In exceptional cases, another individual may exercise control, such as a receiver appointed to manage the affairs of the charity.

5.3.243 For the vast majority of charities, either there will be no individual who is a beneficial owner (apart from the trustees) within the meaning of the ML Regulations, or at most a class of persons who stand to benefit from the charity's objects must be identified. These persons will be self-evident

from a review of the charity's objects in its constitution or the extract from the Register of Charities.

5.3.244 Examples of charities where classes of persons can be identified include charities that relieve poverty, famine or homelessness, educate individuals or alleviate sickness, disability or age. In these cases, a broad description of the class of persons who stand to benefit is sufficient so that the firm understands who the persons are who benefit. Examples of classes might be:

- 'Homeless persons in London'
- 'Deaf and blind people'
- 'Children in the village of Ambridge'

In other charities, no individuals benefit directly from the charity's objects. Examples include charities for the benefit of animals, wildlife or flora, or the conservation or preservation of buildings, habitats or environment.

5.3.245 Neither the Charity Commissioners, nor judges of courts (who may exercise powers over charities) fall within the definition of controllers for these purposes.

Obtain standard evidence

5.3.246 The firm should obtain the following in relation to the charity or church body:

- Full name and address
- Nature of body's activities and objects
- Name(s) of Settlor(s) [if any]
- Names of all trustees (or equivalent)
- Names or classes of beneficiaries

5.3.247 The existence of the charity can be verified from a number of different sources, depending on whether the charity is registered or not, a place of worship or an independent school or college.

Registered charities – England and Wales, and Scotland

5.3.248 The Charity Commission is required to hold a central register of charities in England and Wales and allocates a registered number to each. The Office of the Scottish Charity Regulator carries out a similar function for Scottish charities. When dealing with an application which includes the name of a registered charity, the Charity Commission, or the Office of the Scottish Charity Regulator, can confirm the registered number of the charity and the name and address of the regulator's correspondent for the charity concerned.

5.3.249 Details of all registered charities can be accessed on the Charity Commission website (www.charity-commission.gov.uk), the Office of the Scottish Charity Regulator website (www.oscr.org.uk), or a check can be made by telephone to the respective regulator's enquiry line. Firms should

be aware that simply being registered is not in itself a guarantee of the bona fides of an organisation, although it does indicate that it is subject to some ongoing regulation.

Charities in Northern Ireland

5.3.250 Applications from, or on behalf of, charities in Northern Ireland should be dealt with in accordance with procedures for private companies set out in paragraphs 5.3.163 to 5.3.169, if they are limited by guarantee, and for clubs and societies, those in paragraphs 5.3.283 to 5.3.293. Verification of the charitable status can normally be obtained through HMRC.

Church bodies and places of worship

Charities (exception from Registration) Regulations 1996

Registered Places of Worship Act 1855

5.3.251 Certain church bodies are excepted by law from registering as charities and may not therefore have a registered number. For tax purposes, however, they may notify HMRC of their charitable status; verification of their status may be met by having sight of HMRC's confirmation of the church's application for charitable status. The identity of individual churches may be verified through the headquarters or regional organisation of the denomination, or religion.

Unregistered charities or church bodies

5.3.252 Other than those covered by paragraph 5.3.251, the identities of unregistered charities or church bodies, whether in the UK or elsewhere, cannot be verified by reference to registers maintained by independent bodies. Applications from, or on behalf of, unregistered charities should therefore be dealt with in accordance with the procedures for private companies set out in paragraphs 5.3.163 to 5.3.169, for trusts, as set out in paragraphs 5.3.258 to 5.3.282, or for clubs and societies, as set out in paragraphs 5.3.283 to 5.3.293. Firms should take particular note of those paragraphs addressing customers where the money laundering or terrorist financing risk is greater in relation to particular customers, and if it should be followed in these circumstances.

Independent schools and colleges

5.3.253 Where an independent school or college is a registered charity, it should be treated in accordance with the guidance for charities. Any such body which is not registered as a charity should be treated in accordance with the guidance for private companies in paragraphs 5.3.163 to 5.3.169.

5.3.254 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer.

Other considerations

5.3.255 In assessing the risks presented by different charities, a firm might need to make appropriate distinction between those with a limited geographical remit, and those with unlimited geographical scope, such as medical and emergency relief charities.

5.3.256 If they have a defined area of benefit, charities are only able to expend their funds within that defined area. If this area is an overseas country

or jurisdiction, the charity can quite properly be transferring funds to that country or jurisdiction. It would otherwise be less clear why the organisation should be transferring funds to a third country (which may, within the general context of the firm's risk assessment have a lower profile) and this would therefore be unusual. Such activity would lead to the charity being regarded as higher risk.

5.3.257 Non-profit organisations have been known to be abused, to divert funds to terrorist financing and other criminal activities. FATF published a best practices paper on 'Combating the abuse of non-profit organisations' in June 2015 (available at www.fatf-gafi.org), in support of Recommendation 8.

Other trusts and foundations

5.3.258 There is 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 trusts set up under testamentary arrangements, to small, local trusts funded by small, individual donations from local communities, serving local needs. It is important, in putting proportionate AML/CTF processes into place, and in carrying out their risk assessments, that firms take account of the different money laundering or terrorist financing risks that trusts of different sizes, areas of activity and nature of business being conducted, present.

5.3.259 For trusts or foundations that have no legal personality, those trustees (or equivalent) who enter into the business relationship with the firm, in their capacity as trustees of the particular trust or foundation, are the firm's customers on whom the firm must carry out full CDD measures. Following a risk-based approach, in the case of a large, well known and accountable organisation firms may limit the trustees considered customers to those who give instructions to the firm. Other trustees will be verified as beneficial owners, following the guidance in paragraphs 5.3.8 to 5.3.16.

5.3.260 Most trusts are not separate legal persons, and for AML/CTF purposes should be identified as described in paragraphs 5.3.267 to 5.3.271.

Regulation 6(1), 42(2)(b)

5.3.261 The ML Regulations specify that a beneficial owner of a relevant trust means each of the following

- the settlor;
- the trustees;
- the beneficiaries, or where the individuals benefiting from the trust have not been determined, the class of persons in whose main interest the trust is set up, or operates;
- any individual with control over the trust.

Regulation 6(3)

5.3.262 In relation to a foundation or other legal arrangement similar to a trust, the beneficial owners are those who hold equivalent or similar positions to those set out in paragraph 5.3.261.

Regulation 6(2)

5.3.263 In exceptional cases where persons other than trustees, the settlor and beneficiaries exercise control over the trust property, they are to be considered as beneficial owners. Examples of such persons may include trust protectors.

Regulation 42(2)(b)

5.3.264 For the vast majority of relevant trusts, either there will be clearly identified beneficiaries (who are beneficial owners within the meaning of the ML Regulations), or a class of beneficiaries. These persons will be self-evident from a review of the trust's constitution, or proof of registration document from the Trust Registration Service.

5.3.265 In some trusts, no individuals may benefit directly; examples include trusts for the benefit of animals, wildlife or flora, or the conservation or preservation of buildings, habitats or environment.

Regulation 6(6), (7)

5.3.266 In relation to a legal entity or legal arrangement which is not a trust the beneficial owners (see paragraph 5.3.262) are:

- any individual who benefits from the property of the entity or arrangement;
- where the individuals who benefit from the entity or arrangement have yet to be identified, the class of persons in whose main interest the entity or arrangement is set up or operates;
- any individual who exercises control over the property of the entity or arrangement.

Where an individual is the beneficial owner of a body corporate which benefits from or exercises control over the property of the entity or arrangement, the individual is to be regarded as benefiting from or exercising control over the property of the entity or arrangement.

Obtain standard evidence

5.3.267 In respect of trusts, the firm should obtain the following information:

- Name of the settlor
- Full name of the trust
- Nature, purpose and objects of the trust (e.g., discretionary, testamentary, bare)
- Country of establishment
- Names of all trustees
- Names of any beneficiaries (or, when relevant and as set out in paragraph 5.3.261, a description of the class of beneficiaries)
- Name of any protector or controller

Regulation 30A

Firms must obtain proof of registration or an excerpt of the register of the trust before establishing a business relationship (see 5.3.129A).

Regulation 28(2), (4)(c)

5.3.268 The identity of the trust must be verified on the basis of documents or information obtained from a reliable source which is independent of the customer. This may require sight of relevant extracts from the trust deed, or reference (subject to paragraph 5.3.270) to an appropriate register in the country of establishment. The firm must take reasonable measures to understand the ownership and control structure of the customer.

Beneficial owners

Regulation 6(1)(a)(b)

5.3.269 The ML Regulations specify that the settlor, trustees, beneficiaries and individuals that have control over a trust are beneficial owners. In exceptional cases where persons other than trustees, the settlor and beneficiaries exercise control over the trust property, they are to be considered as beneficial owners. Examples of such persons may include trust protectors.

Regulation 28(9)

5.3.270 The identities of other beneficial owners (e.g., certain beneficiaries), either individuals or a class, as appropriate, must also be verified (see paragraphs 5.3.8 to 5.3.16). Firms do not satisfy their obligations to verify the identity of beneficial owners by relying only on information contained in a register.

Regulation 6(1)

5.3.271 Where there is a large number of trustees the firm may take a risk-based approach to determining on how many, and which, in respect of whom the firm should carry out full CDD measures (see paragraphs 5.3.258ff).

5.3.272 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer. Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

5.3.273 Where a trustee is itself a regulated entity (or a nominee company owned and controlled by a regulated entity), or a company listed on a regulated market, or other type of entity, the identification and verification procedures that should be carried out should reflect the standard approach for such an entity.

Other considerations

5.3.274 Firms should make appropriate distinction between those trusts that serve a limited purpose (such as inheritance tax planning) or have a limited range of activities and those where the activities and connections are more sophisticated, or are geographically based and/or with financial links to other countries.

5.3.275 For situations presenting a lower money laundering or terrorist financing risk, the standard evidence will be sufficient. However, less transparent and more complex structures, with numerous layers, may pose a higher money laundering or terrorist financing risk. Some trusts established in jurisdictions with favourable tax regimes have in the past been associated with tax evasion and money laundering. In respect of trusts in this category, the firm's risk assessment may lead it to require additional information on the purpose, funding and beneficiaries of the trust.

Regulation 33(1)(g)

5.3.276 Where a situation is assessed as carrying a higher risk of money laundering or terrorist financing, the firm must carry out a higher level of verification. Information that might be appropriate to ascertain for higher risk situations includes:

- Donor/settlor/grantor of funds (except where there are large numbers of small donors
- Domicile of business/activity
- Nature of business/activity
- Location of business/activity (operating address)

Non-UK trusts and foundations

5.3.277 The guidance in paragraphs 5.3.258 to 5.3.276 applies equally to UK based trusts and non-UK based trusts. On a risk-based approach, a firm will need to consider whether the geographical location of the trust (or any other risk factor) gives rise to additional concerns, and if so, what they should do.

5.3.278 A foundation ("Stiftung") is described in the FATF October 2006 *Report on the Misuse of Corporate Vehicles* as follows:

"A foundation (based on the Roman law *universitas rerum)* is the civil law equivalent to a common law trust in that it may be used for similar purposes. A foundation traditionally requires property dedicated to a particular purpose. Typically the income derived from the principal assets (as opposed to the assets themselves) is used to fulfil the statutory purpose. A foundation is a legal entity and as such may engage in and conduct business. A foundation is controlled by a board of directors and has no owners. In most jurisdictions a foundation's purpose must be public. However there are jurisdictions in which foundations may be created for private purposes. Normally, foundations are highly regulated and transparent."

5.3.279 Foundations feature in a number of EEA member states and other civil law jurisdictions including, notably, Liechtenstein and Panama. The term is also used in the UK and USA in a looser sense, usually to refer to a charitable organisation of some sort. In the UK and USA, entities referred to as foundations will frequently be legal entities rather than legal arrangements.

5.3.280 The nature of a civil law foundation should normally be well understood by firms, or their subsidiaries or branches, operating in the jurisdiction under whose laws the foundation has been set up. Where a foundation seeks banking or other financial services outside its home jurisdiction, firms will need to be satisfied that there are legitimate reasons for doing so and to establish the statutory requirements within the specific home jurisdiction for setting up a foundation. So far as possible, comparable information should be obtained as indicated in paragraph 5.3.267 for trusts, including the identity of the founder and beneficiaries (who may include the founder), whose identity should be verified as necessary on similar risk-based principles.

5.3.281 Where the founder's identity is withheld, firms will need to exercise caution and have regard to the standing of any intermediary and the extent of assurances that may be obtained from them to disclose information on any parties concerned with the foundation in response to judicial demand in the firm's own jurisdiction. Liechtenstein foundations, for example, are generally established on a fiduciary basis through a licensed trust company to preserve the anonymity of the founder, but the trust companies are themselves subject to AML laws.

5.3.282 Whilst firms may conclude on the basis of their due diligence that the request for facilities is acceptable, they should bear in mind that terms like 'foundation', 'stiftung', 'anstalt' are liable to be hijacked by prime bank instrument fraudsters to add spurious credibility to bogus investment schemes.

Clubs and societies

5.3.283 There is a wide variety of clubs and societies, ranging from large, nationally and internationally active organisations subject to a high degree of public interest and quasi-accountability, to small, local clubs and societies funded by small, individual donations or subscriptions from local communities, serving local needs. It is important, in putting proportionate AML/CTF processes into place, and in carrying out their risk assessments, that firms take account of the different money laundering or terrorist financing risks that clubs and societies of different sizes, areas of activity and nature of business being conducted, present.

5.3.284 Where an application is made on behalf of a club or society, firms should therefore make appropriate distinction between those that serve a limited social or regional purpose and those where the activities and connections are more sophisticated, or are geographically based and/or with financial links to other countries.

5.3.285 Many local clubs and societies are small, with limited resources, and it is important to apply identity verification requirements that are appropriate in the context of the financial crime risk presented by the club or society. This might be particularly relevant in deciding which of the trustees or office holders should be made subject to identity verification.

5.3.286 For the vast majority of clubs and societies, either there will be no individual who is a beneficial owner within the meaning of the ML Regulations, or at most a class of persons who stand to benefit from the club or society's objects must be identified. These persons will be self-evident from a review of the club or society's objects in its constitution.

Obtain standard evidence

5.3.287 For many clubs and societies, the money laundering or terrorist financing risk will be low. The following information should be obtained about the customer:

- Full name of the club/society
- Legal status of the club/society
- Purpose of the club/society
- Names of all officers

5.3.288 The firm should verify the identities of the officers who have authority to operate an account or to give the firm instructions concerning the use or transfer of funds or assets.

5.3.289 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer.

5.3.290 Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

Other considerations

5.3.291 Where the money laundering or terrorist financing risk is considered to be at its lowest, the firm may be able to use the source of funds as evidence of the customer's identity. The guidance in paragraphs 5.3.102 to 5.3.106 should be followed. This does not obviate the need to verify the identity of beneficial owners, where these exist.

5.3.292 The firm's risk assessment may lead it to conclude that the money laundering or terrorist financing risk is higher, and that it should require additional information on the purpose, funding and beneficiaries of the club or society.

5.3.293 Following its assessment of the money laundering or terrorist financing risk presented by the club/society, the firm may decide to verify the identities of additional officers, and/or institute additional transaction monitoring arrangements (see Chapter 5.7).

5.4 Simplified due diligence

Regulation 37(1)

5.4.1 A firm may apply SDD measures in relation to a particular business relationship or transaction if it determines that, taking into account its risk assessment, the business relationship or transaction presents a low degree of risk of ML/TF.

Regulation 37 (3)37(3)(5)

5.4.2 When assessing whether there is a low degree of risk of ML/TF in a particular situation, and the extent to which it is appropriate to apply SDD measures in that situation, a firm must take account of at least the following risk factors:

(i) Whether the customer is –
- a public administration, or a publicly owned enterprise 5.3.192/193
- an individual resident in a geographical area of low risk
- a credit or financial institution subject to the requirements having an equivalent effect to those in the fourth money laundering directive (see paragraph 5.3.133)
- a company listed on a regulated market (see paragraph 5.3.155)
- firms holding a pooled account (see paragraph 5.3.142)

(ii) certain life assurance and e-money products (see Part II, sectors 7 and 3)
(iii) certain pension funds (see paragraphs 5.4.4 and 5.3.228ff)
(iv) Child Trust Funds and Junior ISAs (see paragraphs 5.4.5 - 5.4.7)

5.4.3 Annex 5-III to this chapter sets out suggested Risk Factor Guidelines on Simplified Due Diligence.

Regulation 37(3)(b)(iii)

5.4.4 Subject to an assessment of the ML/TF risk presented, SDD measures may be applied to pension, superannuation or similar schemes which provide retirement benefits to employees, where contributions are made by an employer or by way of deduction from an employee's wages and the scheme rules do not permit the assignment of a member's interest under the scheme.

Regulation 37(3)(b)(vi)(vii)

5.4.5 SDD measures may be applied to Child Trust Funds and Junior ISAs.

5.4.6 In respect of Junior ISAs, although SDD measures may be applied, firms will, however, in due course need to verify identity at the point the child reaches 18 years and becomes entitled to the funds, or at the next 'trigger' event thereafter (unless the child's identity has by then already been verified for the purposes of some other relationship).

5.4.7 With Junior ISAs, the child is able to manage the account from the age of 16, in which case the firm might choose to undertake customer due diligence at that stage in order to avoid delaying any transaction the child should wish to undertake on reaching 18, when the account becomes a 'full' ISA. It is recommended that firms indicate in their product literature etc. what their policy will be when, for example, the child reaches 16 or 18.

5.4.8 SDD measures must not be applied, or continue to be applied, where: the firm's risk assessment changes and it no longer considers that there is a low degree of risk of ML/TF; where the firm suspects money laundering or terrorist financing; or where there are doubts about the veracity or accuracy of documents or information previously obtained for the purposes of identity or verification.

Regulation 28(11)
POCA s330 (2)(b)
Terrorism Act s 21A

5.4.9 A determination that SDD measures may be applied in a particular situation does not remove the obligation to conduct ongoing monitoring of the business relationship, although the extent of this may be adjusted to reflect its determination of the low degree of ML/TF risk. Such determination does not affect the duty to report knowledge or suspicion of money laundering or terrorist financing.

5.4.10 Firms should also document the rationale for the decision to apply SDD.

5.5 Enhanced due diligence

Regulation 33(1)(g)

5.5.1 A firm must apply EDD measures on a risk-sensitive basis in any situation which by its nature can present a higher risk of money laundering or terrorist financing. As part of this, a firm may conclude, under its risk-based approach, that the information it has collected as part of the customer due diligence process (see section 5.3) is insufficient in relation to the money laundering or terrorist financing risk, and that it must obtain additional information about a particular customer, the customer's beneficial owner, where applicable, and the purpose and intended nature of the business relationship.

5.5.2 As a part of a risk-based approach, therefore, firms should hold sufficient information about the circumstances and business of their customers and, where applicable, their customers' beneficial owners, for two principal reasons:

- to inform its risk assessment process, and thus manage its money laundering/terrorist financing risks effectively; and
- to provide a basis for monitoring customer activity and transactions, thus increasing the likelihood that they will detect the use of their products and services for money laundering and terrorist financing.

5.5.3 The extent of additional information sought, and of any monitoring carried out in respect of any particular business relationship, or class/category of business relationship, will depend on the money laundering or terrorist financing risk that the customer, or class/category of business relationship, is assessed to present to the firm.
See 5.5.9 and 5.5.11 for EDD scenarios where additional information must be obtained.

5.5.4 In practice, under a risk-based approach, it will not be appropriate for every product or service provider to know their customers equally well, regardless of the purpose, use, value, etc., of the product or service provided. Firms' information demands need to be proportionate, appropriate and discriminating, and to be able to be justified to customers.

5.5.5 A firm should hold a fuller set of information in respect of those business relationships it assessed as carrying a higher money laundering or terrorist financing risk, or where the customer is seeking a product or service that carries a higher risk of being used for money laundering or terrorist financing purposes.

5.5.6 When someone becomes a new customer, or applies for a new product or service, or where there are indications that the risk associated with an existing business relationship might have increased, the firm should, depending on the nature of the product or service for which they are applying, request information as to the customer's residential status, employment and salary details, and other sources of income or wealth (e.g., inheritance, divorce settlement, property sale), in order to decide

whether to accept the application or continue with the relationship. The firm should consider whether, in some circumstances, evidence of source of wealth or income should be required (for example, if from an inheritance, see a copy of the will). The firm should also consider whether or not there is a need to enhance its activity monitoring in respect of the relationship. A firm should have a clear policy regarding the escalation of decisions to senior management concerning the acceptance or continuation of high-risk business relationships.

5.5.7 The availability and use of other financial information held is important for reducing the additional costs of collecting customer due diligence information and can help increase a firm's understanding of the risk associated with the business relationship. Where appropriate and practical, therefore, and where there are no data protection restrictions, firms should take reasonable steps to ensure that where they have customer due diligence information in one part of the business, they are able to link it to information in another.

5.5.8 At all times, firms should bear in mind their obligations under the Data Protection Act only to seek information that is needed for the declared purpose, not to retain personal information longer than is necessary, and to ensure that information that is held is kept up to date.

Regulation 33(1)

5.5.9 In addition to the general obligation, referred to in paragraph 5.5.1, to apply EDD measures, the ML Regulations prescribe seven specific circumstances in respect of which EDD measures must be applied. These are:

- in any case identified by the firm under its risk assessment (or in information provided by the supervisory authorities) where there is a high risk of ML/TF;
- in any business relationship with a person established in a FATF call for action country or in relation to any relevant transaction where either of the parties is established in a FATF call for action country (see 5.5.11);
- in relation to correspondent relationships with a credit or financial institution (see Part II, Sector 16: *Correspondent relationships*);
- if a firm has determined that a customer or potential customer is a PEP, or a family member or known close associate of a PEP (see paragraphs 5.5.13ff);
- in any case where a customer has provided false or stolen identification documents or information on establishing a relationship;
- in any case where:
  - a transaction is unusually complex or unusually large; or there is an unusual pattern of transactions, or
  - the transaction or transactions have no apparent economic or legal purpose, or
- in any case which by its nature presents a higher risk of money laundering or terrorist financing.

Regulation 33(2)

5.5.10 The obligation to apply EDD measures does not apply when the customer is a branch or majority owned subsidiary undertaking located in a FATF call for action country of an entity which is established in a third country

and subject to requirements in national legislation having an equivalent effect to those laid down in the fourth money laundering directive as an obliged entity, if -

- the branch or subsidiary undertaking is subject to and complies fully with group-wide policies and procedures established by the entity having an equivalent effect to those laid down in the directive; and
- the firm, applying a risk-based approach, does not consider that it is necessary to apply EDD measures.

Regulation 33(1)(b) and (3)

5.5.11 There are two separate scenarios for which EDD measures must be applied when a FATF call for action country is involved: Where there is a business relationship with a person established in a FATF call for action country, or when a firm is undertaking a relevant transaction where either of the parties is established in a FATF call for action country.

A 'FATF call for action country' means a country named on the list of High-Risk Jurisdictions subject to a Call for Action, as published by FATF, that identifies countries with strategic deficiencies in the area of ant-money laundering, counter terrorist financing or counter proliferation financing.[25]

EDD and enhanced ongoing monitoring is required from the date a country is added to the list.

Being 'established in' a country for a legal person means being incorporated in or having its principal place of business in that country, for a financial or credit institution it means having its principal regulatory authority in that country, or for an individual it means being resident in that country (not just being born there).

A 'relevant transaction' means a transaction to which a firm must apply CDD measures under Regulation 27. These are occasional transactions that either exceed £12,000, or they are a transfer of fund amounts within the meaning of Article 3.9 of the funds transfer regulation that exceed £800; In this context a relevant transaction therefore relates to an occasional transaction which the firm undertakes for the customer outside of an established business relationship, and does not include ongoing payment activities undertaken within an established business relationship.

In any business relationship with a person established in a FATF call for action country or in relation to any relevant transaction where either party is established in a FATF call for action country, EDD measures must include obtaining:

- additional information on the customer and their beneficial owner;
- additional information on the intended nature of the business relationship;
- information of the source of funds and source of wealth of the customer and their beneficial owners;
- information on the reasons for the transactions;
- approval of senior management for establishing and continuing the business relationship;

25 https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html

- conducting enhanced monitoring of the business relationship by increasing the number and timing of controls, and selecting patterns of transactions that need further examination.

All of these additional EDD measures must be applied to new and existing customers, but the extent thereof may be considered and adjusted based on the level of risk of the customer. See also Annex 5-IV.

Regulation 33(4A); (4B) 5.5.12 Firms that provide life insurance policies must consider the nature and identity of the beneficiary of the policy, when assessing whether there is a high risk of money laundering and terrorist financing, and the extent of the measures which should be taken to manage and mitigate that risk.

Regulation 33(8) 5.5.12A When the beneficiary of a life insurance policy is a legal person or legal arrangement and presents a high risk of money laundering or terrorist financing for any reason, firms must take reasonable measures to identify and verify the identity of the beneficial owners of the beneficiary, before any payment is made under the policy.

Annex 5-IV to this chapter sets out suggested Risk Factor Guidelines on Enhanced Due Diligence.

Politically exposed persons (PEPs)

Regulation 35(3)(a) 5.5.13 Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to firms as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to known close associates. PEP status itself does not, of course, incriminate individuals or entities. It does, however, put the customer, or the beneficial owner, into a higher risk category. The level of risk associated with any PEP, family member or close associate (and the extent of EDD measures to be applied) must be considered on a case-by-case basis.

Regulation 35(4)(b) 48 5.5.14 The FCA is required to give guidance to the firms it supervises in relation to the EDD measures required under the ML Regulations in respect of PEPs, their family members and known close associates. Firms should have regard to this guidance.

Regulation 35(12) (a); (d-e) 5.5.15 A PEP is defined as an individual who is entrusted with prominent public functions, other than as a middle-ranking or more junior official.

Regulation 35(3A) A domestic PEP is a PEP entrusted with prominent public functions by the UK. A domestic PEP, or a family member or a known close associate of a domestic PEP has an inherently lower risk than a non-domestic PEP, and if there are no enhanced risk factors * present the extent of the EDD applied will be less than that applied to a non-domestic PEP.

Regulation 35(9) 5.5.16 Under the definition of a PEP the obligation to apply EDD measures to an individual ceases after they have left office for one year, or for such longer period as the firm considers appropriate, in order to address risks of ML/TF in relation to that person.

---

*means risk factors other than the customer's or potential customer's position as a domestic PEP or as a family member or a known close associate of that domestic PEP (Regulation 12(f))

Regulation 35(14)

5.5.17 Individuals entrusted with prominent public functions include:

- heads of state, heads of government, ministers and deputy or assistant ministers;
- members of parliaments or of similar legislative bodies;
- members of supreme courts, of constitutional courts or of other high-level judicial bodies the decisions of which are not subject to further appeal, except in exceptional circumstances;
- members of courts of auditors or of the boards of central banks;
- ambassadors, charges d'affaires and high-ranking officers in the armed forces (other than in respect of relevant positions at Community and international level);
- members of the administrative, management or supervisory boards of State-owned enterprises; and
- directors, deputy directors and members of the board or equivalent function of an international organisation.

These categories do not include middle-ranking or more junior officials.

5.5.18 Public functions exercised at levels lower than national should normally not be considered prominent. However, when their political exposure is comparable to that of similar positions at national level, for example, a senior official at state level in a federal system, firms should consider, on a risk-based approach, whether persons exercising those public functions should be considered as PEPs.

Regulation 35(12)(b)

5.5.19 Family members of a PEP include:

- a spouse or partner of that person;
- children of that person and their spouses or partners; and
- parents of that person.

Regulation 35(12)(c)

5.5.20 Known close associates of a PEP include:

- an individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a PEP; and
- an individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a PEP.

Regulation 35(11)

5.5.21 A firm is no longer obliged to apply EDD measures to family members or close associates of a PEP when the PEP is no longer entrusted with a prominent public function, whether or not the period in paragraph 5.5.16 has expired.

Regulation 35(15)

5.5.22 For the purpose of deciding whether a person is known to be a close associate of a PEP, the firm need only have regard to any information which is in its possession, or which is publicly known. Having to obtain knowledge of such a relationship does not presuppose an active research by the firm.

Regulation 35(1), (5)

5.5.23 Firms are required, on a risk-sensitive basis, to:

- have in place appropriate risk management systems and procedures to determine whether a customer or the beneficial owner of a

customer is a PEP, or a family member or known close associate of a PEP;

- obtain appropriate senior management approval for establishing, or continuing, a business relationship with such a customer;
- take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship or occasional transaction; and
- conduct enhanced ongoing monitoring of the business relationship.

Risk-based procedures

5.5.24 The nature and scope of a particular firm's business will generally determine whether the existence of PEPs in their customer base is an issue for the firm, and whether or not the firm needs to screen all customers for this purpose. In the context of this risk analysis, it would be appropriate if the firm's resources were focused in particular on products and transactions that are characterised by a high risk of money laundering.

Regulation 35(3) 35(4)(b)

5.5.25 Firms should take a proportional, risk-based and differentiated approach to conducting transactions or business relationships with PEPs, depending on where they are assessed on the scale of risk.

5.5.26 Establishing whether individuals qualify as PEPs, and therefore the appropriate level of EDD to carry out, is not always straightforward and can present difficulties. On the face of it, the legal definition is quite explicit, but there is clearly a hierarchy, or continuum, of PEPs, from those who may technically qualify under the definition, but be just above a 'middle ranking or junior official' level, to those who have significant, or even absolute, control over the levers, patronage and resources in any given area or jurisdiction. This process can be particularly difficult when seeking to form a view on the status of close family members, such as children and their spouses, who may in reality be quite distant – or even estranged – from their parent(s) or other PEP-status relative.

Regulation 35(3), (4)

5.5.27 In order to determine how to assess individual customers for PEP purposes, firms' analysis should therefore employ an appropriate risk-based approach, to assess where on the PEP continuum an individual lies. Firms are under a legal requirement to conduct EDD on PEPs, their family members and known close associates. The levels of money laundering/terrorist financing risk presented will vary on a case-by-case basis. The higher up the risk scale a PEP is, the more extensive the EDD measures that should be carried out. Conversely, in cases lower down the risk scale, it may be appropriate for firms to take less intrusive and less exhaustive EDD measures.

5.5.28 Where firms need to carry out specific checks, they may be able to rely on an internet search engine, or consult relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations. Resources such as the Transparency International Corruption Perception Index, which ranks approximately 180 countries according to their perceived level of corruption, may be helpful in terms of assessing the risk. The IMF, World Bank and some non-governmental organisations also publish

relevant reports. If there is a need to conduct more thorough checks, or if there is a high likelihood of a firm having PEPs for customers, subscription to a specialist PEP database may be an adequate risk mitigation tool.

Source of wealth

5.5.29 It is for each firm to decide the steps it takes to determine whether a PEP is seeking to establish a business relationship for legitimate reasons.

Regulation 35(5)(b)

5.5.30 Firms must take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship in order to allow the firm to satisfy itself that it does not handle the proceeds from corruption or other criminal activity. The measures firms should take to establish the PEP's source of wealth and the source of funds will depend on the degree of risk associated with the business relationship, and where the individual sits on the PEP continuum. Firms should verify the source of wealth and the source of funds on the basis of reliable and independent data, documents or information where the risk associated with the PEP relationship is particularly high.

5.5.31 Firms should, where possible, refer to information sources such as asset and income declarations, which some jurisdictions expect certain senior public officials to file and which often include information about an official's source of wealth and current business interests[26]. Firms should note that not all declarations are publicly available and that a PEP customer may have legitimate reasons for not providing a copy. Firms should also be aware that some jurisdictions impose restrictions on their PEPs' ability to hold foreign bank accounts or to hold other office or paid employment.

5.5.32 For PEPs who are assessed as being higher on the scale of risk, firms could, for example, and when conducting source of wealth checks on funds from inheritance, request a copy of the relevant will. Where the wealth/funds of such PEPs originate from the sale of property, firms could seek evidence of conveyancing.

Senior management approval

5.5.33 Obtaining approval from senior management for establishing, or continuing, a business relationship does not necessarily mean obtaining approval from the Board of directors (or equivalent body), but from a higher level of authority from the person seeking such approval. As risk

[26] The World Bank has compiled a library on various countries' laws about disclosure of officials' income and assets. See http://publicofficialsfinancialdisclosure.worldbank.org/about-the-library

dictates, firms should escalate decisions to more senior management levels.

5.5.34 The appropriate level of seniority for sign off should therefore be determined by the level of increased risk associated with the business relationship; and the senior manager approving a PEP business relationship should have sufficient seniority and oversight to take informed decisions on issues that directly impact the firm's risk profile, and not (solely) on the basis that the individual is a PEP. When considering whether to approve a PEP relationship, senior management should base their decision on the level of ML/TF risk the firm would be exposed to if it entered into that business relationship and how well equipped the firm is to manage that risk effectively.

On-going monitoring

5.5.35 Guidance on the on-going monitoring of the business relationship is given in Chapter 5.7. Firms should remember that new and existing customers may not initially meet the definition of a PEP, but may subsequently become one during the course of a business relationship. The firm 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. When an existing customer is identified as a PEP, EDD measures must be applied to that customer.

5.5.36 Firms should identify unusual transactions and regularly review the information they hold to ensure that any new or emerging information that could affect the risk assessment is identified in a timely fashion. The frequency of ongoing monitoring and review should be determined by the level of risk associated with the relationship.

5.6 Multipartite relationships, including reliance on third parties

5.6.1 Frequently, a customer may have contact with two or more firms in respect of the same transaction. This can be the case in both the retail market, where customers are routinely introduced by one firm to another, or deal with one firm through another, and in some wholesale markets, such as syndicated lending, where several firms may participate in a single loan to a customer.

5.6.2 However, several firms requesting the same information from the same customer in respect of the same transaction not only does not help in the fight against financial crime, but also adds to the inconvenience of the customer. It is important, therefore, that in all circumstances each firm is clear as to its relationship with the customer and its related AML/CTF obligations, and as to the extent to which it can rely upon or otherwise take account of the verification of the customer that another firm has carried out. Such account must be taken in a balanced way that appropriately reflects the money laundering or terrorist financing

risks. Account must also be taken of the fact that some of the firms involved may not be UK-based.

5.6.3 In other cases, a customer may be an existing customer of another regulated firm in the same group. Guidance on meeting AML/CTF obligations in such a relationship is given in paragraphs 5.6.24 to 5.6.27.

Reliance on third parties

Regulation 39

5.6.4 The ML Regulations expressly permit a firm to rely on another person to apply any or all of the CDD measures, provided that the other person is listed in Regulation 39(3) (see paragraph 5.6.6). The relying firm, however, retains responsibility for any failure to comply with a requirement of the Regulations, as this responsibility cannot be delegated.

5.6.5 For example:

- where a firm (firm A) enters into a business relationship with, or undertakes an occasional transaction for, the underlying customer of another firm (firm B), for example by accepting instructions from the customer (given through Firm B); or
- firm A and firm B both act for the same customer in respect of a transaction (e.g., firm A as executing broker and firm B as clearing broker),

firm A may rely on firm B to carry out CDD measures, while remaining ultimately liable for compliance with the ML Regulations.

Regulation 39(3)

5.6.6 In this context, Firm B must be:

(1) a person who carries on business in the UK who is subject to the requirements of the ML Regulations

(2) a person who carries on business in a third country who is subject to, and supervised for compliance with, CDD and record keeping requirements equivalent to those laid down in 4MLD;

(3) an organisation whose members consist of persons within (1) and (2) above.

Regulation 39(2)(a)

5.6.7 Where a firm relies on a third party to carry out CDD measures, it must immediately obtain from the third party all the information needed to identify the customer or beneficial owner.

Regulation 39(2)(b) 40(6)

5.6.8 The firm must enter into arrangements with the firm being relied on which:

- Enable the firm to obtain from the third party immediately on request copies of any identification and verification data and any other relevant documentation on the identity of the customer or beneficial owner;

- Require the third party to retain copies of the data and documents referred to for the periods set out in Regulation 40 (see paragraphs 8.12 and 8.18).

Regulation 39(7)(8)

5.6.9 Nothing in the ML Regulations prevents a firm applying CDD measures by means of an agent or an outsourcing service provider (but see paragraphs 5.6.13 to 5.6.16), provided that the arrangements between the firm and the agent or outsourcing service provider provide for the firm to remain liable for any failure to apply such measures.

Basis of reliance

5.6.10 For one firm to rely on verification carried out by another firm, the verification that the firm being relied upon has carried out must have been based at least on the standard level of customer verification. It is not permissible to rely on SDD carried out, or any other exceptional form of verification, such as the use of source of funds as evidence of identity.

5.6.11 Firms may also only rely on verification actually carried out by the firm being relied upon. A firm that has been relied on to verify a customer's identity may not 'pass on' verification carried out for it by another firm.

Regulation 10(2)(a),

5.6.12 Under the ML Regulations, the FCA has the additional responsibility for supervising the AML/CTF systems and controls in Annex I Financial Institutions. Such businesses are not regulated by the FCA, and may not therefore be relied on to carry out CDD measures on behalf of other firms until such time as this is permitted under the ML Regulations.

5.6.13 Whether a firm wishes to place reliance on a third party will be part of the firm's risk-based assessment, which, in addition to confirming the third party's regulated status, may include consideration of matters such as:

- its public disciplinary record, to the extent that this is available;
- the nature of the customer, the product/service sought and the sums involved;
- any adverse experience of the other firm's general efficiency in business dealings;
- any other knowledge, whether obtained at the outset of the relationship or subsequently, that the firm has regarding the standing of the firm to be relied upon.

5.6.14 The assessment as to whether or not a firm should accept confirmation from a third party that appropriate CDD measures have been carried out on a customer will be risk-based, and cannot be based simply on a single factor.

5.6.15 In practice, the firm relying on the confirmation of a third party needs to know:

- the identity of the customer or beneficial owner whose identity is being verified;
- the level of CDD that has been carried out; and

- confirmation of the third party's understanding of his obligation to make available, on request, copies of the verification data, documents or other information.

In order to standardise the process of firms confirming to one another that appropriate CDD measures have been carried out on customers, guidance is given in paragraphs 5.6.29 to 5.6.30 below on the use of pro-forma confirmations containing the above information.

5.6.16 The third party has no obligation to provide such confirmation to the product/service provider, and may choose not to do so. In such circumstances, or if the product/service provider decides that it does not wish to rely upon the third party, then the firm must carry out its own CDD measures on the customer.

5.6.17 For a firm to confirm that it has carried out CDD measures in respect of a customer is a serious matter. A firm must not give a confirmation on the basis of a generalised assumption that the firm's systems have operated effectively. There has to be awareness that the appropriate steps have in fact been taken in respect of the customer that is the subject of the confirmation.

Regulation 40(7)

5.6.18 A firm (other than an agent or outsourced service provider) which is relied on by another person must, if requested by the firm relying on it, immediately

- make available to the firm which is relying on it any information about the customer (and any beneficial owner) which the third party obtained when applying CDD measures; and
- forward to the firm which is relying on it copies of any identification and verification data and other relevant documents on the identity of the customer (and any beneficial owner) which the third party obtained when applying those measures

5.6.19 The personal information supplied by the customer as part of a third party's customer identification procedures will generally be set out in the form that the relying firm will require to be completed, and this information will therefore be provided to that firm.

Regulation 40 (6), (7)

5.6.20 A request to forward copies of any identification and verification data and other relevant documents on the identity of the customer or beneficial owner obtained when applying CDD measures, if made, would normally be as part of a firm's risk-based customer acceptance procedures. However, the firm giving the confirmation must be prepared to provide these data or other relevant documents throughout the period for which it has an obligation under the Regulations to retain them.

5.6.21 Where a firm makes such a request, and it is not met, the firm will need to take account of that fact in its assessment of the third party in question, and of the ability to rely on the third party in the future.

5.6.22 A firm must also document the steps taken to confirm that the firm relied upon satisfies the requirements in Regulation 39(3). This is particularly important where the firm relied upon is situated outside the UK.

5.6.23 Part of the firm's AML/CTF policy statement should address the circumstances where reliance may be placed on other firms and how the firm will assess whether the other firm satisfies the definition of third party in Regulation 39(3) (see paragraph 5.6.6).

Group introductions

Regulation 39(6)

5.6.24 Where customers are introduced between different parts of the same financial sector group, entities that are part of the group should be able to rely on identification procedures conducted by that part of the group which first dealt with the customer. One member of a group should be able to confirm to another part of the group that the identity of the customer has been appropriately verified.

Regulation 39(5)

5.6.25 Where a customer is introduced by one part of a financial sector group to another, it is not necessary for their identity to be re-verified, provided that:

- the identity of the customer has been verified by the introducing part of the group in line with AML/CTF standards in the UK, the EU or an assessed low risk jurisdiction; and
- the group entity that carried out the CDD measures can be relied upon as a third party under Regulation 39(3).

5.6.26 The acceptance by a UK firm of confirmation from another group entity that the identity of a customer has been satisfactorily verified is dependent on the relevant records being readily accessible, on request, from the UK.

5.6.27 Where UK firms have day-to-day access to all group customer information and records, there is no need to obtain a group introduction confirmation, if the identity of that customer has been verified previously to AML/CTF standards in the EU, or in an assessed low risk jurisdiction. However, if the identity of the customer has not previously been verified, for example because the group customer relationship pre-dates the introduction of anti-money laundering regulations, or if the verification evidence is inadequate, any missing verification evidence will need to be obtained.

Use of pro-forma confirmations

Regulation 39 (3)

5.6.28 Whilst a firm may be able to place reliance on another party to apply all or part of the CDD measures under Regulation 39(3) (see paragraph 5.6.4), it may still wish to receive, as part of its risk-based procedures, a written confirmation from the third party. This may also be the case, for example, when a firm is unlikely to have an ongoing relationship with the third party. Confirmations can be particularly helpful when dealing with third parties located outside of the UK, where it is necessary to confirm that the relevant records will be available (see 5.6.18).

5.6.29 Pro-forma confirmations for customer identification and verification are attached as Annex 5-I to this chapter.

5.6.30 Pro-forma confirmations in respect of group introductions are attached as Annex 5-II to this chapter.

Situations which are not reliance

(i) One firm acting solely as introducer

5.6.31 At one end of the spectrum, one firm may act solely as an introducer between the customer and the firm providing the product or service, and may have no further relationship with the customer. The introducer plays no part in the transaction between the customer and the firm, and has no relationship with either of these parties that would constitute a business relationship. This would be the case, for example, in respect of name-passing brokers in inter-professional markets, on which specific guidance is given in Part II, Sector 19: *Name passing brokers in the inter-professional market.*

5.6.32 In these circumstances, where the introducer neither gives advice nor plays any part in the negotiation or execution of the transaction, the identification and verification obligations under the ML Regulations lie with the product/service provider. This does not, of course, preclude the introducing firm carrying out identification and verification of the customer on behalf of the firm providing the product or service, as agent for that firm (see paragraphs 5.6.34 – 5.6.35).

(ii) Where the intermediary is the agent of the product/service provider

5.6.33 If the intermediary is an agent or appointed representative of the product or service provider, it is an extension of that firm. The intermediary may actually obtain the appropriate verification evidence in respect of the customer, but the product/service provider is responsible for specifying what should be obtained, and for ensuring that records of the appropriate verification evidence taken in respect of the customer are retained.

5.6.34 Similarly, where the product/service provider has a direct sales force, they are part of the firm, whether or not they operate under a separate group legal entity. The firm is responsible for specifying what is required, and for ensuring that records of the appropriate verification evidence taken in respect of the customer are retained.

(ii) Where the intermediary is the agent of the customer

5.6.35 From the point of view of a product/service provider, the position of an intermediary, as agent of the customer, is influenced by a number of factors. The intermediary may be subject to the ML Regulations, or otherwise to the EU Fourth Money Laundering Directive, or to similar legislation in an assessed low risk jurisdiction. It may be regulated; it may be based in the UK, or in a country or jurisdiction outside the UK, which may or may not be a FATF member. Guidance on assessing which countries or jurisdictions might be low risk jurisdictions is given at Annex 4-I.

Regulation 37(1)

5.6.36 A firm should understand and document who its customer is and which of the underlying parties it has a business relationship with (i.e. customers that require risk-based CDD measures).

5.6.37 Depending on jurisdiction, where the customer is an intermediary carrying on appropriately regulated business, and is acting on behalf of another, and the firm determines that the situation presents a low degree of risk of ML/TF, the product provider may decide to carry out SDD measures on both the customer and on the underlying party (see paragraph 5.3.134).

5.6.38 Where the firm takes instruction from the underlying customer, or where the firm acts on the underlying customer's behalf (e.g. as a custodian) the firm then has an obligation to carry out CDD measures in respect of that customer, although the reliance provisions (see paragraphs 5.6.4ff) may be applied. Where the underlying party is a low risk customer of the firm, SDD may be applied.

5.6.39 In these circumstances, in verifying the identity of the underlying customer, the firm should take a risk-based approach. It will need to assess the AML/CTF regime in the intermediary's jurisdiction, the level of reliance that can be placed on the intermediary and the verification work it has carried out, and as a consequence, the amount of evidence that should be obtained direct from the customer.

5.6.40 In particular, where the intermediary is located in a higher risk jurisdiction, or in a country listed as having material deficiencies, the risk-based approach should be aimed at ensuring that the business does not proceed unless the identity of the underlying customers have been verified to the product/service provider's satisfaction.

5.7 Monitoring customer activity

The requirement to monitor customers' activities

Regulation 28(11)

5.7.1 Firms must conduct ongoing monitoring of the business relationship with their customers. Its monitoring arrangements should be risk based, driven by the nature, size and complexity of the firm's business and form part of its financial crime control framework. Ongoing monitoring of a business relationship includes:

- Scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the firm's knowledge of the customer, its business and risk profile;
- Ensuring that the documents or information obtained for the purposes of applying customer due diligence are kept up to date.

5.7.2 Monitoring customer activity helps identify unusual activity. If unusual activities cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions that take place throughout a relationship helps firms know their customers, assist them to assess risk and provides greater assurance that the firm is not being used for the purposes of financial crime

What is monitoring?

5.7.3 The essentials of any system of monitoring are that:

- it flags up transactions and/or activities for further examination;
- these reports are reviewed promptly by the right person(s); and
- appropriate action is taken on the findings of any further examination.

5.7.4 Monitoring can be either:

- in real time, in that transactions and/or activities can be reviewed as they take place or are about to take place, or
- after the event, through some independent review of the transactions and/or activities that a customer has undertaken. This may be conducted over a reasonable time period to identify patterns/trends

and in either case, the objective is to identify or flag unusual transactions or activities for further examination.

5.7.5 Monitoring may be by reference to specific types of transactions, to the profile of the customer, to networks of connected persons, or by comparing their activity or profile with that of a similar, peer group of customers, or through a combination of these approaches.

5.7.6 Firms should also have systems and procedures to deal with customers who have not had contact with the firm 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 unauthorised use.

5.7.7 In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume and size of transactions with customers, in the context of the assessed customer and product risk.

5.7.8 Monitoring is not a mechanical process and does not necessarily require sophisticated electronic systems. The scope and complexity of the process will be influenced by the firm's business activities, and whether the firm is large or small. The key elements of any system are having up-to-date customer information and being aware of evolving financial crime risks and typologies that are relevant to the firm, on the basis of which it will be possible to spot the unusual, and asking pertinent questions to elicit the reasons for unusual transactions or activities in order to judge whether they may represent something suspicious.

5.7.8A Transaction monitoring is a dynamic process, and therefore monitoring arrangements, including automated monitoring system rules and thresholds should be reviewed regularly to ensure that they remain effective. This may include reallocating resources from less productive or less efficient monitoring arrangements (i.e. activity that never or seldom contributes to the management of financial crime risk) to higher priority risks to ensure that monitoring provides more effective outcomes.

These arrangements and any changes to them should be documented appropriately and be subject to regular review.

Nature of monitoring

5.7.9 Some financial services business typically involves transactions with customers about whom the firm has a good deal of information, acquired for both business and regulatory reasons. Other types of financial services business involve transactions with customers about whom the firm may need to have only limited information. The nature of the monitoring in any given case will therefore depend on the business of the firm, the frequency of customer activity, and the types of customers that are involved.

5.7.10 Effective monitoring is likely to be based on a considered identification of transaction characteristics, such as:

- the unusual nature of a transaction: e.g., abnormal size or frequency for that customer or peer group; the early surrender of an insurance policy;
- the nature of a series of transactions: for example, a number of cash credits;
- the geographic destination or origin of a payment: for example, to or from a high-risk country; the parties concerned: for example, a request to make a payment to or from a person on a sanctions list;
- known threats or typologies (including in the public domain); and
- depending on and in keeping with a firm's nature, size and complexity - networks of connected accounts / counterparties / customers / beneficial owners.

5.7.11 The arrangements should include the training of staff on procedures to spot and deal specially (e.g. by referral to management) with situations that arise that suggest a heightened money laundering risk; or they could involve arrangements for exception reporting by reference to objective triggers (e.g. transaction amount). Staff training is not, however, a substitute for having in place some form of regular monitoring activity.

Regulation 33(1), 33(5)(d)

5.7.12 Higher risk accounts and customer relationships require enhanced ongoing monitoring. This will generally mean more frequent or intensive monitoring on a risk-based approach.

Manual or automated?

5.7.13 A monitoring system may be manual, or may be automated to the extent that a standard suite of exception reports are produced, or it may be a combination of the two. One or other of these approaches may suit most

firms. In firms where there are major issues of volume, or where there are other factors that make a basic exception report regime inappropriate, a more sophisticated automated system may be necessary. Where manual monitoring is in place, firms should have procedures to manage the risk of manual error.

5.7.14 It is essential to recognise the importance of staff alertness. Such factors as staff intuition, direct exposure to a customer face-to-face or on the telephone, and the ability, through practical experience, to recognise transactions that do not seem to make sense for that customer, cannot be automated (see Chapter 8: Staff awareness, training and alertness).

5.7.15 In relation to a firm's monitoring needs, an automated system may add value to manual systems and controls, provided that the parameters determining the outputs of the system are appropriate. Firms should understand the workings and rationale of an automated system, and should understand the reasons for its output of alerts, as it may be asked to explain this to its regulator.

5.7.16 The greater the volume of transactions, the less easy it will be for a firm to monitor them without the aid of some automation. Systems available include those that many firms, particularly those that offer credit, use to monitor fraud. Although not specifically designed to identify money laundering or terrorist financing, the output from these anti-fraud monitoring systems can often indicate possible money laundering or terrorist financing.

5.7.17 There are many automated transaction monitoring systems available on the market; they use a variety of techniques to detect and report unusual/uncharacteristic activity. These techniques can range from artificial intelligence to simple rules. The systems available are not designed to detect money laundering or terrorist financing, but are able to detect and report unusual/uncharacteristic behaviour by customers, and patterns of behaviour that are characteristic of money laundering or terrorist financing, which after analysis may lead to suspicion of money laundering or terrorist financing. The implementation of transaction monitoring systems is difficult due to the complexity of the underlying analytics used and their heavy reliance on customer reference data and transaction data.

The ongoing effectiveness of these systems also depends on the system parameters that are used (e.g. rules/thresholds). Firms should ensure that the thresholds used are relevant and applicable to their business and customer activities.

5.7.18 Monitoring systems, manual or automated, can vary considerably in their approach to detecting and reporting unusual or uncharacteristic behaviour. It is important for firms to ask questions of the supplier of an automated system, and internally within the business, whether in support of a manual or an automated system, to aid them in selecting a solution that meets their particular business needs best. Questions that should be addressed include:

- How does the solution enable the firm to implement a risk-based approach to customers, third parties and transactions?

- How do system parameters aid the risk-based approach and consequently affect the quality of transactions alerted?
- What are the money laundering/terrorist financing typologies that the system addresses, and which component of the system addresses each typology? Are the typologies that are included with the system complete? Are they relevant to the firm's particular line of business? How often are they updated?
- What functionality does the system provide to implement new typologies, how quickly can relevant new typologies be commissioned in the system and how can their validity be tested prior to activation in the live system?
- What functionality exists to provide the user with the reason that a transaction is alerted and is there full evidential process behind the reason given?
- Does the system have robust mechanisms to learn from previous experience and how are unproductive alerts/ 'false positives' continually monitored and reduced?

Although monitoring processes may be outsourced, firms remain responsible for their regulatory obligations.

5.7.19 What constitutes unusual or uncharacteristic behaviour by a customer, is often defined by the system. It will be important that the system selected has an appropriate definition of 'unusual or uncharacteristic' and one that is in line with the nature of business conducted by the firm.

5.7.20 The effectiveness of a monitoring system, automated or manual, in identifying unusual activity will depend on the quality of the parameters which determine what alerts it makes, and the ability of staff to assess and act as appropriate on these outputs. The needs of each firm will therefore be different, and each system will vary in its capabilities according to the scale, nature and complexity of the business. It is important that the balance is right in setting the level at which an alert is generated; it is not enough to fix it so that the system generates just enough output for the existing staff complement to deal with – but equally, the system should not generate large numbers of unproductive alerts/'false positives', which require excessive resources to investigate.

Firms should establish an appropriate governance mechanism for the oversight, review and approval of monitoring processes and parameters, which will include documenting its monitoring arrangements and rationale. This may include consideration of the following, for example:

- Defining responsibilities for the governance mechanism
- Measuring the effectiveness and relevance of monitoring arrangements
- Supporting changes to systems to address evolving ML/TF risks
- Approach and governance for reallocation of resource (e.g. turning off/dialling down less efficient monitoring parameters or introducing different parameters)

5.7.21 Monitoring also involves keeping information held about customers up to date, as far as reasonably possible. Guidance on this is given at paragraphs 5.3.27 - 5.3.28.

ANNEX 5-I/1

CONFIRMATION OF VERIFICATION OF IDENTITY

PRIVATE INDIVIDUAL

INTRODUCTION BY A UK-REGULATED FIRM

1 DETAILS OF INDIVIDUAL (see explanatory notes below)

Full name of Customer	

Current Address		Previous address if individual has changed address in the last three months

Date of Birth	

2 CONFIRMATION

I/we confirm that

(a) the information in section 1 above was obtained by me/us in relation to the customer;

(b) the evidence I/we have obtained to verify the identity of the customer:
[tick only one]

meets the standard evidence set out within the Guidance for the UK Financial Sector issued by JMLSG ; or	
exceeds the standard evidence (written details of the further verification evidence taken are attached to this confirmation).	

Signed:	
Name:	
Position:	
Date:	

3 DETAILS OF INTRODUCING FIRM (OR SOLE TRADER)

Full Name of Regulated Firm (or Sole Trader):	
FCA Reference Number:	

Explanatory notes

1. A separate confirmation must be completed for each customer (e.g. joint holders, trustee cases and joint life cases). Where a third party is involved, e.g. a payer of contributions who is different from the customer, the identity of that person must also be verified, and a confirmation provided.
2. This form cannot be used to verify the identity of any customer that falls into one of the following categories:
   - those who are exempt from verification as being an existing client of the introducing firm prior to the introduction of the requirement for such verification;
   - those who have been subject to Simplified Due Diligence under the Money Laundering Regulations; or
   - those whose identity has been verified using the source of funds as evidence.

ANNEX 5-I/2

CONFIRMATION OF VERIFICATION OF IDENTITY

PRIVATE INDIVIDUAL

INTRODUCTION BY AN EQUIVALENTLY REGULATED[1] THIRD COUNTRY FINANCIAL SERVICES FIRM

1 DETAILS OF INDIVIDUAL (see explanatory notes below)

Full name of Customer	

Current Address		Previous address if individual has changed address in the last three months

Date of Birth	

2 CONFIRMATION

We confirm that

(a) the information in section 1 above was obtained by us in relation to the customer;

(b) the evidence we have obtained to verify the identity of the customer meets the requirements of our national money laundering and terrorist financing legislation that has an equivalent effect to the requirements laid down in the EU Fourth Money Laundering Directive, and any relevant authoritative guidance provided as best practice in relation to the type of business or transaction to which this confirmation relates;

(c) copies of the underlying evidence taken in relation to the verification of the customer's identity will, on request from you (or from UK law enforcement agencies or regulators under court order or relevant mutual assistance procedure), be made available immediately, to the extent that we are required under local law to retain these records.

Signed:	
Name:	
Position:	
Date:	

3 DETAILS OF INTRODUCING FIRM

Full Name of Regulated Firm:	
Jurisdiction:	
Name of Regulator:	
Regulator Reference Number:	

1 A regulated firm that carries on business outside the UK that is (i) subject to requirements in relation to CDD and record keeping that are equivalent to those laid down in the 4th MLD; and (ii) supervised with compliance with those requirements in a manner equivalent to section 2 of Chapter VI of the 4th MLD.

Explanatory notes

1. A separate confirmation must be completed for each customer (e.g. joint holders, trustee cases and joint life cases). Where a third party is involved, e.g. a payer of contributions who is different from the customer, the identity of that person must also be verified, and a confirmation provided.
2. This form cannot be used to verify the identity of any customer that falls into one of the following categories:
   - those who are exempt from verification as being an existing client of the introducing firm prior to the adoption of our national legislation that implements the EU Fourth Money Laundering Directive.

ANNEX 5-I/3

CONFIRMATION OF VERIFICATION OF IDENTITY

CORPORATE AND OTHER NON-PERSONAL ENTITY

INTRODUCTION BY A UK-REGULATED FIRM

1 DETAILS OF CUSTOMER (see explanatory notes below)

Full name of customer	
Type of entity (corporate, trust, etc)	
Location of business (full operating address)	
Registered office in country of incorporation	
Registered number, if any (or appropriate)	
Relevant company registry or regulated market listing authority	
Names* of directors (or equivalent)	
Names* of principal beneficial owners (over 25%)	

*** And dates of birth, if known**

2 CONFIRMATION

I/we confirm that

(a) the information in section 1 above was obtained by me/us in relation to the customer;

(b) the evidence I/we have obtained to verify the identity of the customer: [tick only one]

meets the guidance for standard evidence set out within the guidance for the UK Financial Sector issued by JMLSG; or	
exceeds the standard evidence (written details of the further verification evidence taken are attached to this confirmation).	

Signed:	
Name:	
Position:	
Date:	

3 DETAILS OF INTRODUCING FIRM (OR SOLE TRADER)

Full Name of Regulated Firm (or Sole Trader):	
FCA Reference Number:	

Explanatory notes

1. "Relevant company registry" includes other registers, such as those maintained by charity commissions (or equivalent) or chambers of commerce.
2. This form cannot be used to verify the identity of any customer that falls into one of the following categories:
   - those who are exempt from verification as being an existing client of the introducing firm prior to the introduction of the requirement for such verification;
   - those who have been subject to Simplified Due Diligence under the Money Laundering Regulations; or
   - those whose identity has been verified using the source of funds as evidence.

ANNEX 5-I/4

CONFIRMATION OF VERIFICATION OF IDENTITY

CORPORATE AND OTHER NON-PERSONAL ENTITY *INTRODUCTION BY AN EQUIVALENTLY REGULATED THIRD COUNTRY FINANCIAL SERVICES FIRM*

1 DETAILS OF CUSTOMER (see explanatory notes below)

Full name of customer	
Type of entity (corporate, trust, etc)	
Location of business (full operating address)	
Registered office in country of incorporation	
Registered number, if any (or appropriate)	
Relevant company registry or regulated market listing authority	
Names* of directors (or equivalent)	
Names* of principal beneficial owners (over 25%)	

*** And dates of birth, if known**

2 CONFIRMATION

We confirm that

(a) the information in section 1 above was obtained by us in relation to the customer;

(b) the evidence we have obtained to verify the identity of the customer meets the requirements of our national money laundering and terrorist financing legislation that has an equivalent effect to requirements laid down by the EU Fourth Money Laundering Directive, and any relevant authoritative guidance provided as best practice in relation to the type of business or transaction to which this confirmation relates;

(c) copies of the underlying evidence taken in relation to the verification of the customer's identity will, in the event of any enquiry from you (or from UK law enforcement agencies or regulators under court order or relevant mutual assistance procedure), be made available immediately, to the extent that we are required under local law to retain these records.

Signed:	
Name:	
Position:	
Date:	

3 DETAILS OF INTRODUCING FIRM

Full Name of Regulated Firm:	
Jurisdiction:	
Name of Regulator:	
Regulator Reference Number:	

Explanatory notes

1. "Relevant company registry" includes other registers, such as those maintained by charity commissions (or equivalent) or chambers of commerce.
2. This form cannot be used to verify the identity of any customer that falls into one of the following categories:
   - those who are exempt from verification as being an existing client of the introducing firm prior to the adoption of our national legislation that implements the EU Forth Money Laundering Directive.

ANNEX 5-II/1

CONFIRMATION OF VERIFICATION OF IDENTITY
GROUP INTRODUCTION
PRIVATE INDIVIDUAL

1 DETAILS OF INDIVIDUAL (see explanatory notes below)

Full name of Customer		
Current Address		Previous address if customer has changed address in the last three months
Date of Birth		

2 CONFIRMATION

We confirm that

(a) the verification of the identity of the above customer meets the requirements:

i. of the Money Laundering Regulations 2017 (as amended), and the guidance for standard evidence set out within the guidance for the UK Financial Sector issued by JMLSG; or

ii. of our national money laundering and terrorist financing legislation that implements requirements in a manner equivalent to the EU Forth Money Laundering Directive, and any relevant authoritative guidance provided as best practice in relation to the type of business or transaction to which this confirmation relates; or

iii. of local law and regulation.

(b) copies of the underlying evidence taken in relation to the verification of the customer's identity will, in the event of any enquiry from you (or from UK law enforcement agencies or regulators under court order or relevant mutual assistance procedure), be made available immediately, to the extent that we are required under local law to retain these records.

Signed:	
Name:	
Position:	
Date:	

3 DETAILS OF GROUP FIRM

Full Name of Regulated Firm:	
Relationship to receiving firm:	
Jurisdiction:	
Name of Regulator:	
Regulator Reference Number:	

Explanatory notes

1. A separate confirmation must be completed for each customer (e.g. joint holders). Where a third party is involved, e.g. a payer of contributions who is different from the customer, the identity of that person must also be verified, and a confirmation provided.
2. This form cannot be used to verify the identity of any customer that falls into one of the following categories:
   - those who are exempt from verification as being an existing client of the introducing firm prior to the introduction of the requirement for such verification;
   - those whose identity has not been verified by virtue of the application of a permitted exemption under local anti money laundering law or regulation; or
   - those whose identity has been verified using the source of funds as evidence.

ANNEX 5-II/2

CONFIRMATION OF VERIFICATION OF IDENTITY

GROUP INTRODUCTION

CORPORATE AND OTHER NON-PERSONAL ENTITY

1 DETAILS OF CUSTOMER (see explanatory notes below)

Full name of customer	
Type of entity (corporate, trust, etc)	
Location of business (full operating address)	
Registered office in country of incorporation	
Registered number, if any (or appropriate)	
Relevant company registry or regulated market listing authority	
Names* of directors (or equivalent)	
Names* of principal beneficial owners (over 25%)	

*** And dates of birth, if known**

2 CONFIRMATION

We confirm that

(a) the verification of the identity of the above customer meets the requirements:

(i) of the Money Laundering Regulations 2017 (as amended), and the guidance for standard evidence set out within the guidance for the UK Financial Sector issued by JMLSG; or

(ii) of our national money laundering and terrorist financing legislation that implements requirements in a manner equivalent to the EU Fourth Money Laundering Directive, and any authoritative relevant guidance provided as best practice in relation to the type of business or transaction to which this confirmation relates; or

(iii) of local law and regulation.

(b) copies of the underlying evidence taken in relation to the verification of the customer's identity will, in the event of any enquiry from you (or from UK law enforcement agencies or regulators under court order or relevant mutual assistance procedure), be made available immediately, to the extent that we are required under local law to retain these records.

Signed:	
Name:	
Position:	
Date:	

3 DETAILS OF GROUP FIRM

Full Name of Regulated Firm:	
Relationship to receiving firm:	
Jurisdiction:	
Name of Regulator:	
Regulator Reference Number:	

Explanatory notes

1. "Relevant company registry" includes other registers, such as those maintained by charity commissions (or equivalent) or chambers of commerce.
2. This form cannot be used to verify the identity of any customer that falls into one of the following categories:
   - those who are exempt from verification as being an existing client of the introducing firm prior to the introduction of the requirement for such verification;
   - those whose identity has not been verified by virtue of the application of a permitted exemption under local anti money laundering law or regulation; or
   - those whose identity has been verified using the source of funds as evidence.

ANNEX 5-III

RISK FACTOR GUIDELINES

Simplified Due Diligence

Firms may apply simplified due diligence (SDD) measures in situations where the ML/TF risk associated with a business relationship is low. SDD is not an exemption from any of the CDD measures; however, firms may adjust the amount, timing or type of each or all of the CDD measures in a way that is commensurate to the low risk they identified.

SDD measures firms may apply include, but are not limited to:

- adjusting the timing of CDD, for example where the product or transaction sought has features that limit its use for ML/TF purposes, such as:

  (i) verifying the customer's or beneficial owner's identity during the establishment of the business relationship; or

  (ii) verifying the customer's or beneficial owner's identity once transactions exceed a defined threshold or once a reasonable time limit has lapsed. Firms must make sure that:

    a) this does not result in a *de facto* exemption from CDD, i.e. firms must ensure that the customer or beneficial owner's identity will ultimately be verified;

    b) the threshold or time limit is set at a reasonably low level;

    c) they have systems in place to detect when the threshold or time limit has been reached; and

    d) they do not defer CDD or delay obtaining relevant information about the customer where applicable legislation does not permit this.

- adjusting the quantity of information obtained for identification, verification or monitoring purposes, such as:

  (i) verifying identity on the basis of one document only; or

  (ii) assuming the nature and purpose of the business relationship because the product is designed for one particular use only, such as a company pension scheme or a shopping centre gift card.

- adjusting the quality or source of information obtained for identification, verification or monitoring purposes, for example:

  (i) accepting information obtained from the customer rather than an independent source when verifying the beneficial owner's identity; note that this is not permitted in relation to the verification of the customer's identity;

  (ii) where the risk associated with all aspects of the relationship is determined to be very low, relying on the source of funds to meet some of the CDD requirements,

e.g. where the funds are state benefit payments or where the funds have been transferred from an account in the customer's name at a EEA firm.

- adjusting the frequency of CDD updates and reviews of the business relationship, for example only when trigger events occur such as the customer looking to take out a new product or service, or when a certain transaction threshold is reached; firms must make sure that this does not result in a *de facto* exemption from keeping CDD information up-to-date.

- adjusting the frequency and intensity of transaction monitoring, for example by monitoring transactions above a certain threshold only. Where firms choose to do this, they must ensure that the threshold is set at a reasonable level and that they have systems in place to identify linked transactions which, taken together, would exceed that threshold.

The information a firm obtains when applying SDD measures must enable the firm to be reasonably satisfied that the risk associated with the relationship is low. It must also be sufficient to give the firm enough information about the nature of the business relationship to identify any unusual or suspicious transactions. SDD does not exempt an institution from reporting suspicious transactions to the FIU.

Where there are indications that the risk may not be low, for example where there are grounds to suspect that money laundering or terrorist financing is being attempted or where the firm has doubts about the veracity of the information obtained, SDD must not be applied.

ANNEX 5-IV

RISK FACTOR GUIDELINES

Enhanced due diligence

Unusual transactions

Firms should put in place adequate policies and procedures to detect unusual transactions or patterns of transactions. Where a firm detects transactions that are unusual because:

- they are larger than what the firm would normally expect based on its knowledge of the customer, the business relationship or the category to which the customer belongs; or

- they have an unusual or unexpected pattern compared to the customer's normal activity or the pattern of transactions associated with similar customers, products or services; or

- they are very complex compared to other, similar transactions by similar customer types, products or services,

and the firm is not aware of an economic rationale or lawful purpose or doubts the veracity of the information it has been given, it must apply EDD measures.

These EDD measures should be sufficient to help the firm determine whether these transactions give rise to suspicion and must at least include:

- taking reasonable measures to understand the background and purpose of these transactions, for example by establishing the source and destination of the funds or finding out more about the customer's business to ascertain the likelihood of the customer making such transactions; and

- monitoring the business relationship and subsequent transactions more frequently and with greater attention to detail. A firm may decide to monitor individual transactions where this is commensurate with the risk it has identified.

FATF call for action countries

When dealing with individuals or entities established or residing in a FATF call for action country EDD measures must be applied (see 5.5.11).
When adjusting the extent of EDD measures to be applied (including the timing of existing customer reviews), the following may inform the firm's risk-based approach:

- The constitution, industry sector, and overall money laundering and terrorist financing risk of the firm's customer-base, for example, considering different risk-based approaches to EDD measures applied to:

    - local or expatriate private individuals
    - corporate customers
    - regulated financial institutions
    - other customer types outlined in 5.3.177-5.3.293

- The presence of other AML/CTF regulated entities in a relationship or relationship structure that undertakes due diligence or provides management oversight of the customer, and are established in jurisdictions posing a lower risk;
- Whether the firm has a branch or subsidiary established in a FATF call for action country where the branch or subsidiary is subject to equivalent group wide policies and procedures;
- The specific strategic deficiencies in their AML/CTF regimes, jurisdictional typologies and respective compliance ratings assigned to each FATF recommendation, contributing to the FATF's designation of a particular country on the 'High-risk subject to a call for action' list;
- Existing customers that are already subjected to EDD measures as a result of the firm's customer risk assessment process, which considers the risk factors outlined in Annex 4-II. Firms may conclude that existing customers are already subjected to mandatory EDD measures and therefore no additional EDD is required.

When a country is removed from the FATF call for action list, the obligation to apply EDD measures as set out in 5.5.11 for a customer established in that country ends. Firms must continue to determine the extent of their CDD measures on a risk sensitive basis depending on the type of customer, business relationship, product or transaction.

Other high-risk situations

In all other high-risk situations, firms should take an informed decision which EDD measures are appropriate for each high-risk situation and the appropriate type of EDD (including the extent of additional information sought, and increased monitoring), will depend on the reason why a relationship was classified as high risk.

Firms will not need to apply all EDD measures listed below in all cases. For example, in certain high-risk situations it may be appropriate to focus on enhanced ongoing monitoring during the course of the business relationship.

EDD measures firms should apply may include:

- increasing the quantity of information obtained for CDD purposes:

    (i) about the customer's or beneficial owner's identity, or the customer's ownership and control structure, to be satisfied that the risk associated with the relationship is well known. This may include obtaining and assessing information about the customer's or beneficial owner's reputation and assessing any negative allegations against the customer or beneficial owner. Examples include:

        a. information about family members and close business partners;

        b. information about the customer's or beneficial owner's past and present business activities; and

        c. adverse media searches.

    (ii) about the intended nature of the business relationship, to ascertain that the nature and purpose of the business relationship is legitimate and to help firms obtain a more complete customer risk profile. It includes obtaining information on:

a. the number, size and frequency of transactions that are likely to pass through the account to be able to spot deviations that may give rise to suspicions. In some cases, requesting evidence may be appropriate;

b. why the customer looks for a specific product or service, in particular where it is unclear why the customer's needs cannot be met better in another way, or in a different jurisdiction;

c. the destination of funds; or

d. the nature of the customer's or beneficial owner's business to understand the likely nature of the business relationship better.

- increasing the quality of information obtained for CDD purposes to confirm the customer's or beneficial owner's identity including by:

  (i) requiring the first payment to be carried out through an account verifiably in the customer´s name with a bank subject to UK CDD standards; or

  (ii) establishing that the customer's source of wealth and source of funds that are used in the business relationship are not the proceeds from criminal activity and that they are consistent with the firm's knowledge of the customer and the nature of the business relationship. In some cases, where the risk associated with the relationship is particularly increased, verifying the source of wealth and the source of funds may be the only adequate risk mitigation tool. The sources of funds or wealth can be verified, among others, by reference to VAT and income tax returns, copies of audited accounts, pay slips, public deeds or independent and credible media reports.

- increasing the frequency of reviews, to be satisfied that the firm continues to be able to manage the risk associated with the individual business relationship or conclude that it no longer corresponds to its risk appetite and to help identify any transactions that require further review, including by:

  (i) increasing the frequency of reviews of the business relationship, to ascertain whether the customer's risk profile has changed and whether the risk remains manageable;

  (ii) obtaining the approval of senior management to commence or continue the business relationship to ensure senior management are aware of the risk their firm is exposed to and can take an informed decision about the extent to which they are equipped to manage that risk;

  (iii) reviewing the business relationship on a more regular basis to ensure any changes to the customer's risk profile are identified, assessed and, where necessary, acted upon; or

  (iv) conducting more frequent or in-depth transaction monitoring to identify any unusual or unexpected transactions that may give rise to suspicion of money laundering or terrorist financing. This may include establishing the destination of funds or ascertaining the reason for certain transactions.

See Revisions Sept 2026 Annex 5-V Pooled Accounts

ANNEX 5 - V

POOLED CLIENT ACCOUNTS

Note: This guidance is confined to Pooled Client Accounts.

1.1 Definition

A Pooled Client Account (PCA) is a bank account opened with the firm by a customer, for example a legal practitioner or letting/estate agent, to administer funds that belong to their own clients. Their clients' money will be co-mingled but the customer's clients will not be able to directly instruct the firm to carry out transactions.

Suspense accounts held by respondent institutions are not PCAs (refer to Part II Sector 16 on Correspondent Relationships).

There are two primary vectors of risk:

- The customer's clients misuse a PCA for ML/TF purposes without the knowledge of the customer; and
- The customer is complicit in using its PCAs for ML/TF purposes, either willingly or under duress.

1.2 Purpose

Firms should take reasonable measures to establish and document the purpose of PCAs. Although possible self-evident given the nature and purpose of the business relationship, firms may need to establish information such as: the types of clients whose funds are held in the PCAs, the level of assets deposited and the size of the transactions undertaken, and the exposure to industries and geographies recognised as vulnerable to money laundering, corruption or terrorist financing.

1.3 Risk Assessment

As part of the documented customer risk assessment (see 4.33ff), firms should consider whether the provision of PCAs impacts the customer's ML/TF risk, including whether:

- The funds in the PCA are backed by government schemes with enforcement powers through a judicial body (e.g. letting/property/estate agents and property management agents (known as 'property factors' in Scotland) in the UK);
- The PCA serves a limited, domestic, purpose;
- The customer is subject to the ML Regulations, or equivalent (e.g. UK legal professionals and accountancy practitioners that are subject to professional body AML supervision);
- The customer is subject to other regulatory or professional conduct obligations (e.g. client identification rules, professional conduct rules relating to dealing with funds in PCAs or client money protection regulations);
- The PCA is used for activity that is low risk and not within the scope of the ML Regulations (e.g. managing assets of individuals in care, litigation in the UK, or property management agents);
- The firm has taken reasonable measures to satisfy itself that the customer applies robust and risk-sensitive CDD measures (where relevant to regulated activity) to their own clients and its clients' beneficial owners (e.g. by obtaining copies of external or internal audit reports, appropriate representations from the customer, or reviewing the customer's relevant procedures);
- The customer is unnecessarily and/or unreasonably reluctant to provide information on the PCAs.

1.4 **Written Agreement**

The firm must enter into a written agreement with the customer, in which the customer agrees to provide, upon request, information on the identity (including verification documents/data where the customer undertakes CDD per the ML Regulations) of the owners of the funds held in the PCAs. Firms may decide to obtain this agreement through, for example, the inclusion of an appropriate clause in the product terms and conditions, through an attestation letter or similar.

The timescale agreed with the customer should be proportionate to the ML/TF risk, be reasonable within the context of the business relationship, and be sufficient to meet the needs of a court order should one be issued to the firm in relation to the PCAs.

1.5 **Due Diligence**

Where the firm concludes that the customer and its use of the PCA poses a low risk of ML/TF, it may apply simplified due diligence measures on the PCA. This means that the firm need not identify or verify the owners of the funds in the PCA.

Where the firm concludes that the customer presents a degree of ML/TF risk other than low (i.e. simplified due diligence cannot be applied), the firm must either take reasonable measures to identify and verify the identity of the owners of the funds held in the PCA (e.g. by entering into a formal reliance agreement as per 5.6.4), or take measures to decrease the ML/TF risk until simplified due diligence measures can be applied. Examples of such measures include:

- Subjecting the PCAs and/or wider business relationship to enhanced ongoing monitoring;
- Requesting that the customer sufficiently enhances their practices so that the firm is satisfied that the customer can provide, upon request, information regarding the identity of the owners of funds held in the PCA (including those customers that are not subject to the ML Regulations). Firms should take reasonable measures to confirm that the customer has done so (for example, sample testing the customer's ability to provide CDD or client identity information upon request);
- Restricting the type of customer's clients whose funds are held in the PCAs to those that pose a lower risk;

Firms should allow the customer a reasonable period to implement any such measures, taking into consideration factors such as: the level of ML/TF risk; the complexity of the business relationship; whether the customer is sufficiently low risk not to be subject to the ML Regulations; where the customer is otherwise low risk but not subject to CDD obligations; whether the customer understands the identity of its clients and the purpose of their transactions; whether the customer is complying with their own local legal/regulatory AML/CTF obligations; the level of cooperation provided by the customer, and the existence of legitimate privacy challenges.

CHAPTER 6

SUSPICIOUS ACTIVITIES, REPORTING AND DATA PROTECTION

- **Relevant law/regulation**
  - Regulations 19 (4)(d), 21(5) and 24
  - POCA ss327-340
  - SI2006/1070 (Exceptions to overseas conduct defence)
  - Terrorism Act, ss21, 39
  - Data Protection Act 2018, s7, s29
  - Financial sanctions legislation
- **Core obligations**
  - All staff must raise an internal report where they have knowledge or suspicion, or where there are reasonable grounds for having knowledge or suspicion, that another person is engaged in money laundering, or that terrorist property exists
  - The firm's nominated officer (or their appointed alternate) must consider all internal reports
  - The firm's nominated officer (or their appointed alternate) must make an external report to the National Crime Agency (NCA) as soon as is practicable if he considers that there is knowledge, suspicion, or reasonable grounds for knowledge or suspicion, that another person is engaged in money laundering, or that terrorist property exists
  - The firm must seek consent from the NCA before proceeding with a suspicious transaction or entering into arrangements
  - Firms must freeze funds if a customer is identified as being on the UK Sanctions List, and comply with reporting obligations
  - It is a criminal offence for anyone, following a disclosure to a nominated officer or to the NCA, to do or say anything that might either 'tip off' another person that a disclosure has been made or prejudice an investigation
  - The firm's nominated officer (or their appointed alternate) must report suspicious approaches, even if no transaction takes place
- **Actions required, to be kept under regular review**
  - Enquiries made in respect of disclosures must be documented
  - The reasons why a Suspicious Activity Report (SAR) was, or was not, submitted should be recorded
  - Any communications made with or received from the authorities, including the NCA, in relation to a SAR should be maintained on file
  - In cases where advance notice of a transaction or of arrangements is given, the need for prior consent before it is allowed to proceed should be considered

General legal and regulatory obligations

POCA ss 330, 331
Terrorism Act s 21A

6.1 Persons in the regulated sector are required to make a report in respect of information that comes to them within the course of a business in the regulated sector:

- where they *know* or
- where they *suspect* or
- where they *have reasonable grounds for knowing or suspecting*

that a person is engaged in, or attempting, money laundering or terrorist financing. Within this guidance, the above obligations are collectively referred to as "grounds for knowledge or suspicion".

Regulation 19(4)(d)
POCA s 330

6.2 In order to provide a framework within which suspicion reports may be raised and considered:

- each firm must ensure that any member of staff reports to the firm's nominated officer or their appointed alternate[27] (who may also be the MLRO in an FCA-regulated firm), where they have grounds for knowledge or suspicion that a person or customer is engaged in, or attempting, money laundering or terrorist financing;

Regulation 21(5)

- the firm's nominated officer must consider each such report, and determine whether it gives grounds for knowledge or suspicion;

Regulation 24

- firms should ensure that staff are appropriately trained in their obligations, and in the requirements for making reports to their nominated officer.

POCA, s 331
Terrorism Act s 21A

6.3 If the nominated officer determines that a report does give rise to grounds for knowledge or suspicion, they must report the matter to the NCA. Under POCA, the nominated officer is required to make a report to the NCA as soon as is practicable if they have grounds for suspicion that another person, whether or not a customer, is engaged in money laundering. Under the Terrorism Act, similar conditions apply in relation to disclosure where there are grounds for suspicion of terrorist financing.

6.4 A sole trader with no employees who knows or suspects, or where there are reasonable grounds to know or suspect, that a customer of theirs, or the person on whose behalf the customer is acting, is or has been engaged in, or attempting, money laundering or terrorist financing, must make a report promptly to the NCA.

POCA ss 333A -334
Terrorism Act ss 21D-H, 39

6.5 It is a criminal offence for any person, following a disclosure to a nominated officer or to the NCA, to release information that might 'tip off' another person that a disclosure has been made if the disclosure is likely to prejudice an investigation, if the information released came to that person in the course of a business in the UK regulated sector. It is also an offence for a person to disclose that an investigation into allegations that an offence has been committed is being contemplated or is being carried out; the disclosure is likely to prejudice that investigation and the information on which the disclosure is based came to the person in the course of a business in the regulated sector. It is also an offence for a person to disclose to another anything which is likely to prejudice an investigation resulting from a disclosure, or where the person knows or has reasonable cause to suspect that a disclosure has been or will be made.

Financial sanctions legislation

6.6 It is a criminal offence to make funds, economic resources or, in certain circumstances, financial services available to those persons or entities listed as the targets of financial sanctions legislation (see Part III). There is also a requirement to report to OFSI both details of funds frozen and where firms have knowledge or suspicion that a customer of the firm or a person with whom the firm has had business dealings is a listed person or entity, a person acting on behalf of a listed

[27] References in this chapter to 'nominated officer' should be taken to include 'or their appointed alternate' where applicable.

person or entity or has committed an offence under the sanctions legislation.

Attempted offences

POCA, s 330

Terrorism Act s21A(2)

6.7 POCA and the Terrorism Act provide that a disclosure must be made where there are grounds for suspicion that a person is engaged in money laundering or terrorist financing. "Money laundering" is defined in POCA to include an attempt to commit an offence under s327-329 of POCA. Similarly, under the Terrorism Act a disclosure must be made where a person has knowledge or suspicion that 'another person had committed *or attempted to commit* an offence under any of the sections 15-18'. There is no duty under s330 of POCA or s21A of the Terrorism Act to disclose information about the person who unsuccessfully attempts to commit fraud. This is because the attempt was to commit fraud, rather than to commit an offence under those Acts.

6.8 However, as soon as the firm has reasonable grounds to know or suspect that any benefit has been acquired, whether by the fraudster themself or by any third party, so that there is criminal property or terrorist property in existence, then, subject to paragraph 6.9, knowledge or suspicion of money laundering or terrorist financing must be reported to the NCA (see paragraphs 6.40ff). Who carried out the criminal conduct, and who benefited from it, or whether the conduct occurred before or after the passing of POCA, is immaterial to the obligation to disclose, but should be reported if known.

POCA, s330(3A)

6.9 In circumstances where neither the identity of the fraudster, nor the location of any related criminal property, is known nor is likely to be discovered, limited useable information is, however, available for disclosure. An example of such circumstances would be the theft of a chequebook, debit card, credit card, or charge card, which can lead to multiple low-value fraudulent transactions over a short, medium, or long term. In such instances, there is no obligation to make a report to the NCA where none of the following is known or suspected:

- the identity of the person who is engaged in money laundering;
- the whereabouts of any of the laundered property;
- that any of the information that is available would assist in identifying that person, or the whereabouts of the laundered property.

What is meant by "knowledge" and "suspicion"?

POCA, s 330 (2),(3), s 331 (2), (3)
Terrorism Act ss21A, 21ZA, 21ZB

6.10 Having knowledge means actually knowing something to be true. In a criminal court, it must be proved that the individual *in fact* knew that a person was engaged in money laundering. That said, knowledge can be *inferred* from the surrounding circumstances; so, for example, a failure to ask obvious questions may be relied upon by a jury to imply knowledge. The knowledge must, however, have come to the firm (or to the member of staff) in the course of business, or (in the case of a nominated officer) as a consequence of a disclosure under s 330 of

POCA or s 21A of the Terrorism Act. Information that comes to the firm or staff member in other circumstances does not come within the scope of the regulated sector obligation to make a report. This does not preclude a report being made should staff choose to do so, or are obligated to do so by other parts of these Acts.

6.11 Suspicion is more subjective and falls short of proof based on firm evidence. Suspicion has been defined by the courts as being beyond mere speculation and based on some foundation, for example:

> *"A degree of satisfaction and not necessarily amounting to belief but at least extending beyond speculation as to whether an event has occurred or not";* and
>
> *"Although the creation of suspicion requires a lesser factual basis than the creation of a belief, it must nonetheless be built upon some foundation."*

6.12 A transaction which appears unusual is not necessarily suspicious. Even customers with a stable and predictable transactions profile will have periodic transactions that are unusual for them. Many customers will, for perfectly good reasons, have an erratic pattern of transactions or account activity. So the unusual is, in the first instance, only a basis for further enquiry, which may in turn require judgment as to whether it is suspicious. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report then arises.

6.13 A member of staff, including the nominated officer, who considers a transaction or activity to be suspicious, would not necessarily be expected either to know or to establish the exact nature of any underlying criminal offence, or that the particular funds or property were definitely those arising from a crime or terrorist financing.

6.14 Transactions, or proposed transactions, such as '419' scams, are attempted advance fee frauds, and not money laundering; they are therefore not reportable under POCA or the Terrorism Act, unless the fraud is successful, and the firm is aware of resulting criminal property.

What is meant by "reasonable grounds to know or suspect"?

POCA, s 330 (2)(b), s 331 (2)(b) Terrorism Act s 21A

6.15 In addition to establishing a criminal offence when suspicion or actual knowledge of money laundering/terrorist financing is proved, POCA and the Terrorism Act introduce criminal liability for failing to disclose information when reasonable grounds exist for knowing or suspecting that a person is engaged in money laundering/terrorist financing. This introduces an objective test of suspicion. Reasonable grounds for suspecting are likely to depend upon particular circumstances and the member of staff should take into account such factors as the nature/origin of the transaction, how the funds, cash or asset(s) were discovered, the amounts or values involved, their intended movement and destination, how the funds cash or asset(s) came into the customer's possession, whether the customer(s) and/or the owners of the cash or asset(s) (if different) appear to have any links with

criminals/criminality, terrorists, terrorist groups or sympathisers, whether in the UK or overseas.

6.16 To defend themselves against a charge that they failed to meet the objective test of suspicion, staff within financial sector firms would need to be able to demonstrate that they took reasonable steps in the particular circumstances, in the context of a risk-based approach, to know the customer and the rationale for the transaction, activity or instruction. It is important to bear in mind that, in practice, members of a jury may decide, with the benefit of hindsight, whether the objective test has been met.

6.17 Depending on the circumstances, a firm being served with a court order in relation to a customer may give rise to reasonable grounds for suspicion in relation to that customer. In such an event, firms should review the information it holds about that customer across the firm, in order to determine whether or not such grounds exist.

Internal reporting

Regulation 19(4)(d)
POCA s 330(5)

6.18 The obligation to report to the nominated officer within the firm where they have grounds for knowledge or suspicion of money laundering or terrorist financing is placed on all relevant employees in the regulated sector. All financial sector firms therefore need to ensure that all relevant employees know who they should report suspicions to.

6.19 Firms may wish to set up internal systems that allow staff to consult with their line manager before sending a report to the nominated officer. The obligation under POCA is to report 'as soon as is reasonably practicable', and so any such consultations should take this into account. Where a firm sets up such systems it should ensure that they are not used to prevent reports reaching the nominated officer whenever staff have stated that they have knowledge or suspicion that a transaction or activity may involve money laundering or terrorist financing.

6.20 Whether or not a member of staff consults colleagues, the legal obligation remains with the staff member to decide for themself whether a report should be made; they must not allow colleagues to decide for them. Where a colleague has been consulted, they themself will then have knowledge on the basis of which they must consider whether a report to the nominated officer is necessary. In such circumstances, firms should make arrangements such that the nominated officer only receives one report in respect of the same information giving rise to knowledge or suspicion.

6.21 Short reporting lines, with a minimum number of people between the person with the knowledge or suspicion and the nominated officer, will ensure speed, confidentiality and swift access to the nominated officer.

6.22 All suspicions reported to the nominated officer should be documented, or recorded electronically. The report should include full details of the customer who is the subject of concern and as full a statement as possible of the information giving rise to the knowledge or suspicion.

All internal enquiries made in relation to the report should also be documented, or recorded electronically. This information may be required to supplement the initial report or as evidence of good practice and best endeavours if, at some future date, there is an investigation and the suspicions are confirmed or disproved.

6.23 Once an employee has reported their suspicion in an appropriate manner to the nominated officer, or to an individual to whom the nominated officer has delegated the responsibility to receive such internal reports, they have fully satisfied their statutory obligation.

6.24 Until the nominated officer advises the member of staff making an internal report that no report to the NCA is to be made, further transactions or activity in respect of that customer, whether of the same nature or different from that giving rise to the previous suspicion, should be reported to the nominated officer as they arise.

Non-UK offences

POCA, s 340 (2), (11)
SOCPA, s 102

6.25 The offence of money laundering, and the duty to report under POCA, apply in relation to the proceeds of any criminal activity, wherever conducted (including abroad), that would constitute an offence if it took place in the UK. However, this broad scope excludes activity (other than those referred to in paragraph 6.26) which the firm, staff member or nominated officer knows, or believes on reasonable grounds, to have been committed in a country or territory outside the UK and the activity was not unlawful under the criminal law then applying in the country or territory concerned. Firms may nevertheless have an obligation to report in that overseas country or territory, through an appropriate overseas reporting officer.

SI 2006/1070
1968 c 65
1976 c 32
2000 c 8

6.26 Offences committed overseas which the Secretary of State has prescribed by order as remaining within the scope of the duty to report under POCA are those which are punishable by imprisonment for a maximum term in excess of 12 months in any part of the United Kingdom if they occurred there, other than:

- an offence under the Gaming Act 1968;
- an offence under the Lotteries and Amusements Act 1976; or
- an offence under ss 23 or 25 of FSMA

Terrorism Act s21A (11)

6.27 The duty to report under the Terrorism Act applies in relation to taking any action, or being in possession of a thing, that is unlawful under ss 15-18 of that Act, that would have been an offence under these sections of the Act had it occurred in the UK.

POCA s 331
POCA ss 327-329
Terrorism Act s 21A

6.28 The obligation to consider reporting to the NCA applies only when the nominated officer has received a report made by someone working within the UK regulated sector, or when they themselves become aware of such a matter in the course of relevant business (which may come from overseas, or from a person overseas). The nominated officer is not, therefore, obliged to report everything that comes to their attention from outside of the UK, although they would be prudent to exercise their judgment in relation to information that comes to their attention from non-business sources. In reaching a decision on whether to make a

disclosure, the nominated officer must bear in mind the need to avoid involvement in an offence under ss327-329 of POCA.

Evaluation and determination by the nominated officer

Regulation 21(5)

6.29 The firm's nominated officer must consider each report and determine whether it gives rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion. The firm must permit the nominated officer to have access to any information, including 'know your customer' information, in the firm's possession which could be relevant. The nominated officer may also require further information to be obtained, from the customer if necessary, or from an intermediary who introduced the customer to the firm, to the extent that the introducer still holds the information (bearing in mind their own record keeping requirements). Any approach to the customer or to the intermediary should be made sensitively, and probably by someone other than the nominated officer, to minimise the risk of alerting the customer or an intermediary that a disclosure to the NCA may be being considered.

6.30 When considering an internal suspicion report, the nominated officer, taking account of the risk posed by the transaction or activity being addressed, will need to strike the appropriate balance between the requirement to make a timely disclosure to the NCA, especially if consent is required, and any delays that might arise in searching a number of unlinked systems and records that might hold relevant information.

6.31 As part of the review, other known connected accounts or relationships may need to be examined. Connectivity can arise commercially (through linked accounts, introducers etc.), or through individuals (third parties, controllers, signatories etc.). Given the need for timely reporting, it may be prudent for the nominated officer to consider making an initial report to the NCA prior to completing a full review of linked or connected relationships, which may or may not subsequently need to be reported to the NCA.

6.32 If the nominated officer decides not to make a report to the NCA, the reasons for not doing so should be clearly documented, or recorded electronically, and retained with the internal suspicion report.

External reporting

Regulation 19 (4)(d)
POCA, s 331
Terrorism Act, s 21A

6.33 The firm's nominated officer must report to the NCA any transaction or activity that, after their evaluation, they know or suspect, or have reasonable grounds to know or suspect, may be linked to money laundering or terrorist financing, or to attempted money laundering or terrorist financing. Such reports must be made as soon as is reasonably practicable after the information comes to them.

POCA, s 339

6.34 POCA provides that the Secretary of State may by order prescribe the form and manner in which a disclosure under s330, s331, s332 or s338 may be made.

6.35 The NCA prefers that SARs are submitted electronically via the secure internet system SAR Online, or via a dedicated bulk reporting facility. Information about access to and guidance on the use of SAR Online can be found at https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-illicit-finance/suspicious-activity-reports.

6.36 In order that an informed overview of the situation may be maintained, all contact between particular departments/branches and law enforcement agencies should be controlled through, or reported back to a single contact point, which will typically be the nominated officer. In the alternative, it may be appropriate to route communications through an appropriate member of staff in the firm's legal or compliance department.

6.37 A SAR's intelligence value is related to the quality of information it contains. A firm needs to have good base data from which to draw the information to be included in the SAR; there needs to be a system to enable the relevant information to be produced in hard copy for the law enforcement agencies, if requested under a court order.

6.38 Firms should include in each SAR as much relevant information about the customer, transaction or activity that it has in its records. In particular, the law enforcement agencies have indicated that details of an individual's occupation/company's business and National Insurance number are valuable in enabling them to access other relevant information about the customer. As there is no obligation to collect this information (other than in very specific cases), a firm may not hold these details for all its customers; where it has obtained this information in the course of normal business, however, it would be helpful to include it as part of a SAR made by the firm. The NCA's website (http://www.nationalcrimeagency.gov.uk) contains guidance on completing SARs in a way that gives most assistance to law enforcement. In particular, the NCA has published a glossary of terms, and find it helpful if firms use these terms when completing a SAR. NCA also publish, from time to time, guides to reporting entities.

Financial sanctions legislation

6.39 Firms must report to OFSI details of funds frozen under financial sanctions legislation and where the firm has knowledge or a suspicion that the financial sanctions measures have been or are being contravened, or that a customer is a listed person or entity, or a person acting on behalf of a listed person or entity. The firm may also need to consider whether the firm has an obligation also to report under POCA or the Terrorism Act.

Where to report

6.40 To avoid committing a failure to report offence, nominated officers must make their disclosures to the NCA. The national reception point for

disclosure of suspicions, and for seeking consent to continue to proceed with the transaction or activity, is the UKFIU within the NCA.

6.41 The UKFIU address is PO Box 8000, London, SE11 5EN and it can be contacted during office hours on: 020 7238 8282. SAR Online is a free, secure and 24/7 reporting service. The SAR online portal is available at: https://www.ukciu.gov.uk/(clevur45bdggypq2xpnag555)/saronline.aspx. Urgent disclosures, i.e., those requiring consent, should be transmitted electronically over a previously agreed secure link, if secure electronic methods are not available, by fax, as specified on the NCA website at www.nationalcrimeagency.gov.uk. Speed of response is assisted if the appropriate consent request is clearly mentioned in the title of any faxed report.

6.42 To avoid committing a failure to report offence under financial sanctions legislation, firms must make their reports to HM Treasury. The relevant unit is the Office of Financial Sanctions Implementation, HM Treasury, 1 Horse Guards Road, London SW1A 2HQ. Reports can be submitted electronically at ofsi@hmtreasury.gsi.gov.uk and the Unit can be contacted by telephone on 020 7270 5454.

Sanctions and penalties

POCA s334
Terrorism Act s21A

6.43 Where a person fails to comply with the obligation under POCA or the Terrorism Act to make disclosures to a nominated officer and/or the NCA as soon as practicable after the information giving rise to the knowledge or suspicion comes to the member of staff, a firm is open to criminal prosecution or regulatory censure. The criminal sanction, under POCA or the Terrorism Act, is a prison term of up to five years, and/or a fine.

Financial sanctions legislation

6.44 Where a firm fails to comply with the obligations to freeze funds, not to make funds, economic resources and, in relation to suspected terrorists, financial services, available to listed persons or entities or to report knowledge or suspicion, it is open to prosecution.

Consent

6.45 Care should be taken that the requirement to obtain consent for a particular transaction does not lead to the unnecessary freezing of a customer's account, thus affecting other, non-suspicious transactions.

Consent under POCA

POCA s 336

6.46 Reporting before or reporting after the event are not equal options which a firm can choose between. Where a customer instruction is received prior to a transaction or activity taking place, or arrangements being put in place, and there are grounds for knowledge or suspicion that the transaction, arrangements, or the funds/property involved, may relate to money laundering, a report must be made to the NCA and consent sought to proceed with that transaction or activity. In such circumstances, it is an offence for a nominated officer to consent to a

transaction or activity going ahead within the seven working day notice period from the working day following the date of disclosure, unless the NCA gives consent. Where urgent consent is required, use should be made of the process referred to in paragraph 6.41 above.

POCA ss 330 (6)(a), 331(6), 338 (3)(b)

6.47 When a transaction which gives rise to concern is already within an automated clearing or settlement system, where a delay would lead to a breach of a contractual obligation, or where it would breach market settlement or clearing rules, the nominated officer may need to let the transaction proceed and report it later. Where the nominated officer intends to make a report, but delays doing so for such reasons, POCA provides a defence from making a report where there is a reasonable excuse for not doing so. However, it should be noted that this defence is untested by case law, and would need to be considered on a case-by-case basis.

6.48 When a defence request is sought to undertake a future transaction or activity, or to enter into an arrangement, the disclosure should be sent electronically (ensuring that the tick box for a consent request is marked) or, if electronic methods are not available, faxed to the NCA UKFIU Consent Desk immediately the suspicion is identified. Defence requests should not be sent by post due to the timings involved, and additional postal copies are not required following submission by electronic means or fax. Further information is available on the NCA website www.nationalcrimeagency.gov.uk. The Consent Desk will apply NCA policy to each submission, carrying out the necessary internal enquiries, and will contact the appropriate law enforcement agency, where necessary, for a consent recommendation. Once the NCA's decision has been reached, the disclosing firm will be informed of the decision by telephone, and be given a reference number, which should be recorded. A formal letter will follow.

POCA, s 335, 336A, 336C

6.49 In the event that the NCA does not refuse a defence request within seven working days following the working day after the disclosure is made, the firm may process the transaction or activity, subject to normal commercial considerations. If, however, a defence request is refused within that period, a restraint order must be obtained by the authorities within a further 31 calendar days (the moratorium period[28]) from the day the request is refused, if they wish to prevent the transaction going ahead after that date. The moratorium period may be extended, on application by the authorities, by up to 31 days at a time, to a maximum of 186 further days in total. In cases where a defence request is refused, the law enforcement agency refusing the request should be consulted to establish what information can be provided to the customer.

POCA, s 335(1)(b)

6.50 Granting of a defence request by the NCA (referred to as a 'notice' in POCA), or the absence of a refusal of such a request within seven working days following the working day after the disclosure is made, provides the person handling the transaction or carrying out the activity, or the nominated officer of the reporting firm, with a defence against a possible later charge of laundering the proceeds of crime in respect of that transaction or activity if it proceeds.

[28] The Criminal Finances Bill currently before Parliament proposes changes to this regime.

Consent under Terrorism Act

Terrorism Act s21ZA

6.51 A person does not commit an offence under the Terrorism Act where, before becoming involved in a transaction or arrangement relating to money or other property which he suspects or believes is terrorist property, a report is made to the NCA and consent sought to proceed with that transaction or arrangement. In such circumstances, it is an offence for an authorised officer to consent to a transaction or arrangement going ahead within the seven working day notice period from the working day following the date of disclosure to the NCA, unless the NCA gives consent. [Where urgent consent is required, use should be made of the process referred to in paragraph 6.41 above.]

Terrorism Act s21ZB

6.52 When a transaction which gives rise to concern is already within an automated clearing or settlement system, where a delay would lead to a breach of a contractual obligation, or where it would breach market settlement or clearing rules, the authorised officer may need to let the transaction proceed and report it later. Where the nominated officer intends to make a report, but delays doing so for such reasons, the Terrorism Act provides a defence from making a report where there is a reasonable excuse for not doing so, so long as the report is made on his own initiative and as soon as it is reasonably practical for the person to make it. However, it should be noted that this defence is untested by case law, and would need to be considered on a case-by-case basis.

6.53 When consent is needed to undertake a future transaction or activity, or to enter into an arrangement, the disclosure should be sent electronically (ensuring that the tick box for a consent request is marked) or, if secure electronic methods are not available, faxed to the NCA UKFIU Consent Desk immediately the suspicion is identified. Consent requests should not be sent by post due to the timings involved, and additional postal copies are not required following submission by electronic means or fax. Further information is available on the NCA website www.nationalcrimeagency.gov.uk. The Consent Desk will carry out the necessary internal enquiries, and will contact the appropriate law enforcement agency, where necessary, for a consent recommendation. Once the NCA's decision has been reached, the disclosing firm will be informed of the decision by telephone, and be given a consent number, which should be recorded. A formal consent letter will follow.

Terrorism Act s21ZA(2)

6.54 In the event that the NCA does not refuse consent within seven working days following the working day after the disclosure is made, the firm may proceed with the transaction or arrangement, subject to normal commercial considerations. In cases where consent is refused, the law enforcement agency refusing consent should be consulted to establish what information can be provided to the customer.

Terrorism Act S21ZA(1)-(3)

6.55 Consent from the NCA (referred to as a 'notice' in the Terrorism Act), or the absence of a refusal of consent within seven working days following the working day after the disclosure is made, provides the person handling the transaction or arrangement, or the nominated officer of the reporting firm, with a defence against a possible later

charge under the Terrorism Act in respect of that transaction or arrangement if it proceeds.

General

6.56 The consent provisions can only apply where there is prior notice to the NCA of the transaction or activity; the NCA cannot provide consent after the transaction or activity has occurred. The receipt of a SAR after the transaction or activity has taken place will be dealt with as an ordinary standard SAR, and in the absence of any instruction to the contrary, a firm will be free to operate the customer's account under normal commercial considerations until such time as the LEA determines otherwise through its investigation.

6.57 Where there is a need to take urgent action in respect of an account, and the seven working day consent notice period applies, the NCA will endeavour to provide a response in the shortest timeframe, taking into consideration the circumstances of the particular case. Where possible, this will be sooner than the seven working day time limit. If the customer makes strong demands for the transaction/activity to proceed, the NCA will put the firm in touch with the investigating law enforcement agency for guidance, in order to prevent the customer being alerted to the fact of suspicion and that a disclosure has been made. In these circumstances, each case will be dealt with on its merits.

6.58 In order to provide a defence against future prosecution for failing to report, the reasons for any conscious decision not to report should be documented, or recorded electronically. An appropriate report should be made as soon as is practicable after the event, including full details of the transaction, the circumstances precluding advance notice, and to where any money or assets were transferred.

6.59 The consent regime as it currently operates in the UK is a difficult one for financial practitioners to work with, and continues to be a matter of discussion between the industry and the authorities. There are operational challenges and legal uncertainties concerning what can realistically constitute a 'pre-event' transaction. There are customer service implications - the potentially litigious consequences of declining a customer's instructions, the inability to give an explanation because of the risk of tipping-off and the problematic requirement referred to in 6.73 for (in particular, large) deposit-taking institutions to seek consent for all post-disclosure transactions over £250.

Tipping off, and prejudicing an investigation

POCA s 333A (1), (3)
Terrorism Act, s 21D

6.60 POCA and the Terrorism Act each contains two separate offences of tipping off and prejudicing an investigation. The first offence relates to disclosing that an internal or external report has been made; the second relates to disclosing that an investigation is being contemplated or is being carried out. These offences are similar and overlapping, but there are also significant differences between them. It is important for those working in the regulated sector to be aware of the conditions precedent for each offence. Each offence relates to situations where the

information on which the disclosure was based came to the person making the disclosure in the course of a business in the regulated sector. There are a number of permitted disclosures that do not give rise to these offences (see paragraphs 6.63 to 6.66).

POCA ss 333A (1), 333D(3) Terrorism Act, ss 21D(1), 21G(3)

6.61 Once an internal or external suspicion report has been made, it is a criminal offence for anyone to disclose information about that report which is likely to prejudice an investigation that might be conducted following that disclosure. An offence is not committed if the person does not know or suspect that the disclosure is likely to prejudice such an investigation, or if the disclosure is a permitted disclosure under POCA or the Terrorism Act. Reasonable enquiries of a customer, conducted in a tactful manner, regarding the background to a transaction or activity that is inconsistent with the normal pattern of activity is prudent practice, forms an integral part of CDD measures, and should not give rise to the tipping off offence.

POCA, ss 333A(3), 333D(4) Terrorism Act, ss 21D(3), 21G(4)

6.62 Where a money laundering investigation is being contemplated, or being carried out, it is a criminal offence for anyone to disclose this fact if that disclosure is likely to prejudice that investigation. An offence is not committed if the person does not know or suspect that the disclosure is likely to prejudice such an investigation, or if the disclosure is a permitted disclosure under POCA or the Terrorism Act

Permitted disclosures

POCA s 333D(1) Terrorism Act, s 21G(1)

6.63 An offence is not committed if the disclosure is made to the FCA (or other relevant supervisor) for the purpose of:

- the detection, investigation or prosecution of a criminal offence (whether in the UK or elsewhere);
- an investigation under POCA; or
- the enforcement of any order of a court under POCA.

POCA, s 333B(1) Terrorism Act, Ss 21A, 21E(1)

6.64 An employee, officer or partner of a firm does not commit an offence under POCA, s333A, or the Terrorism Act, s 21A, if the disclosure is to an employee, officer or partner of the same firm.

POCA, s 333B(2) Terrorism Act, s 21E(2)

6.65 A person does not commit an offence if the firm making the disclosure and the firm to which it is made belong to the same group (as defined in directive 2002/87/EC), and:

- the disclosure is to a credit institution or a financial institution: and
- the firm to which the disclosure is made is situated in an EEA State, or a country imposing equivalent money laundering requirements.

POCA s 333C Terrorism Act, s 21F

6.66 A firm does not commit an offence under POCA, s333A or the Terrorism Act s21D, if the disclosure is from one credit institution to another, or from one financial institution to another, and:

- the disclosure relates to
  - a customer or former customer of the firm making the disclosure and of the firm to which the disclosure is made; or
  - a transaction involving them both; or

- the provision of a service involving them both.

- the disclosure is for the purpose only of preventing an offence under Part 7 of POCA or under Part III of the Terrorism Act;
- the firm to which the disclosure is made is situated in an EEA State or in a country imposing equivalent money laundering requirements; and
- the firm making the disclosure and the one to which it is made are subject to equivalent duties of protection of personal data (within the meaning of the Data Protection Act 1998).

POCA, ss 335, 336 Terrorism Act, ss21ZA, ZB

6.67 The fact that a transaction is notified to the NCA before the event, and the NCA does not refuse consent within seven working days following the day after the authorized disclosure is made, or a restraint order is not obtained within the 31 day (or extended) moratorium period, does not alter the position so far as 'tipping off' is concerned.

6.68 This means that a firm:

- cannot, at the time, tell a customer that a transaction is being delayed because a report is awaiting consent from the NCA;
- cannot later – unless law enforcement/the NCA agrees, or a court order is obtained permitting disclosure – tell a customer that a transaction or activity was delayed because a report had been made under POCA or the Terrorism Act; and
- cannot tell the customer that law enforcement is conducting an investigation.

6.69 The judgment in K v Natwest [2006] EWCA Civ 1039 confirmed the application of these provisions. The judgment in this case also dealt with the issue of suspicion stating that the "The existence of suspicion is a subjective fact. There is no legal requirement that there should be reasonable grounds for the suspicion. The relevant bank employee either suspects or he does not. If he does suspect, he must (either himself or through the Bank's nominated officer) inform the authorities." It was further observed that the "truth is that Parliament has struck a precise and workable balance of conflicting interests in the 2002 Act". The Court appears to have approved of the 7 and 31 day scheme and said that in relation to the limited interference with private rights that this scheme entails "many people would think that a reasonable balance has been struck". A full copy of the judgment is at http://www.bailii.org/ew/cases/EWCA/Civ/2006/1039.html. The court's view in this case was upheld in Shah and another v HSBC Private Bank Ltd [2012] EWHC 1283 (QB). This judgment is at http://www.bailii.org/ew/cases/EWHC/QB/2012/1283.html.

6.70 If a firm receives a complaint in these circumstances, it may be unable to provide a satisfactory explanation to the customer, who may then bring a complaint to the Financial Ombudsman Service (FOS). The FOS has a secure process in place as well as specialist AML trained teams who only deal with these types of complaints. It is important that these complaints are identified early so they can reach these teams and be progressed quickly. The dedicated email address for firms to send any sensitive information is: Legal_6732@financial-ombudsman.org.uk.

6.71 The NCA has confirmed that, in such cases, a firm may tell the FOS's legal department (via the email in 6.70) about a report to the NCA and the outcome, on the basis that the FOS will keep the information confidential (which they must do, to avoid any 'tipping off'). A firm may, however, wish to take legal advice about what information it should pass on. The FOS's legal department will then ensure that the case is handled appropriately in these difficult circumstances – liaising as necessary with the NCA. FOS's communications with the customer will still be in the name of a case handler/ ombudsman, so that the customer is not alerted.

Transactions following a disclosure

6.72 Firms must remain vigilant for any additional transactions by, or instructions from, any customer or account in respect of which a disclosure has been made, and should submit further disclosures, and consent applications, to the NCA, as appropriate, if the suspicion remains.

POCA s 339A

6.73 In the case of deposit-taking institutions alone, following the reporting of a suspicion, any subsequent transactions (including 'lifestyle' payments) involving the customer or account which was the subject of the original report may only proceed if it meets the 'threshold' requirement of £3,000 or less; where the proposed transaction exceeds £3,000, permission to vary the 'threshold' payment is required from the NCA before it may proceed.

POCA s339A

6.74 If regular transactions are over this £3,000 threshold, the deposit taker can apply to the NCA for a Threshold Variation, and seek permission to impose a higher threshold on the account for regular payments. When seeking such a variation, the NCA requires the deposit taker to specify what 'lifestyle' payments are to be paid, which named account they are coming from and going to, and to specify the amount for each transaction.

POCA, ss 337 (1), 338(4)
Terrorism Act s 21B

6.75 The disclosure provisions within POCA and the Terrorism Act protect persons making SARs from any potential breaches of confidentiality, whether imposed under contract, statute (for example, the Data Protection Act), or common law. These provisions apply to those inside and outside the regulated sector, and include reports that are made voluntarily, in addition to reports made in order to fulfil reporting obligations. The NCA has established a SARs Confidentiality Hotline (0800 234 6657) to report breaches from reporters and end-users alike.

6.76 The NCA's consent following a disclosure is given to the reporting institution solely in relation to the money laundering offences. Consent provides the staff involved with a defence against a charge of committing a money laundering offence under ss 327-329 of POCA or a terrorist finance offence under ss 15-18 of the Terrorism Act. It is not intended to override normal commercial judgement, and a firm is not committed to continuing the relationship with the customer if such action would place the reporting institution at commercial risk.

6.77 Whether to terminate a relationship is essentially a commercial decision, and firms must be free to make such judgements. However, in the circumstances envisaged here a firm should consider liaising

with the law enforcement investigating officer to consider whether it is likely that termination would alert the customer or prejudice an investigation in any other way. If there is continuing suspicion about the customer or the transaction or activities, and there are funds which need to be returned to the customer at the end of the relationship, firms should ask the NCA for consent to repatriate the funds.

6.78 Where the firm knows that the funds in an account derive from criminal activity, or that they arise from fraudulent instructions, the account must be frozen. Where it is believed that the account holder may be involved in the fraudulent activity that is being reported, then the account may need to be frozen, but the need to avoid tipping off would have to be considered.

6.79 When an enquiry is under investigation, the investigating officer may contact the nominated officer to ensure that he has all the relevant information which supports the original disclosure. This contact may also include seeking supplementary information or documentation from the reporting firm and from other sources by way of a court order. The investigating officer will therefore work closely with the nominated officer who will usually receive direct feedback on the stage reached in the investigation. There may, however, be cases when the nominated officer cannot be informed of the state of the investigation, either because of the confidential nature of the enquiry, or because it is sub judice.

6.80 Where the firm does not wish to make the payment requested by a customer, it should notify the NCA of this fact and request them to identify any information that they are prepared to allow the firm to disclose to the court and to the customer in any proceedings brought by the customer to enforce payment. The NCA should be reminded that:

- the court may ask him to appear before it to justify his position if he refuses to consent to adequate disclosure; and
- the refusal to allow adequate disclosure is likely to make it apparent to the customer that the firm's reasons for refusing payment are due to a law enforcement investigation.

6.81 If the investigating officer is able to consent to the disclosure of adequate information to permit the firm to defend itself against any proceedings brought by the customer, that information may be shown to the court and to the customer without a tipping off offence being committed. In the event that the firm and the investigating officer cannot reach agreement on the information to be disclosed, an application can be made to the court for directions and/or an interim declaration.

6.82 In any proceedings that might be brought by the customer, the firm may only disclose to the court and the other side such information as has been consented to by the investigating officer or the court.

Constructive trusts

6.83 The duty to report suspicious activity and to avoid tipping off could, in certain circumstances, lead to a potential conflict between the reporting firm's responsibilities under the criminal law and its obligations under the civil law, as a constructive trustee, to a victim of a fraud or other crimes.

6.84 A firm's liability as a constructive trustee under English law can arise when it either knows that the funds held by the firm do not belong to its customer, or is on notice that such funds may not belong to its customer. The firm will then take on the obligation of a constructive trustee for the rightful owner of the funds. If the firm pays the money away other than to the rightful owner, and it is deemed to have acted dishonestly in doing so, it may be held liable for knowingly assisting a breach of trust.

6.85 Having a suspicion that it considers necessary to report under the money laundering or terrorist financing legislation may, in certain circumstances, indicate that the firm knows that the funds do not belong to its customer, or is on notice that they may not belong to its customer. However, such suspicion may not itself be enough to cause a firm to become a constructive trustee. Case law suggests that a constructive trust will only arise when there is some evidence that the funds belong to someone other than the customer.

6.86 If, when making a suspicious activity report, a firm knows that the funds which are the subject of the report do not belong to its customer, or has doubts that they do, this fact, and details of the firm's proposed course of action, should form part of the report that is forwarded to the NCA.

6.87 If the customer wishes subsequently to withdraw or transfer the funds, the firm should, in the first instance, contact the NCA for consent. Consent from the NCA will, however, not necessarily protect the firm from the risk of committing a breach of constructive trust by transferring funds. In situations where the assistance of the court is necessary, it is open to a firm to apply to the court for directions as to whether the customer's request should be met. However, the powers of the court are discretionary, and should only be used in cases of real need. That said, it is unlikely that a firm acting upon the direction of a court would later be held to have acted dishonestly such as to incur liability for breach of constructive trust.

6.88 Although each case must be considered on its facts, the effective use of customer information, and the identification of appropriate underlying beneficial owners, can help firms to guard against a potential constructive trust suit arising out of fraudulent misuse or misappropriation of funds.

6.89 It should be noted that constructive trust is not a concept recognised in Scots law.

Data Protection - Subject Access Requests, where a suspicion report has been made[29]

6.90 Occasionally, a Subject Access Request under the Data Protection Act will include within its scope one or more money laundering/terrorist financing reports which have been submitted in relation to that customer. Although it might be instinctively assumed that to avoid tipping off there can be no question of ever including this information when responding to the customer, an automatic assumption to that effect must not be made, even though in practice it will only rarely be decided that it is appropriate to include it. However, all such requests must be carefully considered on their merits in line with the principles below.

6.91 The following guidance is drawn from guidance issued by HM Treasury in April 2002. This guidance – The UK's Anti-Money Laundering Legislation and the Data Protection Act 1998 – Guidance notes for the financial sector - is available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/271862/money_laundering_1_.pdf.

Data Protection Act, s 7

6.92 On making a request in writing (a Subject Access Request) to a data controller (i.e. any organisation that holds personal data), an individual is normally entitled to:

- be informed whether the data controller is processing (which includes merely holding) his personal data; and if so
- be given a description of that data, the purposes for which they are being processed and to whom they are or may be disclosed; and
- have communicated to him in an intelligible form all the information that constitutes his personal data and any information available to the data controller as to the source of that data.

Data Protection Act, s 29

6.93 Section 29 of the Data Protection Act provides that personal data are exempt from disclosure under section 7 of the Act in any case where the application of that provision would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. However, even when relying on an exemption, data controllers (i.e., firms) should provide as much information as they can in response to a Subject Access Request.

6.94 Where a firm withholds a piece of information in reliance on the section 29 exemption, it is not obliged to tell the individual that any information has been withheld. The information in question can simply be omitted and no reference made to it when responding to the individual who has made the request.

6.95 To establish whether disclosure would be likely to prejudice an investigation or a potential investigation, firms should approach the NCA for guidance; the NCA will usually discuss this with past or present investigating agencies/officers. This may also involve cases that are closed, but where related investigations may still be continuing.

[29] *Note: This section has been updated and is awaiting formal HMT approval - until such time the update is available under the Revisions tab at https://www.jmlsg.org.uk/revisions/.*

6.96 Each Subject Access Request must be considered on its own merits in determining whether, in a particular case, the disclosure of a suspicion report is likely to prejudice an investigation and, consequently, constitute a tipping-off offence. In determining whether the section 29 exemption applies, it is legitimate to take account of the fact that although the disclosure does not, in itself, provide clear evidence of criminal conduct when viewed in isolation, it might ultimately form part of a larger jigsaw of evidence in relation to a particular crime. It is also legitimate to take account generally of the confidential nature of suspicious activity reports when considering whether or not the exemption under section 29 might apply.

6.97 In cases where the fact that a disclosure had been made had previously been reported in legal proceedings, or in a previous investigation, and the full contents of such a disclosure had been revealed, then it is less likely that the exemption under section 29 would apply. However, caution should be exercised when considering disclosures that have been made in legal proceedings for the purposes of the section 29 exemption, as often the disclosure will have been limited strictly to matters relevant to those proceedings, and other information contained in the original report may not have been revealed.

6.98 To guard against a tipping-off offence, nominated officers should ensure that no information relating to SARs is released to any person without the nominated officer's authorisation. Further consideration may need to be given to suspicion reports received internally that have not been submitted to the NCA. A record should be kept of the steps that have been taken in determining whether disclosure of a report would involve tipping off and/or the availability of the section 29 exemption.

Data Protection Act s 7(8)

6.99 Firms should bear in mind that there is a statutory deadline for responding to Subject Access Requests of 40 days from their receipt by the firm. The timing of enquiries to the NCA, or any other party, to obtain further information, or for guidance on whether disclosure would be likely to prejudice an investigation, should be made with this deadline in mind.

CHAPTER 7

STAFF AWARENESS, TRAINING AND ALERTNESS

- **Relevant law/regulation**
  - Regulation 21, 24
  - POCA ss 327-329, 330 (6),(7), 333, 334(2)
  - Terrorism Act ss 18, 21A
  - SYSC 6.3.7 (1) G
  - TC, Chapter 1
  - Financial sanctions legislation
- **Core obligations**
  - Relevant employees should be
    - made aware of the risks of money laundering, terrorist financing and proliferation financing, the relevant legislation, and their obligations under that legislation
    - made aware of the identity and responsibilities of the firm's nominated officer and MLRO
    - trained in the firm's procedures and in how to recognise and deal with potential money laundering, terrorist financing or proliferation financing transactions or activity
  - Staff training should be given at regular intervals, and details recorded
  - MLRO is responsible for oversight of the firm's compliance with its requirements in respect of staff training
  - The relevant director or senior manager has overall responsibility for the establishment and maintenance of effective training arrangements
- **Actions required, to be kept under regular review**
  - Provide appropriate training to make relevant employees aware of money laundering, terrorist financing and proliferation financing issues, including how these crimes operate and how they might take place through the firm
  - Ensure that relevant employees are provided with information on, and understand, the legal position of the firm and of individual members of staff, and of changes to these legal positions
  - Consider providing relevant employees with case studies and examples related to the firm's business
  - Train relevant employees in how to operate a risk-based approach to AML/CTF

Why focus on staff awareness and training?

7.1 One of the most important controls over the prevention and detection of money laundering is to have staff who are alert to the risks of money laundering/terrorist financing/proliferation financing and well trained in the identification of unusual activities or transactions which may prove to be suspicious.

7.2 The effective application of even the best designed control systems can be quickly compromised if the staff applying the systems are not adequately trained. The content and effectiveness of such training will therefore be important to the success of the firm's AML/CTF strategy.

7.3 It is essential that firms implement a clear and well-articulated policy to ensure that relevant employees are aware of their obligations in respect of the prevention of money laundering, terrorist financing and proliferation financing and for training them in the identification and

reporting of anything that gives grounds for suspicion. This is especially important for staff who directly handle customer transactions or instructions. Temporary and contract staff carrying out such functions should also be covered by these training programmes.

POCA ss 327-329, 334 (2)
Terrorism Act ss 18, 21A

7.4 Under POCA and the Terrorism Act, individual members of staff face criminal penalties if they are involved in money laundering or terrorist financing, or if they do not report their knowledge or suspicion of money laundering or terrorist financing where there are reasonable grounds for their knowing or suspecting such activity. It is important, therefore, that staff are made aware of these obligations, and are given training in how to discharge them.

General legal and regulatory obligations

SYSC 3.1.6 R
SYSC 5.1.1 R

7.5 The FCA requires regulated firms to employ personnel with the skills, knowledge and expertise necessary for the discharge of the responsibilities allocated to them.

TC 2.1
SYSC 3.1.9 G
SYSC 5.1.4A G

7.6 Firms carrying out retail activities that are subject to TC are responsible for ensuring that

- its employees are competent;
- its employees remain competent for the work they do;
- its employees are appropriately supervised;
- its employees' competence is regularly reviewed; and
- the level of competence is appropriate to the nature of the business.

Other firms may nevertheless wish to take TC into account in complying with the high-level training and competence requirement in SYSC.

Regulation 21(1)

7.7 Where appropriate with regard to the size and nature of its business, a firm must carry out screening of relevant employees and agents appointed by the firm, both before the appointment is made, and at regular intervals during the course of the appointment.

Regulation 21(2)(a)

7.8 Screening of relevant employees means an assessment of:

- the skills, knowledge and expertise of the individual to carry out their functions effectively; and
- the conduct and integrity of the individual.

Regulation 21(2)(b)

7.9 A relevant employee is one whose work is –

- relevant to the firm's compliance with any requirement in the ML Regulations; or
- otherwise capable of contributing to the
  - identification or mitigation of the risks of ML/TF to which the firm's business is subject; or
  - prevention or detection of ML/TF in relation to the firm's business.

7.10 Where an employee is found to have breached the firm's internal rules, or requirements imposed by the FCA, there may be an obligation on the firm to report such a breach to the FCA, rather than only dealing with the matter internally.

Regulation 24(1)

7.11 The obligations on senior management and the firm in relation to staff awareness and staff training address each requirement separately. The ML Regulations require firms to take appropriate measures to ensure that relevant employees and agents are made aware of the law relating to money laundering, terrorist financing and proliferation financing (and to data protection, insofar as relevant to the implementation of the ML Regulations), and that they are regularly given training in how to recognise and deal with transactions and other activities or situations which may be related to money laundering, terrorist financing and proliferation financing.

Regulation 24(1)(b), (3)(a)

7.12 In determining the nature and extent of such training measures, firms must take account of the nature and size of their businesses, and the nature and extent of the risks of money laundering, terrorist financing and proliferation financing to which their businesses is subject. Records of the training measures taken must be kept.

SYSC 6.3.9 (1) R

SYSC 6.3.7 (1) G

7.13 The FCA specifically requires the MLRO to have responsibility for oversight of the firm's AML systems and controls, which include appropriate training for the firm's employees in relation to money laundering.

POCA, s 330 (6) and (7)

7.14 Where a staff member is found to have had reasonable grounds for knowing or suspecting money laundering, but failed to make a disclosure, he will have a defence under POCA if he does not know or suspect, and has not been provided with AML training by his employer. No such defence is available under the Terrorism Act.

Regulation 24

7.15 A successful defence by a staff member under POCA may leave the firm open to prosecution or regulatory sanction for not having adequate training and awareness arrangements. Firms should therefore not only obtain acknowledgement from the individual that they have received the necessary training, but should also take steps to assess its effectiveness.

Responsibilities of the firm, and its staff

Responsibilities of senior management

Regulation 19, 19A

7.16 Senior management must be aware of their obligations under the ML Regulations to establish appropriate policies, controls and procedures to mitigate and manage effectively the risks of money laundering, terrorist financing and proliferation financing identified in the firm's risk assessment. It is an offence not to have appropriate policies, controls and procedures in place, whether or not money laundering, terrorist financing and proliferation financing has taken place.

Regulation 21(1)(a)

7.17 Where appropriate with regard to the size and nature of its business, a firm must appoint a member of its board of directors (or equivalent management body) or of its senior management as the officer responsible for the firm's compliance with the ML Regulations.

SYSC 6.3.8 R
SYSC 6.3.9 R

7.18 For firms within scope of the Senior Managers Regime, a senior manager must be allocated the prescribed responsibility for the firm's policies and procedures for countering the risk that the firm might be used to further financial crime. An MLRO must be appointed for oversight of the firm's compliance with its requirements in respect of training in relation to money laundering and terrorist financing. Awareness and training arrangements specifically for senior management, the MLRO and the nominated officer should therefore also be considered.

7.19 As noted in paragraph 1.41, the relationship between the MLRO and the SMF manager(s) allocated the prescribed responsibility for the firm's policies and procedures for countering the risk that the firm might be used to further financial crime is one of the keys to an effective AML/CTF regime. It is important that this relationship is clearly defined and documented, so that each knows the extent of his, and the other's, role and day to day responsibilities. It is permitted, but not required, for the relevant SMF manager(s) also to be appointed as MLRO.

Regulation 21(1)(a)

7.20 Where the firm is required to appoint a board member or a member of its senior management as the officer responsible for the firm's compliance with the ML Regulations, it is important that this individual, the MLRO and the SMF Manager allocated the prescribed responsibility for the firm's policies and procedures are all clear as to the responsibilities of each. Firms should ensure, in consultation with their normal regulatory contact, that the FCA understands how particular responsibilities in this area are allocated or shared.

7.21 Firms should take reasonable steps to ensure that relevant employees are aware of:

- their responsibilities under the firm's arrangements for the prevention of money laundering and terrorist financing, including those for obtaining sufficient evidence of identity, recognising and reporting knowledge or suspicion of money laundering or terrorist financing;
- the identity and responsibilities of the nominated officer and the MLRO; and
- the potential effect on the firm, on its employees personally and on its clients, of any breach of that law.

7.22 The firm's approach to training should be built around ensuring that the content and frequency of training reflects the risk assessment of the products and services of the firm and the specific role of the individual.

Responsibilities of staff

7.23 Staff should be made aware of their personal responsibilities and those of the firm at the start of their employment. These responsibilities

should be documented in such a way as to enable staff to refer to them as and when appropriate throughout their employment. In addition, selected or relevant employees should be given regular appropriate training in order to be aware of:

- the criminal law relating to money laundering and terrorist financing;
- the ML Regulations;
- the FCA Rules;
- industry guidance;
- the risks money laundering and terrorist financing pose to the business;
- the vulnerabilities of the firm's products and services; and
- the firm's policies and procedures in relation to the prevention of money laundering and terrorist financing.

7.24 Where staff move between jobs, or change responsibilities, their training needs may change. Ongoing training should be given at appropriate intervals to all relevant employees.

Legal obligations on staff

POCA, ss327 – 329, 330-332
Terrorism Act ss18, 21A

7.25 There are several sets of offences under POCA and the Terrorism Act which directly affect staff – the various offences of money laundering or terrorist financing, failure to report possible money laundering or terrorist financing, tipping off, and prejudicing an investigation.

POCA, ss327 – 329
Terrorism Act s18

7.26 The offences of involvement in money laundering or terrorist financing apply to all staff, whether or not the firm is in the regulated sector. This would include staff of general insurance firms and mortgage intermediaries. The offences have no particular application to those engaged in specific customer-related activities – that is, they also apply to back office staff and contractors.

POCA ss330-332
Terrorism Act s21A

7.27 The offence under POCA and the Terrorism Act of failing to report applies to staff in the regulated sector, and to all nominated officers, whether in the regulated sector or not. Although general insurance firms and mortgage intermediaries are not in the regulated sector, if they have opted to appoint a nominated officer, the obligations on nominated officers apply to these appointees.

POCA s333

7.28 Once a report has been made to the firm's nominated officer, it is an offence to make any further disclosure that is likely to prejudice an investigation.

Training in the firm's procedures

7.29 The firm should train staff, in particular, on how its products and services may be used as a vehicle for money laundering, terrorist financing and proliferation financing, and in the firm's procedures for managing this risk. They will also need information on how the firm may itself be at risk of prosecution if it processes transactions without the consent of the NCA where a SAR has been made.

7.30 Relevant employees should be trained in what they need to know in order to carry out their particular role. Staff involved in customer acceptance, in customer servicing, or in settlement functions will need different training, tailored to their particular function. This may involve making them aware of the importance of the "know your customer" requirements for money laundering prevention purposes, and of the respective importance of customer ID procedures, obtaining additional information and monitoring customer activity. The awareness raising and training in this respect should cover the need to verify the identity of the customer, and circumstances when it should be necessary to obtain appropriate additional customer information in the context of the nature of the transaction or business relationship concerned.

7.31 Relevant employees should also be made aware of the particular circumstances of customers who present a higher risk of money laundering, terrorist financing, proliferation financing, or who are financially excluded, and how best to identify these. Training should include how identity should be verified in such cases, what additional steps should be taken, and/or what local checks can be made.

Staff alertness to specific situations

7.32 Sufficient training will need to be given to all relevant employees to enable them to recognise when a transaction is unusual or suspicious, or when they should have reasonable grounds to know or suspect that money laundering, terrorist financing or proliferation financing is taking place.

7.33 The set of circumstances giving rise to an unusual transaction or arrangement, and which may provide reasonable grounds for concluding that it is suspicious (see paragraph 6.11), will depend on the customer and the product or service in question. Illustrations of the type of situation that may be unusual, and which in certain circumstances might give rise to reasonable grounds for suspicion, are:

- transactions which have no apparent purpose, or which make no obvious economic sense (including where a person makes a loss), or which involve apparently unnecessary complexity;
- the use of non-resident accounts, companies or structures in circumstances where the customer's needs do not appear to support such economic requirements;
- where the transaction being requested by the customer, or the size or pattern of transactions, is, without reasonable explanation, out of the ordinary range of services normally requested or is inconsistent with the experience of the firm in relation to the particular customer;
- dealing with customers not normally expected in that part of the business;
- transfers to and from high-risk jurisdictions, without reasonable explanation, which are not consistent with the customer's declared foreign business dealings or interests;

- where a series of transactions are structured just below a regulatory threshold;
- where a customer who has entered into a business relationship with the firm uses the relationship for a single transaction or for only a very short period of time;
- unnecessary routing of funds through third party accounts;
- unusual investment transactions without an apparently discernible profitable motive.

7.34 Issues around the customer identification process that may raise concerns include such matters as the following:

- Has the customer refused, or appeared particularly reluctant, to provide the information requested without reasonable explanation?
- Do you understand the legal and corporate structure of the client entity, and its ownership and control, and does the structure appear to make sense in view of the purpose of the transaction/business relationship?
- Is the staff member aware of any inconsistencies between the information provided and what would be expected, given the location of the customer?
- Is the area of residence given consistent with other profile details, such as employment?
- Does an address appear vague or unusual – e.g., an accommodation agency, a professional 'registered office' or a trading address?
- Does it make sense for the customer to be opening the account or relationship in the jurisdiction that he is asking for?
- Is the information that the customer has provided consistent with the banking or other services or facilities that he is seeking?
- Does the supporting documentation add validity to the other information provided by the customer?
- Does the customer have other banking or financial relationships with the firm, and does the collected information on all these relationships appear consistent?
- Does the client want to conclude arrangements unusually urgently, against a promise to provide information at a later stage, which is not satisfactorily explained?
- Has the customer suggested changes to a proposed arrangement in order to avoid providing certain information?

7.35 Staff should also be on the lookout for such things as:

- sudden, substantial increases in cash deposits or levels of investment, without adequate explanation;
- transactions made through other banks or financial firms;
- regular large, or unexplained, transfers to and from countries known for money laundering, terrorism, corruption or drug trafficking;
- large numbers of electronic transfers into and out of the account;
- significant/unusual/inconsistent deposits by third parties; and
- reactivation of dormant account(s).

7.36 Staff awareness and training programmes may also include the nature of terrorism funding and terrorist activity, in order that staff are alert to customer transactions or activities that might be terrorist-related.

7.37 Examples of activity that might suggest to staff, when assessed in the context of the overall risk presented by the customer, that there could be potential terrorist activity include:

- round sum deposits, followed by like-amount wire transfers;
- frequent international ATM activity;
- no known source of income;
- use of wire transfers and the internet to move funds to and from high-risk countries and geographic locations;
- frequent address changes;
- purchases of military items or technology; and
- media reports on suspected, arrested terrorists or groups.

7.38 It is important that staff are appropriately made aware of changing behaviour and practices amongst money launderers and those financing terrorism. As well as their regular series of publications on the typologies of financial crime, FATF's Guidance for Financial Institutions in Detecting Terrorist Financing issued in April 2002 contains an in-depth analysis of the methods used in the financing of terrorism and the types of financial activities constituting potential indicators of such activities. These documents are available at www.fatf-gafi.org.

7.39 Illustrations, based on real cases, of how individuals and organisations might raise funds and use financial sector products and services for money laundering or to finance terrorism, are also available on the FATF website at www.fatf-gafi.org.

7.40 The NCA publishes a range of material at www.nationalcrimeagency.gov.uk, such as threat assessments and risk profiles, of which firms may wish to make their staff aware. The information on this website could usefully be incorporated into firms' training materials.

Staff based outside the UK

7.41 Where activities relating to UK business operations are undertaken by processing staff outside the UK, those staff must be made aware of and trained to follow the AML/CTF policies and procedures applicable to the UK operations. It is important that any local training and awareness obligations are also met, where relevant.

Training methods and assessment

7.42 There is no single solution when determining how to deliver training; a mix of training techniques may be appropriate. On-line learning systems can often provide an adequate solution for many employees, but there will be classes of employees for whom such an approach is not suitable. Focused classroom training for higher risk or minority areas

can be more effective. Relevant videos always stimulate interest, but continually re-showing the same video may produce diminishing returns.

7.43 Procedures manuals, whether paper or intranet based, are useful in raising staff awareness and in supplementing more dedicated forms of training, but their main purpose is to provide ongoing reference and they are not generally written as training material.

7.44 Ongoing training should be given at appropriate intervals to all relevant employees. Particularly in larger firms, this may take the form of a rolling programme.

Regulation 24(1)(b)

7.45 Whatever the approach to training, it is vital to establish comprehensive records (see paragraph 8.24) to monitor who has been trained, when they received the training, the nature of the training given and its effectiveness.

CHAPTER 8

RECORD KEEPING

➢ **Relevant law/regulation** ▪ Data Protection Act 2018 ▪ Regulations 18, 19 and 39-41 ▪ SYSC Chapter 3
➢ **Core obligations** ▪ Firms must retain for five years after the end of the customer relationship or five years after the completion of an occasional transaction: • copies of, or references to, the evidence they obtained of a customer's identity • details of customer transactions ▪ Firms should retain: • details of actions taken in respect of internal and external suspicion reports • details of information considered by the nominated officer in respect of an internal report where no external report is made ▪ Firms must delete any personal data relating to CDD and client transactions in accordance with Regulation 40
➢ **Actions required, to be kept under regular review** ▪ Firms should maintain appropriate systems for retaining records ▪ Firms should maintain appropriate systems for making records available when required, within the specified timescales

General legal and regulatory requirements

Regulation 19(1)(a)

8.1 This chapter provides guidance on appropriate record keeping procedures that will meet a firm's obligations in respect of the prevention of money laundering and terrorist financing. There are general obligations on firms to maintain appropriate records and controls more widely in relation to their business; this guidance is not intended to replace or interpret such wider obligations.

8.2 Record keeping is an essential component of the audit trail that the ML Regulations and FCA Rules seek to establish in order to assist in any financial investigation and to ensure that criminal funds are kept out of the financial system, or if not, that they may be detected and confiscated by the authorities.

Regulation 18(4), 19(1)(b), 39(2)(b)

8.3 As well as legislating for record keeping in relation to customer identification, and transactions with customers, there are obligations on firms to document their risk assessment, and their policies, controls and procedures. See paragraphs 1.54 and 2.3. A firm is also required to have written arrangements with any third party on which they rely to apply customer due diligence measures.

Regulation 40
SYSC 3.2.20 R
SYSC 6.3.1 R

8.4 Firms must retain records concerning customer identification and transactions as evidence of the work they have undertaken in complying with their legal and regulatory obligations, as well as for use as evidence in any investigation conducted by law enforcement. FCA-regulated

firms must take reasonable care to make and keep adequate records appropriate to the scale, nature and complexity of their businesses.

Regulation 39

8.5 Where a firm has an appointed representative, it must ensure that the representative complies with the record keeping obligations under the ML Regulations. This principle would also apply where the record keeping is delegated in any way to a third party (such as to an administrator or an introducer).

What records have to be kept?

8.6 The precise nature of the records required is not specified in the legal and regulatory regime. The objective is to ensure that a firm meets its obligations and that, in so far as is practicable, in any subsequent investigation the firm can provide the authorities with its section of the audit trail.

8.7 The firm's records should cover:

- Customer information
- Transactions
- Internal and external suspicion reports
- MLRO annual (and other) reports
- Information not acted upon
- Training and compliance monitoring
- Information about the effectiveness of training

Customer information

Regulation 40(2)

8.8 In relation to the evidence of a customer's identity, firms must keep a copy of any documents or information it obtained to satisfy the CDD measures required under the ML Regulations. Where a firm has received a confirmation of identity certificate, this certificate will in practice be the evidence of identity that must be kept. Some documents which may be used for evidence of identification are more sensitive than others (for example, Armed Forces Cards and Firearms certificates), and firms should deal with such evidence with care.

8.9 When a firm has concluded that it should treat a client as financially excluded for the purposes of customer identification, it should keep a record of the reasons for doing so.

8.10 A firm may often hold additional information in respect of a customer obtained for the purposes of enhanced customer due diligence or ongoing monitoring.

8.11 The Home Office current guidance on copying passports is available at http://www.nationalarchives.gov.uk/documents/information-management/reproduction-british-passport.pdf

Regulation 40(3)(b)(ii)

8.12 Records of identification evidence must be kept for a period of five years after the business relationship with the customer has ended, i.e. the closing of the account or accounts.

Regulation 40(5)

8.13 Upon the expiry of the five year period referred to in paragraph 8.12, firms must delete any personal data unless:

- the firm is required to retain records containing personal data by, or under, any enactment, or for the purposes of any court proceedings; or
- the firm has reasonable grounds for believing that records containing the personal data need to be retained for the purpose of legal proceedings; or
- the data subject has given consent to the retention of that data.

Regulation 40(6)

8.14 A firm which is relied on by another firm for the purposes of customer due diligence must keep the records referred to in paragraph 8.8 for five years from the ending of the business relationship with the customer.

8.15 Where documents verifying the identity of a customer are held in one part of a group, they do not need to be held in duplicate form in another. The records do, however, need to be accessible to the nominated officer and the MLRO and to all areas that have contact with the customer, and be available on request, where these areas seek to rely on this evidence, or where they may be called upon by law enforcement to produce them.

8.16 When an introducing branch or subsidiary undertaking ceases to trade or have a business relationship with a customer, as long as the customer's relationship with other group members continues, particular care needs to be taken to retain, or hand over, the appropriate customer records. Similar arrangements need to be made if a company holding relevant records ceases to be part of the group. This will also be an issue if the record keeping has been delegated to a third party.

Transactions

8.17 All transactions carried out on behalf of or with a customer in the course of relevant business must be recorded within the firm's records. Transaction records in support of entries in the accounts, in whatever form they are used, e.g. credit/debit slips, cheques, should be maintained in a form from which a satisfactory audit trail may be compiled where necessary, and which may establish a financial profile of any suspect account or customer.

Regulation 40(3)(a)(b)

8.18 Records of all transactions relating to a customer must be retained for a period of five years from:

- where the records relate to an occasional transaction, the date when the transaction is completed; or
- in other cases, the date the business relationship ended, i.e. the closing of the account or accounts.

Regulation 40(4)

But: a firm is not required to retain records relating to transactions occurring in a business transaction relationship for more than 10 years.

8.19 In the case of managers of investment funds or issuers of electronic money, where there may be no business relationship as defined in the ML Regulations, but the customer may nevertheless carry out further occasional transactions in the future, it is recommended that all records

be kept for five years after the investment has been fully sold or funds disbursed.

Regulation 40(5)

8.20 Upon the expiry of the period referred to in paragraph 8.18, firms must delete any personal data unless:

- the firm is required to retain records containing personal data by, or under, any enactment, or for the purposes of any court proceedings; or
- the firm has reasonable grounds for believing that records containing the personal data need to be retained for the purpose of legal proceedings; or
- the data subject has given consent to the retention of that data.

Internal and external reports

8.21 A firm should make and retain:

- records of actions taken under the internal and external reporting requirements; and
- when the nominated officer has considered information or other material concerning possible money laundering, but has not made a report to the NCA, a record of the other material that was considered.

8.22 In addition, copies of any SARs made to the NCA should be retained.

8.23 Records of all internal and external reports should be retained for at least five years from the date the report was made.

Other

8.24 A firm's records should include:

(a) in relation to training:

- dates AML training was given;
- the nature of the training;
- the names of the staff who received training; and
- the results of the tests undertaken by staff, where appropriate.

(b) in relation to compliance monitoring -

- reports by the MLRO to senior management; and
- records of consideration of those reports and of any action taken as a consequence.

Regulation 21(8),(9)

8.25 A firm must establish and maintain systems which enable it to respond fully and rapidly to enquiries from financial investigators accredited under s3 of POCA, persons acting on behalf of the Scottish Ministers in their capacity as an enforcement authority under the Act or constables, relating to:

- whether it maintains, or has maintained during the previous five years, a business relationship with any person; and

- the nature of that relationship.

Form in which records have to be kept

8.26 Most firms have standard procedures which they keep under review, and will seek to reduce the volume and density of records which have to be stored, whilst still complying with statutory requirements. Retention may therefore be:

- by way of original documents;
- by way of photocopies of original documents;
- on microfiche;
- in scanned form;
- in computerised or electronic form.

8.27 The record retention requirements are the same, regardless of the format in which they are kept, or whether the transaction was undertaken by paper or electronic means.

8.28 Firms involved in mergers, take-overs or internal reorganisations need to ensure that records of identity verification and transactions are readily retrievable for the required periods when rationalising computer systems and physical storage arrangements.

Location

8.29 The ML Regulations do not state where relevant records should be kept, but the overriding objective is for firms to be able to retrieve relevant information without undue delay.

8.30 Where identification records are held outside the UK, it is the responsibility of the UK firm to ensure that the records available do in fact meet UK requirements. No secrecy or data protection legislation should restrict access to the records either by the UK firm freely on request, or by UK law enforcement agencies under court order or relevant mutual assistance procedures. If it is found that such restrictions exist, copies of the underlying records of identity should, wherever possible, be sought and retained within the UK.

8.31 Firms should take account of the scope of AML/CTF legislation in other countries, and should ensure that group records kept in other countries that are needed to comply with UK legislation are retained for the required period.

8.32 There can sometimes be tension between the provisions of the ML Regulations and data protection legislation; the nominated officer and the MLRO must have due regard to both sets of obligations.

8.33 When setting document retention policy, financial sector businesses must weigh the statutory requirements and the needs of the investigating authorities against normal commercial considerations. When original vouchers are used for account entry, and are not returned to the customer or their agent, it is of assistance to the law enforcement agencies if these

original documents are kept to assist in forensic analysis. This can also provide evidence for firms when conducting their own internal investigations. However, this is not a requirement of the AML legislation, and retaining electronic/digital copies may be a more realistic storage method.

Sanctions and penalties

Regulation 86(1)

8.34 Where the record keeping obligations under the ML Regulations are not observed, a firm or person is open to prosecution, including imprisonment for up to two years and/or a fine, or regulatory censure.

GLOSSARY OF TERMS

Term/expression	Meaning
Annex I Financial Institution	An undertaking (other than a credit institution or a consumer credit institution) that carries out one or more of the operations (other than trading on their own account where the undertaking's only customers are group companies) listed on Schedule 2 to the ML Regulations. [ML Regulations 10(2)(a), 54(2)]
Appropriate person	Someone in a position of responsibility, who knows, and is known by, a customer, and may reasonably confirm the customer's identity. It is not possible to give a definitive list of such persons, but the following may assist firms in determining who is appropriate in any particular case: ➢ The Passport Office has published a list of those who may countersign passport applications: see www.direct.gov.uk/en/TravelAndTransport/Passports/Applicationinformation/DG_174151 ➢ Others might include members of a local authority, staff of a higher or further education establishment, or a hostel manager.
Basel Committee	Basel Committee on Banking Supervision.
Beneficial owner(s)	The individual who ultimately owns or controls the customer on whose behalf a transaction or activity is being conducted. Special rules have been made for bodies corporate, partnerships, trusts, entities or arrangements that administer and distribute funds and estates of deceased persons. [ML Regulations 5 and 6]
Controlled function	A function relating to the carrying on of a regulated activity by a firm which is specified under s 59 of FSMA, in FCA's table of controlled functions.
Criminal property	Property which constitutes a person's benefit from criminal conduct or which represents such a benefit (in whole or part and whether directly or indirectly), and the alleged offender knows or suspects that the property constitutes or represents such a benefit. [POCA s 340 (3)]
Criminal conduct	Conduct which constitutes an offence in any part of the United Kingdom, or would constitute an offence in any part of the United Kingdom if it occurred there. [POCA s 340 (2)]
Customer	In relation to an FCA-regulated firm, a customer is a person who is using, or may be contemplating using, any of the services provided by the firm. As noted in paragraph 5.3.3, this is not the definition of customer that applies in SYSC. [FSMA, s 59 (11)]

EU Fourth Money Laundering Directive	The Fourth Money Laundering Directive, adopted in 2015 (2015/849EC), updated European Community legislation in line with the revised FATF 40 Recommendations, published in 2012. It repealed and replaced the Third Directive.
EC Sanctions Regulation	Regulation 2580/2001, on specific restrictive measures directed against certain persons and entities with a view to combating terrorism.
FATF Recommendations	A series of Forty Recommendations on the structural, supervisory and operational procedures that countries should have in place to combat money laundering, issued by the FATF. The Forty Recommendations were originally published in 1990, revised in 1996 and 2004, and last revised in February 2012 (and they are updated regularly). FATF issued a series of Special Recommendations on Terrorist Financing in October 2001 and October 2004, and these were subsumed within the revised Forty Recommendations in February 2012. The FATF Forty Recommendations have been recognised by the International Monetary Fund and the World Bank as the international standards for combating money laundering and terrorist financing.
FCA-regulated firm	A firm holding permission from the FCA under FSMA, Part 4A, to carry on certain of the activities listed in FSMA, Schedule 2.
Government-issued	Issued by a central government department or by a local government authority or body.
Guidance Paper 5	Guidance Paper No 5: Guidance paper on anti-money laundering and combating the financing of terrorism, issued by IAIS in October 2004.
HM Treasury Sanctions Notices and News Releases	Notices issued by HM Treasury advising firms of additions to the UN Consolidated List maintained under Security Council resolution 1390 (2002) and to the list of persons and entities subject to EC Regulation 2580/2001.
Identification	Ascertaining the name of, and other relevant information about, a customer or beneficial owner.
IOSCO Principles paper	IOSCO paper 'Principles on Client Identification and Beneficial Ownership for the Securities Industry', published May 2004.
Mind and management	Those individuals who, individually or collectively, exercise practical control over a non-personal entity.

ML Regulations	The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 [SI 2017/692] (as amended)
Money laundering	An act which: ➢ constitutes an offence under ss 327, 328 or 329 of POCA or ➢ constitutes an attempt, conspiracy or incitement to commit such an offence or ➢ constitutes aiding, abetting, counselling or procuring the commission of such an offence or ➢ would constitute an offence specified above if done in the United Kingdom. [POCA, s 340 (11)] A person also commits an offence of money laundering if he enters into or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property: ➢ by concealment; ➢ by removal from the jurisdiction; ➢ by transfer to nominees; or ➢ in any other way. [Terrorism Act, s 18]
Money service business	An undertaking which by way of business operates a currency exchange office, transmits money (or any representations of monetary value) by any means or which cashes cheques which are made payable to customers. [ML Regulation 3(1)]
Nominated officer	A person in a firm or organisation nominated by the firm or organisation to receive disclosures under Regulation 21(5) and s 330 of POCA from others within the firm or organisation who know or suspect that a person is engaged in money laundering. Similar provisions apply under the Terrorism Act.
Occasional transaction	Any transaction which is not carried out as part of a business relationship. [ML Regulation 3 (1)]
Politically exposed person	An individual who is or has, at any time in the preceding year, been entrusted with prominent public functions, other than as a middle ranking or more junior official. [ML Regulation 35(12)]
Regulated Activities Order	Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (SI 2001/544).
Regulated activity	Activities set out in the Regulated Activities Order, made under s 22 and Schedule 2 of FSMA and not excluded by the Financial Services and Markets Act 2000

	(Exemption) Order 2001 (which exempts certain persons carrying on specific activities from carrying on regulated activities).
Regulated market	A multilateral system operated and/or managed by a market operator, which brings together or facilitates the bringing together of multiple third-party buying and selling interests in financial instruments - in the system and in accordance with its non-discretionary rules - in a way that results in a contract, in respect of the financial instruments admitted to trading under its rules and/or systems, and which is regulated and functions regularly [and in accordance with the provisions of Articles 36-47 of MiFID]. [MiFID Article 4(14)]
Regulated sector	Persons and firms which are subject to the ML Regulations.
Senior management	An officer or employee of a firm in the regulated sector with sufficient knowledge of the firm's money laundering and terrorist financing risk exposure, and of sufficient authority, to take decisions affecting its risk exposure. [ML Regulation19(7)]
Senior manager	An individual, other than a director (or equivalent), who is employed by the firm, and to whom the Board (or equivalent) or a member of the Board, has given responsibility, either alone or jointly with others, for management and supervision.
Terrorism Act	Terrorism Act 2000, as amended by the Anti-terrorism, Crime and Security Act 2001.
Terrorist property	➢ Money or other property which is likely to be used for the purposes of terrorism (including any resources of a proscribed organisation); or ➢ Proceeds of the commission of acts of terrorism; or ➢ Proceeds of acts carried out for the purposes of terrorism "Proceeds of an act" includes a reference to any property which wholly or partly, and directly or indirectly, represents the proceeds of the act (including payments or other rewards in connection with its commission). "Resources" includes any money or other property which is applied or made available, or is to be applied or made available, for use by the organisation. [Terrorism Act, s 14]
Tipping off	A tipping-off offence is committed if a person knows or suspects that a disclosure falling under POCA ss 337 or 338 has been made, and he makes a disclosure which is likely to prejudice any investigation which may be conducted following the disclosure under s 337 or s 338. [POCA, s 333]

Verification	Verifying the identity of a customer, by reference to documents or information obtained from a reliable source which is independent of the customer, or of a beneficial owner through carrying out reasonable measures so that the firm is satisfied that it knows who the beneficial owner is.

Abbreviation	
ACPO	Association of Chief Police Officers
AML	Anti-money laundering
CTF	Combating terrorism financing
DWP	Department of Work and Pensions
ESAs	The European Supervisory Authorities – The European Banking Authority, the European Securities Markets Authority and the European Insurance and Occupational Pensions Authority, working together
FATF	Financial Action Task Force, an intergovernmental body whose purpose is to develop and promote broad AML/CTF standards, both at national and international levels
FCA	Financial Conduct Authority, the UK regulator of the financial services industry
FSMA	Financial Services and Markets Act 2000
HMT	Her Majesty's Treasury
IAIS	International Association of Insurance Supervisors
IOSCO	International Organisation of Securities Commissions
MiFID	The Marketing in Financial Instruments Directive
MLRO	Money Laundering Reporting Officer
NCA	The National Crime Agency, the UK's financial intelligence unit.
POCA	Proceeds of Crime Act 2002
SAR	Suspicious activity report
SMR	The FCA supervisory regime (the Senior Manager Regime) applying to staff holding Senior Management Functions in certain categories of firm
SOCPA	Serious Organised Crime and Police Act 2005
SYSC	FCA Sourcebook: Senior Management Arrangements, Systems and Controls

APPENDIX I

ANTI-MONEY LAUNDERING RESPONSIBILITIES IN THE UK

UK Government	Law Enforcement, other investigating bodies and prosecutors	Regulator	Industry
Home Office • UK primary legislation (Proceeds of Crime Act 2002, Terrorism Act 2000 and Anti-terrorism, Crime and Security Act 2001) • Police strategy and resourcing • Asset recovery strategy • Chairs (jointly with HM Treasury) Money Laundering Advisory Committee (MLAC), a forum for key stakeholders to coordinate the AML regime and review its efficiency and effectiveness **HM Treasury** • Represents UK in EU and FATF • Implements EU Directives, principally through the Money Laundering Regulations • Approves industry guidance under POCA, Terrorism Act and Money Laundering Regulations • Implements and administers the UK's financial sanctions regime, through the Office of Financial Sanctions Implementation	**National Crime Agency** • As UK's financial intelligence unit receives suspicious activity reports (about money laundering and terrorist financing) and sends cleared intelligence to law enforcement agencies for investigation • Assesses organised crime threats • Exercises powers under POCA to recover the proceeds of crime through criminal, civil, or tax recovery processes • Supports law enforcement agencies • Trains financial investigators **Police** • 43 forces in the UK • Investigate crime, including money laundering and terrorism **HM Revenue and Customs** • Investigates money laundering, drug trafficking and certain tax offences • Licenses money service businesses and dealers in high value goods **The Revenue and Customs Prosecutions Office** • Prosecutes money laundering, drug trafficking and certain tax offences investigated by HMRC	**Financial Conduct Authority** • UK's financial regulator • Statutory objectives (under Financial Services and Markets Act 2000) include reduction of financial crime • Approves persons to perform "controlled functions" (including money laundering reporting officer function) • Makes, supervises and enforces, amongst other things, rules on money laundering • Power to prosecute firms under the Money Laundering Regulations (except in Scotland) **Other regulators include** • HM Revenue and Customs • Gambling Commission • 22 professional body supervisors, listed in Schedule 1 of the Money Laundering Regulations	**The Joint Money Laundering Steering Group** • Industry body made up of 14 financial sector trade bodies • Produces guidance on compliance with legal and regulatory requirements and good practice

	Crown Prosecution Service • Prosecutes crime, money laundering and terrorism offences in England and Wales **Procurator Fiscal** • Prosecutes crime, money laundering and terrorism offences in Scotland **Public Prosecution Service of Northern Ireland** • Prosecutes crime, money laundering and terrorism offences in Northern Ireland		

APPENDIX II

SUMMARY OF UK LEGISLATION

Proceeds of Crime Act 2002[30] (as amended)

1. The Proceeds of Crime Act 2002 (POCA) consolidates and extends the existing UK legislation regarding money laundering. The legislation covers all crimes and any dealing in criminal property, with no exceptions and no de minimis. POCA, as amended:

   - empowers the NCA, to conduct an investigation[31] to discover whether a person holds criminal assets and to recover the assets in question.

   - creates five investigative powers for the law enforcement agencies:
     - a production order[32]
     - a search and seizure warrant[33]
     - a disclosure order[34]
     - a customer information order[35]
     - an account monitoring order[36]

   - establishes the following criminal offences:

     - a criminal offence37 to acquire, use, possess, conceal, disguise, convert, transfer or remove criminal property from the jurisdiction, or to enter into or become concerned in an arrangement to facilitate the acquisition, retention, use or control of criminal property by another person

     - a criminal offence38 for persons working in the regulated sector of failing to make a report where they have knowledge or suspicion of money laundering, or reasonable grounds for having knowledge or suspicion, that another person is laundering the proceeds of any criminal conduct, as soon as is reasonably practicable after the information came to their attention in the course of their regulated business activities

       Note: There are no provisions governing materiality or de minimis thresholds for having to report under POCA (although for deposit-taking firms, a transaction under £250 may be made without consent under certain circumstances – see paragraph 6.73).

     - a criminal offence39 for anyone to take any action likely to prejudice an investigation by informing (e.g., tipping off) the person who is the subject of a suspicion report, or anybody else, that a disclosure has been made to a nominated officer or to the NCA, or

[30] 2002 ch 29
[31] section 341(2)
[32] section 345
[33] section 352
[34] section 357
[35] section 363
[36] section 370 – see also Terrorism Act s38A
[37] sections 327 - 329
[38] sections 330 and 331
[39] section 333A

that the police or customs authorities are carrying out or intending to carry out a money laundering investigation.

- a criminal offence[40] of destroying or disposing of documents which are relevant to an investigation.

- a criminal offence[41] by a firm of failing to comply with a requirement imposed on it under a customer information order, or in knowingly or recklessly making a statement in purported compliance with a customer information order that is false or misleading in a material particular.

- sets out maximum penalties:

  - for the offence of money laundering of 14 years' imprisonment and/or an unlimited fine.

    Note: An offence is not committed if a person reports the property involved to the National Crime Agency (NCA) or under approved internal arrangements, either before the prohibited act is carried out, or as soon afterwards as is reasonably practicable.

  - for failing to make a report of suspected money laundering of five years' imprisonment and/or an unlimited fine.

  - for "tipping off" of two years' imprisonment and/or an unlimited fine.

  - for destroying or disposing of relevant documents of five years' imprisonment and/or an unlimited fine.

Terrorism Act 2000[42], and the Anti-terrorism, Crime and Security Act 2001[43]

2. The Terrorism Act establishes a series of offences related to involvement in arrangements for facilitating, raising or using funds for terrorism purposes. The Act:

   - makes it a criminal offence for any person not to report the existence of terrorist property where there are reasonable grounds for knowing or suspecting the existence of terrorist property

   - makes it a criminal offence[44] for anyone to take any action likely to prejudice an investigation by informing (i.e. tipping off) the person who is the subject of a suspicion report, or anybody else, that a disclosure has been made to a nominated officer or to the NCA, or that the police or customs authorities are carrying out or intending to carry out a terrorist financing investigation

   - grants[45] a power to the law enforcement agencies to make an account monitoring order, similar in scope to that introduced under POCA

   - sets out the following penalties:

[40] section 341(2)(b)
[41] section 366
[42] 2000 ch 11
[43] 2001 ch 24
[44] section 39
[45] section 38A and Schedule 6A

- the maximum penalty for failure to report under the circumstances set out above is five years' imprisonment, and/or a fine.

- the maximum penalty for the offence of actual money laundering is 14 years' imprisonment, and/or a fine.

3. The definition of terrorist property, involvement with which is an offence, includes resources of a proscribed organisation. The primary source of information on proscribed organisations, including up-to-date information on aliases, is the Home Office. A list of organisations which have been proscribed under the Terrorism Act can be found at https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2.

4. The Anti-terrorism, Crime and Security Act 2001 gives the authorities power to seize terrorist cash, to freeze terrorist assets and to direct firms in the regulated sector to provide the authorities with specified information on customers and their (terrorism-related) activities. Additionally under the Anti-Terrorism, Crime and Security Act 2001, HM Treasury may issue a freezing order in respect of individuals, entities or organisations outside of the UK where there is reasonable belief that they have taken or are likely to take action which is:

- to the detriment of the UK economy
- a threat to the life or property of one or more nationals or residents of the UK

Counter-terrorism Act 2008, Schedule 7

5. Schedule 7 to the CTA gives power to HM Treasury to issue directions to firms in the financial sector. The kinds of requirement that may be imposed by a direction under these powers relate to:

- customer due diligence;
- ongoing monitoring;
- systematic reporting;
- limiting or ceasing business.

6. The requirements to carry out CDD measures and ongoing monitoring build on the similar obligation under the ML Regulations. The requirements for systematic reporting and limiting or ceasing business are new.

7. The Treasury may give a direction **if one or more** of the following conditions is met in relation to a non-EEA country:

- that the Financial Action Task Force has advised that measures should be taken in relation to the country because of the risk of terrorist financing or money laundering activities being carried on
  (a) in the country,
  (b) by the government of the country, or
  (c) by persons resident or incorporated in the country.
- that the Treasury reasonably believe that there is a risk that terrorist financing or money laundering activities are being carried on

(a) in the country,

(b) by the government of the country, or

(c) by persons resident or incorporated in the country,

and that this poses a significant risk to the national interests of the UK.

- that the Treasury reasonably believe that

(a) the development or production of nuclear, radiological, biological or chemical weapons in the country, or

(b) the doing in the country of anything that facilitates the development or production of any such weapons,

poses a significant risk to the national interests of the UK.

Financial sanctions

8. The Foreign, Commonwealth and Development Office publishes and maintains the UK Sanctions List of designated targets. This list can be found at:

https://www.gov.uk/government/publications/the-uk-sanctions-list

9. It is a criminal offence to make payments, or to allow payments to be made, to targets on the UK Sanctions List. This would include dealing direct with targets, or dealing with targets through intermediaries (such as lawyers or accountants). Firms therefore need to have an appropriate means of monitoring payment instructions to ensure that no payments are made to targets or their agents. In the regulated sector this obligation applies to all firms, and not just to banks.

10. Guidance on compliance with the financial sanctions regime is set out in paragraphs 5.3.54 – 5.3.61.

Money Laundering Regulations 2017[46]

11. The ML Regulations specify arrangements which must be in place within firms within the scope of the Regulations, in order to prevent operations relating to money laundering or terrorist financing.

12. The ML Regulations apply[47], inter alia, to:

- The regulated activities of all financial sector firms, i.e.:
  - banks, building societies and other credit institutions;
  - individuals and firms engaging in regulated investment activities under FSMA;
  - issuers of electronic money;
  - insurance companies undertaking long-term life business, including the life business of Lloyd's of London;
- Bureaux de change, cheque encashment centres and money transmission services (money service businesses);
- Trust and company service providers;

[46] SI 2017/692(as amended)
[47] Regulation 8

- Casinos;
- Dealers in high-value goods (including auctioneers) who accept payment in cash of €10,000 or more (either single or linked transactions);
- Estate agents and letting agents, legal and accountancy services providers, when undertaking relevant business;
- Art market participants;
- Cryptoasset exchange providers;
- Custodian wallet providers.

13. The ML Regulations require firms to appoint a nominated officer to receive internal reports relating to knowledge or suspicion of money laundering.

14. Firms within the scope of the ML Regulations are required to establish and maintain policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified in a risk assessment undertaken by the firm. These policies, controls and procedures cover:

- Risk management practices;
- internal controls;
- customer due diligence;
- reporting and record-keeping;
- monitoring and management of compliance with, and the internal communication of, such policies, controls and procedures.

15. The FCA may[48] institute proceedings (other than in Scotland) for offences under prescribed regulations relating to money laundering. This power is not limited to firms or persons regulated by the FCA. Whether a breach of the ML Regulations has occurred is not dependent on whether money laundering has taken place: firms may be sanctioned for not having adequate AML/CTF systems. Where failure to comply with any of the requirements of the ML Regulations constitutes an offence, the punishment is a maximum of two years' imprisonment, or a fine, or both.

FCA-regulated firms – the FCA Handbook

16. FSMA makes the prevention of financial crime integral to the discharge of the FCA's functions and fulfilment of its objectives. This means that the FCA is concerned that the firms it regulates and their senior management are aware of the risk of their businesses being used in connection with the commission of financial crime, and take appropriate measures to prevent financial crime, facilitate its detection and monitor its incidence.

17. Firms may only engage in a regulated activity[49] in the UK if it is a regulated or exempt person. A person can become a regulated person as a result of: (a) being given a "permission" by the FCA under Part 4A of FSMA (known as a "Part 4A permission"); or (b) by qualifying for authorisation under FSMA itself. As an example of the latter, an EEA firm establishing a branch in, or providing cross-border services into, the UK can qualify for regulation under FSMA Schedule 3 and, as a result,

[48] FSMA, s 402(1)(b)

[49] FSMA s22, Schedule 2, and the Regulated Activities Order. These activities are substantially the same as set out in Regulation [2 (2)(a)].

be given a permission; although such firms are, generally, regulated by their home state regulator, they are regulated by the FCA in connection with the regulated activities carried on in the UK.

18. A firm may only carry on regulated business in accordance with its permission. A firm with a Part 4A permission may apply to the FCA to vary its permission, add or remove regulated activities, to limit these activities (for example, the types of client with or for whom the firm may carry on an activity) or to vary the requirements on the firm itself. Before giving or varying a Part 4A permission, the FCA must ensure that the person/firm will satisfy and continue to satisfy the threshold conditions in relation to all of the regulated activities for which he has or will have permission. If a firm is failing, or is likely to fail, to satisfy the threshold conditions, the FCA may vary or cancel a firm's permission.

19. Threshold condition 5 (Suitability) requires the firm to satisfy the FCA that it is "fit and proper" to have Part 4A permission having regard to all the circumstances, including its connection with other persons, the range and nature of its proposed (or current) regulated activities and the overall need to be satisfied that its affairs are and will continue to be conducted soundly and prudently. Hence, the FCA "will consider whether a firm is ready, willing and organised to comply, on a continuing basis, with the requirements and standards under the regulatory system which apply to the firm, or will apply to the firm, if it is granted Part 4A permission, or a variation of its permission". The FCA will also have regard to all relevant matters, whether arising in the UK or elsewhere. In particular, the FCA will consider whether a firm "has in place systems and controls against money laundering of the sort described in SYSC 6.1.1 R to SYSC 6.3.10 G". (COND 2.5.7G)

20. SYSC requires FCA-regulated firms (subject to some specified exceptions: see paragraph 1.35 above) to have effective systems and controls for countering the risk that a firm might be used to further financial crime, and specific provisions regarding money laundering risks. It also requires such firms to ensure that approved persons exercise appropriate responsibilities in relation to these AML systems and controls. Parts of the FCA Handbook that are relevant to AML procedures, systems and controls, include:

    - APER - Principle 5 requires an approved person to take reasonable steps to ensure that the business of the firm for which he is responsible is organised so that it is controlled effectively[50];
    - COND – In relation to its ongoing assessment as to whether a firm meets the fitness and properness criterion, a firm is specifically required to have in place systems and controls against money laundering of the sort described in SYSC 6.1.1 R to SYSC 6.3.10 G[51];
    - DEPP – When considering whether to take disciplinary action in respect of a breach of the money laundering rules in SYSC 3.2 or SYSC 6.3 the FCA will have regard to whether a firm has followed relevant provisions in the JMLSG guidance for the financial sector[52];
    - PRIN - Principle 3 requires a firm to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems[53]; and
    - SYSC - Chapters 2, 3 and 6 set out particular requirements relating to senior management responsibilities, and for systems and controls processes, including specifically addressing the risk that the firm may be used to further financial crime. SYSC 6.3.1 R to SYSC 6.3.10 G (and SYSC 6.3) cover systems and controls requirements in relation to money laundering[54].

[50] APER 2.1.2P

[51] COND 2.5.7(10) G

[52] DEPP 6.2.3 G

[53] PRIN 2.1.1 R

[54] SYSC 2 and 3

21. The FCA Handbook of rules and guidance contains high level standards that apply, with some exceptions, to all FCA-regulated firms, (for example, the FCA Principles for Businesses, COND and SYSC) and to all approved persons (for example, the Statements of Principle and Code of Practice for Approved Persons). SYSC sets out particular rules relating to senior management responsibilities, and for systems and controls processes. Some of these rules focus on the management and control of risk[55], and specifically require appropriate systems and controls over the management of money laundering risk[56].

22. The FCA has also issued a publication *"Financial Crime: A Guide for Firms"* which provides practical assistance and information for firms on actions they can take to counter the risk that they might be used to further financial crime.

[55] SYSC 6.1.1 R
[56] SYSC 6.3.7 G