HM Treasury

Home Office

National risk assessment of money laundering and terrorist financing 2017

October 2017

HM Treasury

Home Office

National risk assessment of money laundering and terrorist financing 2017

October 2017

© Crown copyright 2017

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at public.enquiries@hmtreasury.gsi.gov.uk

ISBN 978-1-912225-22-4

PU2107

Contents

Foreword		2
Executive summary		4
Chapter 1	Legal, regulatory and law enforcement framework	7
Chapter 2	Money laundering threat	19
Chapter 3	Terrorist financing threat	26
Chapter 4	Financial services	29
Chapter 5	Financial technology	38
Chapter 6	Accountancy services	43
Chapter 7	Legal services	49
Chapter 8	Property and estate agency services	54
Chapter 9	Trusts and corporate structures	58
Chapter 10	Cash	65
Chapter 11	Money service businesses	68
Chapter 12	Non-profit organisations	73
Chapter 13	Gambling	76
Chapter 14	High value dealers	80
Annex A	Methodology	83
Annex B	Glossary	85

Foreword

The UK is one of the world's largest and most open economies, whose strength is built on extensive and productive relationships across the globe. As Ministers with responsibility for national security and financial services, we want the UK to continue to be an attractive country for legitimate business and a leading global financial centre. But we also recognise that the UK's openness and status as a global financial centre exposes it to the risk of illicit financial flows.

Money laundering and terrorist financing are significant threats. Recent terrorist attacks in London, Manchester and elsewhere highlight the importance of the fight to deprive terrorists of the resources they need. Serious and organised crime has been estimated to cost the UK tens of billions of pounds every year. That is why we must continue to crack down on dirty money, strengthening the UK's security and prosperity as well as that of our partners overseas.

The UK is not alone in facing these threats, and we work hand in hand with our international partners to tackle them. The UK has been at the forefront of recent global efforts to shut down safe spaces for money laundering and terrorist financing. The 2016 London Anti-Corruption Summit led to over 600 specific commitments made by more than 40 countries and six major international organisations.

In 2015, the UK published its first ever national risk assessment of money laundering and terrorist financing, setting out candidly the areas where action was needed. In 2016, the government published an action plan outlining the most significant reforms to our anti-money laundering and counter-terrorist financing regime in over a decade.

Many of the actions in this plan have now been launched or delivered. The Criminal Finances Act 2017 provided tough new powers such as Unexplained Wealth Orders for tackling money laundering and terrorist financing. The Money Laundering Regulations 2017 bring the latest international regulatory standards into UK law. Reforms of the suspicious activity reports regime and the supervisory regime are underway, and our commitment to public-private partnership is embodied in the development of the Joint Money Laundering Intelligence Taskforce, which continues to deliver concrete outcomes in disrupting criminal activity.

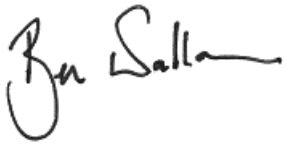
This year, the UK's anti-money laundering and counter-terrorist financing regime will be assessed by the Financial Action Task Force. The UK will be evaluated for the first time against the strengthened global standards introduced in 2012.

This government is determined to demonstrate the UK's commitment to tackling illicit financial flows. We must not stand still. As money laundering and terrorist

financing risks continue to evolve, so must our understanding and our response. This second national risk assessment shows how that has happened since 2015.

This assessment will provide a critical component of the evidence base for the response to money laundering and terrorist financing over the coming years. The government is confident that by responding to these risks, and through continued partnership between government, law enforcement, supervisors and the private sector, we can ensure that the UK economy is a hostile environment for illicit finance and an open, attractive destination for legitimate business.

Stephen Barclay
Economic Secretary to the Treasury



The Rt Hon Ben Wallace
Minister of State for Security

Executive summary

The 2017 national risk assessment (NRA) of money laundering and terrorist financing comes amidst the most significant period for the UK's anti-money laundering (AML) and counter-terrorist financing (CTF) regime for over a decade.

In 2015, the UK published its first NRA, recognising that the same factors which make the UK attractive for legitimate financial activity also make it attractive for criminals and terrorists. In 2016, the government set out how it would address the risks identified in the 2015 NRA when it published its action plan for AML and CTF. This action plan outlined wide-ranging reforms to the law enforcement response to illicit finance, to the AML/CTF supervisory regime and to the way in which we engage internationally to tackle these risks, all underpinning by a strengthened public-private partnership.

As a result of the action plan a number of major changes have been implemented, including through the Criminal Finances Act 2017 (CFA), and the Money Laundering Regulations 2017 (MLRs). Other changes have transformed the way our AML/CTF regime works, including the expansion of the Joint Money Laundering Intelligence Taskforce (JMLIT), which facilitates information sharing between the financial sector and law enforcement. The JMLIT has delivered concrete outcomes in disrupting money laundering and terrorist financing and has provided a model for other countries to follow.

These reforms and others, alongside the 2017 NRA, provide a strong foundation for the UK to build on for its 2017/18 mutual evaluation by the Financial Action Task Force (FATF). The FATF is the international inter-governmental body which sets the global standards for AML and CTF.[1] The FATF will assess the UK next year against these standards, as part of its regular peer review cycle, culminating in a published report known as a mutual evaluation report (MER). This will be the UK's first FATF peer review since 2007, and the final report will be published in December 2018.

Central to all of this remains the principle of developing and maintaining a robust and shared national understanding of money laundering (ML) and terrorist financing (TF) risks. This assessment serves as a stocktake of our understanding of these risks, including how they have changed since the 2015 NRA, and will inform the government's continuing work to prevent terrorists and criminals moving money through the UK.

[1] The FATF also sets to global standards for counter-proliferation financing, though this is out of scope of the NRA.

The 2015 national risk assessment

Key findings from the 2015 NRA included:

- The substantial risk from high-end money laundering, typically involving the laundering of major frauds, corruption or tax evasion through exploitation of financial and other professional services. Significant intelligence gaps were identified in this area, particularly in relation to the precise roles and types of professionals involved.
- Cash-based money laundering was recognised as a continuing area of risk, with few intelligence gaps due to longstanding law enforcement investment in tackling the illegal drugs trade and acquisitive crime.
- Other areas, including gambling, high value dealers (HVDs), e-money and digital currencies, were assessed to pose lower risks, though there were also gaps in the collective understanding of relevant authorities.
- The risks in these areas were assessed to be exacerbated by mixed standards of compliance by firms with the relevant regulations and legislation, and inconsistencies in the supervisory regime.
- Risks were also found to be exacerbated by gaps in the law enforcement response to money laundering at the local police force level and by weaknesses in the UK's regime for suspicious activity reports (SARs).

In response to these findings, the 2015 NRA set out a number of priority areas to be addressed through the 2016 AML/CTF action plan. These are outlined in more detail below under the UK's legal, regulatory and law enforcement framework.

The 2017 national risk assessment

The 2017 NRA has built on the work undertaken in 2015 to identify where risks have changed and where our understanding of these risks has developed, and to explore in further detail those areas identified as high risk. The assessment is the product of extensive consultation across government, including law enforcement and intelligence agencies, and with supervisors and the private sector. The assessment has also drawn on public reports, such as the EU supranational risk assessment of money laundering and terrorist financing.

Key findings of the 2017 assessment include:

- High-end money laundering and cash-based money laundering remain the greatest areas of money laundering risk to the UK. New typologies continue to emerge, including risks of money laundering through capital markets and increasing exploitation of technology, though these appear less prevalent than longstanding and well-known risks.
- The distinctions between typologies are becoming increasingly blurred. Law enforcement agencies see criminal funds progressing from lower level laundering before accumulating into larger sums to be sent overseas through more sophisticated methods, including retail banking and money transmission services.
- Professional services are a crucial gateway for criminals looking to disguise the origin of their funds. While intelligence gaps remain in these areas, we

have developed our understanding substantially since 2015 and have a better understanding of the specific services and specific types of professional at greatest risk of abuse.

- Cash, alongside cash intensive sectors, remains the favoured method for terrorists to move funds through and out of the UK. The UK's terrorist financing threat largely involves low levels of funds being raised by UK individuals to send overseas, fund travel or fund attack planning. The primary means of doing this are assessed to be through cash, retail banking or money service businesses (MSBs).
- A wide-ranging set of reforms by government and law enforcement over recent years is still in its early days, but starting to take effect. These reforms have included reforms to tackle abuse of professional services, legislation to improve the law enforcement response and measures to improve corporate transparency. In addition, improvements to the public-private partnership have already delivered strong results.

Throughout, where we identify risks around services, sectors or entities, our message is not that all those involved in these areas are likely to be criminally complicit or negligent. Rather, it is that those individuals and firms acting in areas of higher risk should be vigilant towards the persistent efforts of criminals and terrorists to exploit the vulnerabilities involved.

Chapter 1

Legal, regulatory and law enforcement framework

1.1 The 2015 NRA outlined the legal, regulatory and law enforcement frameworks governing the AML/CTF regime in the UK. This section provides a recap of that outline, with a particular focus on where aspects of the regime have changed since 2015.

The Financial Action Task Force (FATF)

1.2 The FATF is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The objectives of the FATF are to set standards and promote effective implementation measures for combating money laundering, terrorist financing and proliferation financing.

1.3 The UK was a founding member of the FATF and continues to play a leading role in this body. In addition, the UK is a Cooperating and Supporting Nation to the Caribbean FATF (CFATF) and the Eastern and South African Anti-Money Laundering Group (ESAAMLG), and attends the Middle East North Africa FATF (MENAFATF) and MONEYVAL as an observer. HM Treasury leads the UK delegation to the FATF and represents the UK at the FATF-style regional bodies, working in collaboration with a number of other government departments, agencies and regulatory bodies.

1.4 The FATF's two primary functions are setting the global FATF recommendations and monitoring their implementation among members through a peer review process (mutual evaluation). The government is committed to continuing to implement the FATF recommendations and to showing that the UK has an effective AML/CTF regime during its mutual evaluation, which will be conducted by the FATF in 2017/18.

The European Union (EU)

1.5 The EU implements the FATF recommendations through EU directives that member states are required to transpose into national law. The 2015 NRA outlined the directives and regulations in force at that time. After the FATF updated its recommendations in 2003, the Third Money Laundering Directive was adopted in October 2005. The UK transposed this directive through the Money Laundering Regulations 2007, which built upon existing legislation such as the Proceeds of Crime Act 2002 (POCA) and the Terrorism Act 2000 (TACT). The EU Funds Transfers Regulation[1] was adopted in

[1] Regulation (EC) No 1781/2006 of the European Parliament and of the Council

November 2006, transposing the FATF recommendation on ensuring traceability of payment to prevent the financing of terrorism.[2]

1.6 The EU Fourth Anti-Money Laundering Directive (4MLD) and the Funds Transfer Regulation 2017, which reflect the latest (2012) FATF Standards, as well as the European Commission's assessment of implementation of the Third Money Laundering Directive, were published in the Official Journal of the EU on 20 May 2015.

1.7 4MLD was transposed into UK law through the MLRs, which came into effect on 26 June 2017 bringing the UK's AML and CTF regime into line with the latest international standards. Elements of 4MLD were reopened following recent terrorist attacks in Europe and the leak of the 'Panama Papers'. These negotiations are still ongoing. The government expects to consult on the amending directive once it has been published in the Official Journal of the EU and has come into force. On 23 June 2016, the people of the United Kingdom voted to leave the EU. Until exit negotiations are concluded, the UK remains a full member of the EU and all the rights and obligations of EU membership remain in force. During this period the government continues to negotiate, implement and apply EU legislation. The outcome of these negotiations will determine what arrangements apply in relation to EU legislation in future once the UK has left the EU.

The Money Laundering Regulations 2017

1.8 The 2015 NRA outlined some of the requirements placed by the Money Laundering Regulations 2007, which were in force at the time. These have now been replaced by the MLRs 2017 (the MLRs). These regulations place stringent requirements on relevant persons for the purpose of preventing and detecting money laundering and terrorist financing. Relevant persons subject to the MLRs must have systems and controls in place to identify, assess, manage and mitigate risk for the purposes of preventing and detecting money laundering and terrorist financing.

1.9 The MLRs include (but are not limited to) the requirement for relevant persons to:

- assess risks
- conduct an appropriate level of customer due diligence (CDD)
- have policies and procedures in place to manage risks
- monitor and manage compliance with those policies and procedures
- ensure awareness and training of staff
- keep relevant records

Industry guidance

1.10 In addition to the MLRs, HM Treasury approves AML/CTF guidance written by and for most regulated industry sectors. This guidance provides detailed assistance to firms on the practical application of legal and regulatory

[2] 'FATF IX Special Recommendations', FATF, October 2001

requirements to their business or sector. Guidance is also reviewed by the Money Laundering Advisory Committee (MLAC) a forum through which senior representatives from industry, law enforcement, supervisors and government advise on the operation of an effective and proportionate AML/CTF regime.

Proceeds of Crime Act 2002

1.11 The Proceeds of Crime Act 2002 (POCA) contains the single set of money laundering offences applicable throughout the UK to the proceeds of all crimes. POCA provides the framework for asset recovery in the UK, as well as a number of powers to enable law enforcement agencies to investigate money laundering and to recover the proceeds of crime.

1.12 POCA requires institutions in the regulated sector to submit SARs where there are suspicions of money laundering and terrorist financing to the UK Financial Intelligence Unit (UKFIU). Any person can seek a defence against committing a money-laundering offence if they request the consent of the National Crime Agency (NCA) to conduct a transaction or activity about which they have suspicions through submitting a 'Defence Against Money Laundering' (DAML) SAR.

1.13 POCA provides financial investigatory powers to the police, officers of Her Majesty's Revenue and Customs (HMRC), the NCA and certain non-warranted accredited financial investigators. These powers allow those bodies to investigate and develop cases to recover the proceeds of crime.

1.14 POCA also sets out the legislative framework for the recovery of criminal assets. There are different routes available, comprising: criminal confiscation (seeking to recover the financial benefit that an individual has gained as a result of their offending); civil recovery (recovering the proceeds of unlawful conduct without the need for a conviction); cash seizure and forfeiture (allowing authorised persons to seize cash suspected of being the recoverable property of unlawful conduct); and taxation (enabling the NCA to adopt the direct taxation functions of HMRC where no tax has been paid as the result of criminal conduct).

1.15 The CFA introduces measures to enhance the ability to investigate and recover the proceeds of crime, and strengthen the suspicious activity reporting regime. Specific measures are described later in this chapter.

Terrorist financing legislation and regulations

1.16 The legal definition of terrorist property is contained in section 14 of TACT. Terrorist property refers to: money or other property which is likely to be used for the purposes of terrorism, proceeds of the commission of acts of terrorism and proceeds of acts carried out for the purposes of terrorism. The terrorist financing offences in TACT include inviting, providing, or receiving money or property with the intention or reasonable suspicion that it will be used for the purposes of terrorism and using or intending to use money or other property for the purposes of terrorism.

1.17 The UK terrorist asset freezing regime meets obligations placed on the UK by UN Security Council Resolutions (UNSCRs) and associated EU regulations. It is

implemented by the Terrorist Asset-Freezing etc. Act 2010 (TAFA). In March 2016, the government created the new Office of Financial Sanctions Implementation (OFSI) to strengthen the UK's sanctions implementation. OFSI is part of HM Treasury and is responsible for implementing and enforcing financial sanctions in the UK, including implementation of terrorist asset freezes. OFSI works with a wide range of individuals, businesses and non-profit organisations (NPO) affected by sanctions to raise awareness, provide financial sanctions guidance, while delivering a professional service to the public and industry. OFSI also works closely with other government departments to ensure that sanctions breaches are rapidly detected and addressed effectively. OFSI's overarching aims are to: support the UK's foreign policy and national security goals; and to help maintain the integrity of and confidence in the UK financial services sector.

1.18 In December 2015, a special session of the UN Security Council attended by the previous Chancellor of the Exchequer adopted UNSCR 2253, strengthening measures against Daesh financing in place through UNSCR 1267. On 20 July 2017, the Security Council unanimously adopted UNSCR 2368, further updating this regime. FATF Recommendation 6 requires freezing 'without delay' of the assets of individuals or entities designated under UNSCRs 1267[3] and 1373.[4] The purpose of implementing a freeze without delay is to avoid asset flight in the period between identification of an individual or entity and the freeze being imposed. The 2015 NRA highlighted the UK's concerns that the delay in implementing UN listings at EU level gave led to a possible risk of asset flight. The government has now addressed this risk through powers in the Policing and Crime Act 2017, allowing the UK to implement UN Security Council Resolutions on a temporary basis until implemented at EU level.

1.19 When the UK leaves the EU, sanctions will continue to be implemented through new powers to fulfil our international obligations under the UN and impose further sanctions domestically. These powers are currently being taken through Parliament through the Sanctions and Anti Money Laundering Bill.

Law enforcement response to money laundering

1.20 High-end money laundering has been identified as one of the top six national priorities for agencies tackling serious and organised crime. [5] The NCA is the lead agency for the response to serious and organised crime in the UK. The NCA's National Intelligence Hub is responsible for gathering, analysing and disseminating information, and its Prosperity Directorate leads the response to economic crime across the UK – including working with law enforcement, regulatory bodies and the private sector.

---

3 UNSCR 1267 requires states to freeze the assets of designated individuals and entities associated with Al Qaida and Daesh. The UK implements UN asset freezes by way of EU Regulation which takes direct effect in the UK. The ISIL (Da'esh) and Al Qaida (Asset Freezing) Regulations 2011 impose criminal penalties for breaching this regime.

4 UNSCR 1373 requires states to freeze the assets of terrorists and prohibit their nationals and persons within their jurisdiction from making funds, resources or financial services available to them. It is implemented in the UK by TAFA and EU Common Position 931 and Regulation 2580/2001.

5 'NCA Annual Plan 2017/18', NCA, March 2017

1.21 The tools available to the NCA to tackle money laundering, as well as other crimes, include: intelligence and evidence-gathering; cash seizure and forfeiture; restraint and confiscation; and civil recovery and taxation. In 2016/17, the NCA led and coordinated operational activity resulting in £82.8 million being denied to criminals impacting on the UK, and recovering assets of £28.3 million. NCA activity has also led directly to 1,441 arrests in the UK and 1,176 arrests overseas across all crimes.[6]

1.22 All forces within the UK can carry out money laundering investigations. There are 43 police forces in England and Wales subject to oversight from Police and Crime Commissioners. Scotland has a single national police service, Police Scotland, which is funded by and accountable to the Scottish Police Authority. In Northern Ireland, the Police Service of Northern Ireland (PSNI) is funded by the Northern Ireland Department of Justice and is accountable to the Northern Ireland Policing Board. The City of London Police (as national lead force for economic crime and fraud) and the Metropolitan Police Service (MPS) regularly take on national investigations and provide support to the NCA. In 2015/16 the police secured over £91 million in cash forfeiture and confiscation remittances. Over £120 million of new orders were granted in the same period. In 2016, 1,435 individuals were convicted of money laundering in the UK, though it should be noted that criminals may also be charged and convicted under the relevant predicate offence.

1.23 Police forces in England and Wales have collaborated to form Regional Organised Crime Units (ROCUs) across nine policing regions. These units deliver specialist investigative and intelligence capabilities within their regions and are the primary interface between the NCA and forces and are accountable to their respective Police and Crime Commissioners. Within each ROCU is a Regional Asset Recovery Team (RART), which develops financial intelligence in aid of investigation and disruption of subjects. There are over 180 staff in the RARTs, all of whom are operational.

1.24 In addition to these capabilities is the Asset Confiscation Enforcement (ACE) network funded by the Asset Recovery Incentivisation Scheme (ARIS). This capability has a presence across every region in England and Wales and has had a significant impact on tackling unenforced confiscation orders. the current financial year, the ACE network has collected over £30 million.

1.25 The UKFIU, an operationally independent part of the NCA, receives financial intelligence gathered from SARs, and makes all SARs available to law enforcement agencies for their own analysis and investigations (with the exception of SARs in certain sensitive categories). The 2015 NRA reported that the UKFIU received 354,186 SARs in 2013/14, of which 14,155 were DAML SARs.[7] This has now increased to 419,451 SARs and 18,198 DAML SARs in 2015/16.[8] The UKFIU works in close partnership with other key

---

6 'NCA Annual Report and Accounts', NCA, 2016/17

7 In 2016 the UKFIU introduced the term 'Defence Against Money Laundering' (DAML) as the term 'consent' was frequently misinterpreted by reporters. The term 'DAML' is aimed at educating reporters and improving submissions by clarifying what the UKFIU can/cannot grant.

8 'Suspicious Activity Reports (SARs) Annual Report 2014', NCA, December 2014; Suspicious Activity Reports (SARs) Annual Report 2017', NCA, October 2017.

international organisations to fight money laundering and terrorist financing. The UKFIU is a fully active member of the international Egmont Group of Financial Intelligence Units, set up to improve cooperation in the fight against money laundering and the financing of terrorism.

1.26 The Serious Fraud Office (SFO) is an independent government department that investigates and prosecutes serious or complex fraud, and corruption. It has jurisdiction in England, Wales and Northern Ireland but not in Scotland, where this responsibility rests with the Crown Office and Procurator Fiscal Service. The SFO's Proceeds of Crime Division comprises a team of lawyers and financial investigators who deal with confiscation investigations, restraint proceedings, money laundering investigations and civil recovery work across the SFO's cases, as well as mutual legal assistance (MLA) requests. In the period 2016/17 the SFO obtained 12 confiscation orders with a combined value of £25.3 million (an increase from £22.7 million in 2014/15), and recovered £9.1 million through enforcement of previous orders.

1.27 HMRC, as the UK's tax authority, is a non-ministerial department reporting to Parliament through its Treasury Minister. HMRC is also a supervisor for some businesses under the MLRs, and is responsible for investigating crime involving all of the regimes it deals with using civil, as well as criminal, procedures similar to those available to other law enforcement agencies. HMRC can investigate money laundering (and predicate) offences using POCA investigative powers, recover criminal cash through summary proceedings and recover the proceeds of crime through working with the independent prosecutors. HMRC's Proceeds of Crime Intervention Team (POCIT) was set up in 2015 to target cash couriers, MSBs and HVDs. A confirmed total of over £4.9 million has been seized by POCIT since its establishment.

1.28 The Crown Prosecution Service (CPS) is the principal independent prosecuting authority in England and Wales and is responsible for prosecuting money laundering and other criminal cases investigated by the police, HMRC, the NCA and other government agencies. It advises law enforcement on lines of inquiry, reviews cases for possible prosecution; determines the charge in all but minor cases; prepares cases for court; and applies for restraint, receivership and confiscation orders in respect of CPS prosecutions. The CPS also obtains restraint orders and enforces overseas confiscation orders on behalf of overseas jurisdictions pursuant to MLA requests.

1.29 The Public Prosecution Service Northern Ireland (PPSNI) is responsible for prosecuting criminal cases investigated by the police, HMRC and the NCA in Northern Ireland. It is headed by the Director of Public Prosecutions Northern Ireland who is accountable to the Attorney General Northern Ireland.

1.30 The Crown Office and Procurator Fiscal Service (COPFS) is responsible for the prosecution of all crime in Scotland. COPFS' responsibilities include the investigation, prosecution and disruption of crime, including the maximisation of measures to ensure the recovery of proceeds of crime. COPFS has an investigative role and can provide instructions and directions to the police and all other specialist reporting agencies. In all matters of

international cooperation, Scotland deals directly with the criminal authorities in other countries. COPFS is headed by the Crown Agent who is accountable to the Lord Advocate, the principal law officer of the Crown in Scotland.

Law enforcement response to terrorist financing

1.31 The Home Office is responsible for UK CTF policy, with other key government departments and operational partners critical in undertaking activity to disrupt key terrorist financing threats and risks.

1.32 UK intelligence agencies are responsible for monitoring and assessing the terrorist financing threats to the UK and its interests overseas. These agencies are supported by the National Terrorist Financial Investigation Unit (NTFIU), part of the Metropolitan Police Service Counter Terrorism Command, which has the strategic police lead for countering terrorist financing in the UK. NTFIU leads investigations where the primary focus is on addressing the finances of a terrorist, a financier of terrorism or of a terrorist organisation, and supports mainstream MPS counter-terrorism investigations with both financial intelligence and financial disruption options. Nationally, there are ten additional Counter-Terrorism Units (CTUs) and intelligence units located in England, Scotland, Wales and Northern Ireland, responsible for investigating instances of terrorist financing occurring within their geographical regions and for supporting mainstream counter terrorism investigations with financial intelligence. The UKFIU's Terrorist Finance Team identifies, assesses and exploits SARs submitted under both TACT and POCA. Due to the additional sensitivity around SARs submitted under TACT, and those SARs submitted under POCA identified as having a terrorist financing link, these SARs are made available only to a restricted group of end users.

1.33 In relation to terrorist asset-freezing, proposals for designation under TAFA are made to OFSI by the police and the Security Service, or by other government departments or international governments where there is evidence to support a designation. The investigation of breaches is conducted by the relevant CTU, with engagement from others including OFSI and the CPS.

AML/CTF action plan 2016

1.34 Following the first NRA in 2015, and following the priority areas for action set out by that assessment, the UK published an action plan on AML and CTF in April 2016. The action plan focussed on four key areas: a stronger partnership with the private sector; improving the effectiveness of the supervisory regime; enhancing the law enforcement response to tackle the most serious threats; and increasing our international reach.

1.35 The UK has implemented a series of reforms and actions since this point to address these areas, including regulatory and supervisory reforms to tackle abuse of professional services, legislation to improve the law enforcement response to illicit finance, measures to improve corporate transparency and improvements to the public-private information sharing.

Strengthening the public-private partnership

1.36 The action plan responded to the 2015 findings on SARs by recommending reform of the SARs regime. A programme of work to deliver SARs reform was established in 2016 and has set out a 'twin track' approach to deliver short-term improvements in 2017/18 and set the long-term direction for the future regime. The shorter-term improvements include working with the financial sector to improve the quality of reporting, in-depth training for law enforcement agencies to enable them to make better use of SARs intelligence, and measures introduced by the CFA.[9] The Home Office and NCA recognise that more fundamental reform of the regime is required and are currently conducting an analysis of options. Work has also commenced to replace the SARs IT systems.

1.37 In addition, in light of the risks from the size, complexity and international exposure of the UK's financial sector, the action plan recommended that the JMLIT be placed on a permanent footing, after a successful pilot period. This has been successfully executed and is a successful example of partnership working.[10]

1.38 The 2015 NRA also identified risks arising from the size, complexity and international exposure of the UK's professional service sector, and the role of some professionals in the accountancy and legal sectors in laundering of proceeds of crime. The Home Office, in partnership with the NCA, HMRC the accountancy professional body supervisors, and certain legal professional body supervisors, has delivered targeted communications campaigns to professionals within these sectors from 2014. The campaigns aimed to increase awareness of the risks of money laundering within these sectors and encourage the reporting of suspicious activity to the NCA. The campaigns, delivered through national and press media, resulted in an increased awareness of the NCA's AML/CTF guidance with visits 153% higher in 2016/17 compared to the previous year. Data from the NCA has also highlighted increased reporting of suspicious activity. Ongoing communications activity will continue to raise awareness of the indicators of money laundering activity, the risks of involvement and the importance of reporting suspicious activity.

Enhancing the law enforcement response

1.39 The CFA was introduced in response to the need identified in the 2015 NRA to strengthen the law enforcement response to money laundering and terrorist financing. The Act contains some of the most significant changes to POCA since its creation.

1.40 In recent years, the UK's efforts to tackle international corruption and serious organised crime have been hampered by difficulties identifying and recovering assets in the UK which are the proceeds of crimes committed overseas. Unexplained Wealth Orders, introduced through the CFA, can be used to require those suspected of involvement in or association with serious

[9] These include the power for the NCA to obtain further information, the extension of the moratorium period, and the ability for regulated entities to share information with each other to submit joint SARs,

[10] The activities and impact of the JMLIT are discussed further in chapter 4.

crime to explain the origin of their assets where disproportionate to their known income. Failure to provide a full or truthful response could lead to or assist with civil recovery action, or could lead to a criminal conviction. The Act allows this power to be applied to politically exposed persons (PEPs) entrusted with a prominent public function by an international organisation or a state outside the European Economic Area (or those associated with them) even with no specific suspicion of serious criminality and can also be applied in relation to property held in a trust. The Act also allows for recovery of property obtained through gross human rights abuses overseas by public officials.

1.41 The CFA introduced a new power to seize or freeze bank accounts, where there is a suspicion that they contain recoverable property, or that the contents will be used to commit further offences. This strengthens law enforcement agencies' ability to disrupt criminal funding, allow the recovery of criminal property, and prevent abuse of the financial system. The CFA also introduced a new power into POCA to seize mobile stores of value. The measure allows law enforcement agencies to search for and seize certain personal items (and subsequently apply for a forfeiture order), such as precious metal and jewels, when suspicious that these items are the proceeds of crime or intended for use in unlawful conduct. Where law enforcement agencies believe they have sufficient grounds, they can apply to a court for a forfeiture order. In addition to these, the Act widened the definition of cash to include betting slips, gaming tokens and casino chips.[11]

1.42 Previously where a DAML SAR related to complex cases, the moratorium period of 31 days did not allow investigators sufficient time to gather the necessary evidence to apply for a restraint order or a property freezing order. This led to a risk of criminal proceeds being laundered before law enforcement agencies could act. The Act allows the moratorium period to be renewed by a court for periods of up to 31 days, to a total of 186 additional days. This will allow investigators to gather evidence to determine whether further action should take place. The CFA also introduces a new power to request further information on a SAR. This allows the NCA (or additionally police, for terrorist finance purposes) to apply for a Further Information Order to compel the provision of the information within a specified period of time.

1.43 The CFA contains various provisions which will improve the UK's ability to recover criminal assets. The Act will simplify and expedite the process for obtaining information in confiscation and money laundering investigations by allowing investigating officers to apply for disclosure orders. This measure will provide officers with a more streamlined application process, providing investigators with a powerful and flexible tool enabling more effective investigation of hidden or disguised assets. The Act also provides direct access to investigators from the SFO to further powers in relation to: search, seizure, detention and sale of property in confiscation; recovery of cash; and application for investigation orders and warrants. This measure recognises the SFO's unique role in the investigation of complex financial crime.

11 This is discussed in more detail in chapter 13.

1.44 The Act also makes complementary changes to the law enforcement response to the threat of terrorist financing. This includes mirroring many of the provisions in the Act so that they also apply for investigations into offences under TACT. The Anti-Terrorism Crime and Security Act 2001, which provides various powers and offences relating to the civil recovery of terrorist property, was amended by the CFA to introduce powers to freeze and forfeit terrorist property, including 'terrorist cash', 'terrorist assets' and 'terrorist related funds' held in bank or building society accounts.

1.45 The UK has also taken further action over recent years to improve corporate transparency in light of money laundering risks highlighted by the Panama Papers and reports bringing to light the exploitation of Scottish limited partnerships (SLPs). This has included the introduction in 2016 of the publicly accessible register of people with significant control (PSC) in companies and extension of its requirements to SLPs in June 2017; the abolition of bearer shares; and the introduction of a register of trusts with tax consequences. These steps will mitigate the risk of corporate structures being used to launder the proceeds of corruption and organised crime, including where the structures are operated and controlled overseas.

1.46 In addition to this, the law enforcement response to money laundering and terrorist financing continues to benefit from evolution of the intelligence picture. The 2015 NRA identified a number of intelligence gaps around money laundering and terrorist financing. While some of these gaps remain, law enforcement agencies have taken significant steps to address the gaps, in particular around high-end money laundering. These steps have included improving cross-agency intelligence flows and improving cooperation with the private sector and regulatory bodies.

Improving the effectiveness of the supervisory regime

1.47 HM Treasury is responsible for appointing AML/CTF supervisors. There are currently 22 professional body supervisors in the UK, in addition to supervision of specific industry sectors by the Financial Conduct Authority (FCA), HMRC and the Gambling Commission.

1.48 The 2015 NRA identified a number of vulnerabilities in the UK's supervisory regime. The NRA found that the effectiveness of the UK's supervisory regime was inconsistent and, while some supervisors were found to be highly effective in some areas, room for improvement was identified across the board, including in understanding and applying a risk-based approach to supervision and in providing a credible deterrent. The number of professional body supervisors in some sectors risked inconsistencies of approach, and data was not yet seen to be shared between supervisors (or with law enforcement agencies) freely or frequently enough.

1.49 In response to these vulnerabilities, the government announced in March 2017 its intention to create a new supervisory function within the FCA, called the Office for Professional Body AML Supervision (OPBAS). The government has proposed that OPBAS oversees the adequacy of the AML/CTF supervisory arrangements of professional body supervisors in the UK. Strengthening oversight of the AML/CTF supervisory regime will ensure

that all AML supervisors provide effective supervision, as required by the 4MLD.

1.50 OPBAS is expected to be up and running by the end of 2017, will promote a risk-based approach to supervision, and will have a number of supervisory and enforcement powers to fulfil its role. These powers were set out in draft regulations published in July 2017. OPBAS will not only seek to ensure that supervisory standards are consistent across the professional bodies, but will also seek to enable better information and intelligence sharing between the bodies.

Increasing the UK's international reach

1.51 Increasing the UK's international reach was highlighted by the first NRA as key to tackling the threat from money laundering and terrorist financing. Since 2015, the UK has continued to prioritise working with other countries to tackle underlying criminal activity, detect illicit assets and facilitators responsible for money laundering, and restore the assets to their source country.

1.52 On 12 May 2016, the UK hosted the London Anti-Corruption Summit, and bought together world leaders, civil society, businesses, sports bodies and international organisations to make fighting corruption a global priority. The summit led to over 600 specific commitments made by more than 40 countries and six major international organisations, alongside a Global Declaration against Corruption. Alongside wider anti-corruption measures, many of these commitments are significant in terms of tackling predicate offences and money laundering activities.[12] In terms of wider multilateral efforts to tackle illicit finance, the UK has been working with the FATF to identify barriers to cross-border information sharing and is currently co-leading a FATF project on tracking illicit financial flows from human trafficking. The UK continues to play a leading role in the Global Coalition against ISIL, including at the international Counter-ISIL Finance Group, and engages strongly in the OECD's Taskforce on Tax Crime and Other Financial Crime (TFTC). HMRC is leading a TFTC project on the risk posed by Professional Enablers and will host the next OECD Forum on Tax and Crime in London in November 2017.

1.53 In terms of bilateral and operational work, there are significant levels of cooperation that continue to be built upon by law enforcement agencies across international boundaries. The NCA has a significant presence overseas through its network of International Liaison Officers. The NCA conducts regular reviews of this network to ensure that officers are in the right places and has recently increased its presence in priority countries. HMRC has a network of overseas Fiscal Crime Liaison Officers (FCLOs) working with overseas tax, customs and police administrations to target and tackle serious fraud and money laundering. A new International Anti-Corruption Coordination Centre, hosted by the NCA in London, became operational in July 2017. The IACCC brings together specialist law enforcement officers

[12] The full list of country-specific commitments is available at https://www.gov.uk/government/publications/anti-corruption-summit-country-statements.

from multiple agencies into a single location to coordinate the global law enforcement response to allegations of grand corruption.

1.54 The UK and US are co-hosting the first Global Forum for Asset Recovery in December 2017. The World Bank estimates that tens of billions of dollars of state funds are funnelled each year into the pockets of corrupt politicians and officials in developing countries, and from there to bank accounts, property and other assets abroad. The forum presents a significant opportunity for political recommitment to asset recovery, case progression, and capacity building initiatives.

Asset recovery action plan 2017

1.55 The commitment to publish an asset recovery action plan was made last year in the Home Office response to the Public Accounts Committee, setting out the ambition to do more to improve performance in the asset recovery regime. The asset recovery action plan, to be published later this year, will set out how the UK is responding to the challenges involved in improving the recovery of the proceeds of crime. While the UK's performance in asset recovery has been broadly stable, the government strives to be more ambitious in tackling criminal finances and the action plan will outline a new approach to asset recovery. In particular, the plan will seek to develop more effective ways of calculating the value of the wider benefits of financial investigation and make this information available to the public.

Chapter 2
Money laundering threat

2.1 This chapter provides an update on the nature and scale of the money laundering threat in the UK, defined as those activities which lead to criminal intent to launder money. This is both in terms of the domestic threat (proceeds-generating predicate offences in the UK) and the cross-border threat (the UK's exposure to criminals operating overseas seeking to launder money into or through the UK, as well as the risks of UK funds being laundered overseas).

2.2 Those responsible for money laundering threats to the UK make use of a wide range of methodologies, purposes and levels of scale and complexity. They can range from laundering small amounts of cash within the UK to sophisticated processes involving large sums of money and exploiting UK and overseas financial and professional services industries.

2.3 While a significant amount of criminal activity in the UK generates its proceeds in cash, law enforcement agencies are seeing increasingly blended methodologies, as criminals seek to exploit different vulnerabilities in different sectors. The purpose behind the methodologies employed can vary. It can be either to confuse the audit trail, to further invest in criminal activity or simply to enjoy the benefits of crime.

2.4 The traditional areas of money laundering activity remain, though new methodologies continue to emerge within these. Cash-based money laundering is still heavily characterised by the use of cash intensive businesses to disguise criminal sources of wealth, combined with the abuse of legitimate UK services such as money transmission (often managed through international controllers) and retail banking to move funds. High-end money laundering is defined as the laundering of large amounts of criminal funds (often the proceeds of serious fraud or overseas corruption) through the UK financial and professional services sectors. It exploits the global nature of the financial system, often transferring funds through complex corporate vehicles and offshore jurisdictions. Trade based money laundering involves the exploitation of the international import and export system to disguise, convert and transfer criminal proceeds through movement of goods as well as funds. Often the methodology employed depends on how the proceeds of crime are generated, and the section below provides an outline of the different sources of criminal proceeds assessed to be highest priority for the UK.

Domestic threat

2.5 The 2015 NRA highlighted a downward trend in overall UK crime levels over the past 20 years, while recognising the substantial social and economic costs still imposed by organised crime and those facilitating it. The 2016/17 Crime Survey for England and Wales (CSEW) showed 5.9 million incidents of crime, a 7% reduction compared with the previous year's survey.[1]

2.6 The UK adopts an 'all-crimes approach' to money laundering, meaning that laundering the proceeds of any crime is an offence. While financial gain may not always be the principal motivation for involvement in serious and organised crime, those involved pose a particular threat as they seek to make use of corruption or technology to enable offending, and can have links to or are part of organised crime groups (OCGs) based overseas. Most serious and organised crime is conducted by criminals operating in loose networks based on trust, reputation and experience. At the end of 2016, there were around 5,900 criminal groups in the UK, comprising approximately 39,400 individuals.[2]

2.7 The 2015 Strategic Defence and Security Review reaffirmed serious and organised crime as a threat to national security. The 2015 NRA highlighted that the social and economic costs of the most serious and organised crimes total £24 billion per year,[3] with most of this related to drugs supply at £10.7 billion and fraud at £8.9 billion, while also identifying intelligence gaps around the size of criminal markets in the UK.

2.8 The 2015 NRA identified offences in the UK that generate a significant scale of criminal proceeds. These were fraud and drugs supply.

Drugs supply and drugs offences

2.9 The scale of illicit drugs supply is best estimated by considering demand. The 2015 NRA highlighted the reduction in drug misuse among adults and young people compared with a decade ago in England and Wales. Drugs misuse has continued to decline since 2015.

2.10 The size of the illicit drugs market in the UK in 2010 was estimated to be £3.7 billion.[4] Drugs misuse has dropped from 10.5% of the adult population in 2005/6 to 8.4% in 2015/16.[5] There were 148,553 drug seizures in England and Wales in 2015/16, an 11% decrease compared with the previous year. Over the same period there was a 13% decrease in the number of police recorded drug offences.[6]

2.11 The illicit drugs market has diversified in recent years to include the manufacture of synthetic cannabinoids and psychoactive substances, which can be bought online or imported by criminal gangs. These drugs have been

[1] This excludes the new experimental statistics on fraud and computer misuse.

[2] 'National Strategic Assessment of Serious and Organised Crime', NCA, 2017

[3] 'Understanding Organised Crime: estimating the scale and social and economic costs', Mills, Skodbo & Blyth, 2013

[4] 'Understanding Organised Crime: estimating the scale and social and economic costs', Mills, Skodbo & Blyth, 2013

[5] 'Drug misuse: findings from the 2015 to 2016 Crime Survey for England and Wales', Home Office, 2016

[6] 'Seizure of drugs in England and Wales, year ending 31 March 2016', Home Office, 2016

identified by UNODC as one of the most significant problems worldwide. In 2016, the government made it an offence to produce, supply, possess and import and export psychoactive substances, through the Psychoactive Substances Act 2016.

2.12 In terms of asset confiscation orders made from 2015 to 2017, drug trafficking orders account for 54% of all orders, and 16% of the value. These figures are similar to those from 2010-14 in the 2015 NRA.

Fraud and tax evasion

2.13 The 2015 NRA highlighted fraud and tax offences as the largest known source of criminal proceeds from offending in the UK.

2.14 Fraud is, in many ways, a unique crime covering a broad range of crime types, victims and perpetrators. It includes crimes against the public, private and charity sectors and can be committed both online and offline. Its true scale is difficult to assess given issues around under-reporting (such as due to embarrassment or business reputation) and non-reporting (such as individuals not understanding they are a victim).

2.15 The precise scale of fraud in the UK remains an intelligence gap, though experimental statistics published as part of the CSEW 2016/17 indicate that there were 3.4 million incidents of fraud in the year ending March 2017, with the majority relating to bank and credit account fraud.[7]

2.16 The NCA has assessed that it is likely that fraud losses in the UK are increasing.[8] Adults in England and Wales are more likely to be a victim of fraud than any other crime type.[9] Financial Fraud Action UK estimated financial fraud losses across payment cards, remote banking and cheques to total over £768 million in 2016, a 2% increase from 2015.[10]

2.17 Tax evasion is illegal activity, where registered individuals or businesses deliberately omit, conceal or misrepresent information in order to reduce their tax liabilities. HMRC's estimate of the tax gap is a useful tool for understanding fraud against the public sector. The estimated tax gap for evasion in 2014/15 was £5.2 billion. The tax and duty regimes are also subject to criminal attacks including the coordinated and systematic smuggling of goods such as alcohol or tobacco and VAT frauds. Criminal attacks on the tax system are estimated to have lost the government £4.8 billion in 2016.

Cyber crime

2.18 Cyber crime is defined as: crimes that can be committed through the use of information communications technology (ICT) devices, where the devices are both the tool for committing the crime and the target of the crime (such as hacking or deployments of malware); or traditional crimes which are changed significantly by ICT in terms of scale and reach (such as cyber-

7 'Crime in England and Wales: Year ending March 2017. ONS. Statistical Bulletin. July 2017

8 'National Strategic Assessment of Serious and Organised Crime', NCA, 2017

9 'Crime Survey of England and Wales 2016/17', Office for National Statistics, July 2017

10 'Fraud the Facts 2017', Financial Fraud UK, 2017

enabled fraud or data theft). High-profile incidents include the May 2017 WannaCry global ransomware attack, which affected victims across the world, including various NHS trusts and businesses in the UK.

2.19 There were 19,537 computer misuse offences recorded by the National Fraud Intelligence Bureau in the year ending March 2017, an increase of 48% (13,210) from year ending March 2016. Hacking of social media and email was the most commonly reported offence, followed closely by reports of computer virus or malware and spyware. The CSEW reported that in the year ending March 2017 there were 1.8 million computer misuse incidents against individuals, and that of the 3.4 million incidents of fraud 57% were cyber-related.[11] However, under-reporting by both individuals and organisations (including financial institutions) remains a significant issue, with CSEW statistics estimating that only 6.4% of computer misuse incidents were reported to the police or to Action Fraud. This means that the true scale and cost of cyber crime continues to be obscured.

2.20 The new National Cyber Security Centre, part of GCHQ, is focussed on improving collaboration with industry, ease of reporting and strengthening relationships between government agencies and industry. This will facilitate better communication, better victim notification, remediation and more immediate and effective law enforcement activity.

Acquisitive crime

2.21 Acquisitive crime covers theft, robbery and burglary, and may be carried out by individuals or OCGs. The 2015 NRA highlighted downward trends in acquisitive crime since the mid-1990s, with the 2013/14 CSEW reporting 4.56 million theft and robbery offences. This has now declined further to 3.45 million offences in the 2016/17 CSEW, though incidents of acquisitive crime reported to the police have slightly increased. The NCA's National Strategic Assessment of Serious and Organised Crime 2017 states that the theft of motor vehicles is on an upward trend, across all regions and vehicle types, with some vehicles stolen for export. Some vehicles, particularly motorcycles and scooters, have then been used for further acquisitive crimes. There has also been an increase in the number of ATM attack methodologies over recent years. There has been a slight decrease in cash and valuables in transit incidents and a reduction in 'smash and grab' and armed robbery offences. UK law enforcement agencies continue to work with industry to mitigate these threats.

Organised immigration crime

2.22 There were over 1 million illegal border crossings into the EU in 2015 and more than 510,000 in 2016, driven in part by instability in Africa and the Middle East. This demand is being facilitated by OCGs due to the perception that the facilitation of illegal migration represents a low risk and high reward activity. As a result, organised immigration crime is now assessed to be the fastest growing criminal market in Europe.[12] Europol estimated that in 2015,

11 'Cyber-related' refers to where the internet or any type of online activity was related to any aspect of the offence.

12 'Europol-Interpol Report on Migrant Smuggling Networks', Europol and Interpol, May 2016

migrant smuggling networks offered facilitation services and generated an estimated €4.7 billion to €5.7 billion in profit across Europe. The UK's Organised Immigration Crime Taskforce, launched in 2015, brings together officers from the NCA, Border Force, Immigration Enforcement and the CPS to tackle OCGs' migrant smuggling operations. There remains an intelligence gap around the financial flows from organised immigration crime and the UK as a destination of illicit funds.

Modern slavery

2.23 The term 'modern slavery' includes the offences of human trafficking, slavery, servitude and forced or compulsory labour. The true scale within the UK is unknown and the estimate made in the 2015 NRA of between 10,000 and 13,000 victims remains the most robust quantitative assessment available. Though there has been an increase in reporting, it has not been possible to prove whether this has been because of an increase in incidence or because of improved reporting. The 2015 NRA highlighted an intelligence gap around how the proceeds of modern slavery are laundered; the FATF project currently being co-led by the UK on tracking illicit financial flows from human trafficking should help pave the way towards addressing this gap.

International threat

2.24 Money laundering and terrorist financing are global threats. The UK is a major global financial centre and the world's largest centre for cross-border banking. It accounts for 17% of the total value of international bank lending and 41% of foreign exchange trading. The UK also attracts significant investment, ranking first in Europe for foreign direct investment projects in 2016. The vast majority of financial transactions through and within the UK are entirely legitimate. The UK government recognises, however, that as a global financial centre the UK is particularly vulnerable to money laundering threats overseas.

2.25 The integrity of the UK as a global financial centre is essential for our international reputation and long-term prosperity. Since the publication of the 2015 NRA, the UK government and private sector have taken steps to make the UK more hostile to money laundering and terrorist financing. These actions are captured in the UK's 2016 action plan for anti-money laundering and counter-terrorist financing.

2.26 The UK's open economy means that businesses and banks have relationships across the globe. This section outlines those jurisdictions assessed to be particularly relevant to the cross-border money laundering risks faced by the UK, in particular due to their levels of economic, financial and law enforcement relationships with the UK, as well as due to the range of money laundering threats they face domestically.

Threats from organised crime and overseas corruption

2.27 Corruption is assessed to cost the global economy billions of pounds every year, to perpetuate poverty in developing countries and to impede effective government. The think tank Global Financial Integrity produces estimates of

the amounts lost to developing countries through illicit financial flows (including corruption) each year, with its most recent estimates suggesting Mainland China ($1.39 trillion) and Russia ($1.05 trillion) lost the most to illicit flows from 2004-2013.

2.28 The Chinese Government has taken significant steps to strengthen its AML regime in recent years, and has recently demonstrated its commitment to tackling corruption by launching a major anti-corruption initiative. China co-chaired the G20 anti-corruption working group with the UK last year. In addition to corruption risks, UK operational activity has identified illicit financial flows to China laundering the proceeds of organised crime, including illicit drugs manufacturing, counterfeiting, fraud and tax evasion. China has launched a number of initiatives to tackle these issues. Alongside commitments to global initiatives on cooperation and information sharing, the UK is working with the People's Bank of China on a number of projects to exchange expertise on preventing money laundering. More widely, the UK and China remain committed to developing bilateral trade and investment.

2.29 Russia, as an active member of the FATF, also continues to make progress in strengthening its AML/CTF regime. The domestic threat from money laundering remains high, and outward flows of illicit capital from Russia pose a particular international threat. For the UK, the key money laundering risk in relation to Russia is that the proceeds of crime and corruption may be channelled through the UK economy, through both regulated and unregulated sectors. To manage this risk, the UK continues to encourage firms to take a risk-based approach in establishing and maintaining relationships with jurisdictions with higher levels of corruption.

Remittances and other financial flows

2.30 Given the large remittance and business links between Pakistan and the UK, both countries are exposed to this corridor being abused for money laundering or terrorist financing. There is a risk of criminal groups exploiting these links to facilitate money laundering, particularly the laundering of the proceeds of corruption, fraud and drug trafficking. Criminals have exploited tools including MSBs, cash smuggling, front businesses, trade based money laundering and property to launder funds both from the UK to Pakistan and vice versa. Cooperation with Pakistan on these issues is a priority for the government and law enforcement and the UK fully supports the work of the FATF in this area. In March 2017, the UK signed new agreements with Pakistan to enhance cooperation on a number of security and home affairs priorities, including on criminal finances. Progress will be reviewed on an annual basis.

2.31 Nigeria is estimated to be the largest recipient of UK remittances, with World Bank data suggesting $3.8 billion was remitted from the UK in 2014. The bilateral remittance corridor leads to a risk of proceeds from predicate offences including drugs trafficking and illicit goods smuggling being laundered through the UK, in addition to the risk of corruption proceeds being invested in UK assets such as property. Anti-corruption is a priority for the Nigerian Government; Nigeria has made significant progress in strengthening its anti-money laundering regime and is no longer subject to

the FATF's monitoring process. In 2016, the UK signed an MOU with the Nigerian Federal Government to facilitate the swift return of corrupt assets to Nigeria. The MOU makes provision for transparency, monitoring and accountability in the return of any assets to Nigeria to minimise any risk of them being re-corrupted, and anticipates that they will be used for projects to benefit Nigeria's poor and improve access to justice. The UK is working with Nigeria to develop its capability to disrupt and prosecute serious and organised crime.

International financial centres

2.32 As global hubs for trade, a number of international financial centres share a similar range of money laundering threats to London and find themselves at particular risk of being used as destinations or transit points for the proceeds of crime.

2.33 The UAE, as a major financial hub for the Middle East, is an attractive regional centre for legitimate business activity while also being exposed to risks from money laundering. UK criminals have been identified as laundering assets to and through the UAE, with particular risks around trade based and cash-based money laundering. These issues underline the importance of the growing cooperation between UK and UAE law enforcement. In recent years, this has resulted in the repatriation of £580,000 of criminal proceeds under the UK-UAE Mutual Legal Assistance Treaty and the deportation of a known UK tax fraudster from the UAE in 2017. A joint Proceeds of Crime Conference held in Abu Dhabi in September 2016 underlines political commitment to this cooperation on both sides. The UK FCA also engages bilaterally with the UAE Central Bank and the Dubai Financial Services Authority in its supervisory and enforcement activities.

2.34 Hong Kong, as a financial gateway into and out of mainland China and a location of significant business activity by UK companies, is an important partner for the UK in tackling the threat of illicit transactions. The UK is working with Hong Kong to deliver mutually beneficial cooperation in a number of areas. In launching the Fraud and Money-Laundering Intelligence Taskforce in 2017 (on the model of the UK's Joint Money-Laundering Intelligence Taskforce), Hong Kong has reiterated its commitment to global efforts to tackle money-laundering. In addition to this, Hong Kong has introduced a number of new measures to improve financial transparency in line with international standards, including concluding bilateral agreements between the FCA and the Hong Kong Monetary Authority.

Chapter 3
Terrorist financing threat

Threat from international terrorism

3.1 The threat to the UK from international terrorism continues to be assessed as 'severe', which means an attack is highly likely (it was briefly raised to 'critical' in May 2017 following the Manchester Arena bombing and in September 2017 following the Parsons Green bombing). Terrorist groups in Syria and Iraq, including Al Qaida and Daesh, possess both the intention and the capability to direct attacks against the West. The UK is a high-priority target for Islamist extremists and they pose a significant threat to the UK, including interests and citizens abroad. Despite the current main focus on terrorism originating from Syria and Iraq, the threat of terrorism also emanates from other parts of the Middle East and regions such as North, East and West Africa, and South and South East Asia. The geographic threat picture remains largely similar to 2015, although the fall of Mosul and subsequent victories against Daesh are reducing their territorial footprint.

3.2 However, the majority of terrorist attack plots in this country have been planned by British residents, the largest of which were the 7/7 bombings and more recently the May 2017 Manchester Arena bombing. Low complexity attacks by lone actor UK-based extremists have also increased and are inherently harder to detect than more complex and ambitious plots, as demonstrated by the further attacks in London in 2017.

3.3 Unlike most other criminals, the raising and moving of funds is not a terrorist's primary aim. Instead, these funds are used to support terrorist groups or finance attacks. The UK does not typically see large scale coordinating fundraising activity for terrorist groups. Recent terrorist attacks across Europe have demonstrated that the costs involved can be very low; for example, as low as hiring or stealing a vehicle or purchasing knives. Nevertheless, tackling financial activity and making use of financial intelligence continues to be a heavily utilised and hugely valuable tool for law enforcement.

3.4 Terrorist financing activity in the UK is varied, but usually low-level. Small amounts of funds, which are difficult to detect, are raised by UK-based individuals predominantly to send to associates abroad located with terrorist groups, to fund their own travel to join terrorist groups, or to fund their own attack plan aspirations. Terrorists and their supporters employ a variety of methods to raise and move terrorist funds, looking to any means at their disposal to do so.

3.5 Methods used to raise funds include legitimate means, self-funding, fraud or other proceeds of crime.[1] Methods used to move funds include the use of MSBs and carrying cash out of the country. No one method appears to be more prevalent than others; rather, the choice of method is assessed to be dependent on personal knowledge or end destination of funds. These methods are discussed in more detail in subsequent chapters, with particular relevance to the chapters on financial services, financial technology, cash, MSBs and NPOs.

3.6 Tackling terrorism and terrorist financing at home and abroad through CONTEST (the UK's Counter-Terrorism Strategy) is one of UK's priorities under the National Security Objectives set out in the UK's National Security Strategy. The aim of CONTEST is to provide a stable strategic framework for tackling the terrorist threats the UK faces. There are four strands to CONTEST which provide a framework for all UK counter-terrorism activity. These are more commonly referred to as the 'Four Ps':

- Pursue: to stop terrorist attacks
- Prevent: to stop people becoming terrorists or supporting terrorism
- Protect: to strengthen our protections against a terrorist attack
- Prepare: to mitigate the impact of a terrorist attack

3.7 This strategy has provided the framework though which policy makers and operational partners have continued to refine and improve the UK's response to specific terrorist threats. For example, in response to the threat posed by Foreign Terrorist Fighters the UK government revised legislation to provide law enforcement agencies with the necessary powers to disrupt travel and prevent return, alongside specific measures to prevent insurance being used to fund ransom payments for terrorist kidnappings.

3.8 While the UK is not assessed to be exposed to large scale raising or transfer of funds for use by terrorist groups overseas, the risk of this happening globally continues to threaten the international fight against terrorist financing. The UK is an active member of the Global Coalition Against ISIL and the Counter ISIL Finance Group, taking part in upstream operations against both financial and non-financial targets At the July 2017 G20 summit, the Prime Minister highlighted the importance of combatting "safe spaces" for terrorist financing in the global financial system. The UK has urged G20 countries to increase their political and practical commitment to addressing these issues in order to deprive terrorist groups of their resources.

Threat from Northern Ireland related terrorism (NIRT)

3.9 The threat from Northern Ireland Related Terrorism (NIRT) is assessed as 'severe' in Northern Ireland and 'substantial' in Great Britain. It is driven by a small number of groups, who continue to pose an enduring threat. These groups aim to destabilise the framework for the peaceful settlement of Northern Ireland's future, as set out in the 1998 Belfast Agreement. As a

[1] Including online fraud, abuse of benefits and abuse of student loans.

result, terrorist financing threat in Northern Ireland is focused around the internal threat from Dissident Republicans (DRs).[2]

3.10 Following the signing of the Belfast Agreement the nature of terrorist financing changed, with paramilitaries and terrorist groups increasingly focusing on forms of organised crime; not all of this activity is specifically intended to raise funds for terrorism. DR groups in Northern Ireland (NI) undertake a range of activities which provide the platform for sustained violence, including using a range of methods to raise money. This includes cigarette smuggling, fuel laundering, extortion and robbery, benefit fraud and both legitimate and semi-legitimate business activity. In addition, overt fundraising through support and welfare groups focused on specific political issues is also used. The border also exposes Northern Ireland to money flowing to and from the Republic of Ireland. Most of these cross-border transactions take place in cash. The lines between raising finance for DR groups and personal gain are also often blurred.

3.11 Financial arrangements are not standardised within DR organisations, with different sub-groups and individuals receiving and controlling different portions of money. In larger, more professional DR groups there is judged to be a greater likelihood of centralised control over finance. This allows money to be distributed amongst personnel according to the aims of the organisation rather than in an ad hoc fashion dependent on an individual's geography or proximity to funding streams.

3.12 Finance is assessed to be crucial to DR groups, but they do not require significant amounts of money to sustain a campaign of violence. DR groups do require a regular income to cover running costs (such as car, fuel, other travel expenses, and legally acquired engineering components) and procure weapons to carry out attacks. DR groups do not necessarily have to purchase weapons as they either have, or are sometimes able to obtain, access to existing stockpiles. A willing volunteer with access to a rifle or handgun and ammunition can also carry out an attack with little financial cost to his or her organisation. In the long-term, when the replenishment of such items is necessary, it requires only relatively small amounts of money (generally less than £1,000) which is within the gift of most groups, most of the time.

3.13 The vague lines between organised crime and terrorist funding in Northern Ireland have dictated how law enforcement responds to the risks. As predicate offences often fall under the category of organised crime, the law enforcement response is more likely to address this activity through a proceeds of crime offence framework. In May 2016, the Fresh Start Panel report on the Disbandment of Paramilitary Groups in Northern Ireland reported that the scale of paramilitary activity has greatly reduced over the course of the peace process, though some individuals continue to engage in violence, intimidation and other criminal activities.[3]

---

2 DR groups currently operating in Northern Ireland are the new IRA, Oglaigh na h'Eireann (ONH), Continuity IRA (CIRA) and Arm na Poblachta (ANP).

3 'The Fresh Start Panel Report on the Disbandment of Paramilitary Groups in Northern Ireland', Fresh Start Panel, May 2016

Chapter 4
Financial services

Summary and risks

4.1 The UK financial services sector is a major global hub that attracts investment from across the world. However, its size and openness also make it attractive to criminals seeking to hide the proceeds of crime among the huge volumes of legitimate business. The 2015 NRA assessed the banking sector overall to be at high risk of money laundering and at medium risk of terrorist financing. It also identified gaps within law enforcement understanding, particularly in terms of high-end, complex money laundering, and poor information sharing between law enforcement and the banking sector. Since 2015, a number of steps have been taken to address these risks by government, law enforcement, the FCA and banks, in particular around embedding senior engagement with AML/CTF responsibilities within firms and ensuring that banks and law enforcement agencies are able to share intelligence with one another to tackle financial crime.

4.2 Overall, while these initiatives have started to result in improvements, the risk profile is not judged to have shifted substantially over recent years. The banking sector is still vulnerable to a wide range of money laundering methodologies, from basic retail banking services being exploited as an entry point for illicit funds from OCGs, through to the use of complex trading arrangements to obscure the origin of funds from overseas.

4.3 However, due to steps taken by law enforcement agencies, the FCA and firms to plug the intelligence gaps around high-end money laundering within financial services, we now have an increased understanding of the varying risk profiles across different parts of the sector. The 2017 NRA therefore provides separate assessments for retail banking, wholesale banking and capital markets, and wealth management.

4.4 Retail banks (those providing personal and business accounts, cash savings accounts and payment services) continue to be exposed to the highest volume of criminal activity out of all financial sectors. While controls are more developed in retail banking than other areas, the widespread criminal intent to exploit retail banking products and the increasing speed and volume of transactions mean that the sector remains at **high** risk of money laundering. The 2015 NRA identified the terrorist financing risk within the banking sector as medium. While the risk profile is not assessed to have shifted, when looking specifically at retail banking the terrorist financing risk is assessed to be **high** relative to other financial and non-financial sectors.

4.5 Wholesale banking (transactions between large institutions) and capital markets (raising and trading equity and debt and trading derivatives, currency and commodities) are assessed to be exposed to **high** risks of money laundering due to the known risks around correspondent banking, as well as the risks of large sums being laundered through capital markets and the relative lack of controls. There are however, significant intelligence gaps around the extent and nature of the risk around capital markets. While it is possible that international terrorist funds could or have transited through UK capital markets, no specific incidents of this taking place have been identified and the terrorist financing risk in this area is assessed to be **low**.

4.6 Wealth management and private banking (providing financial and investment advice and services, usually for high net worth individuals) are assessed to be exposed to **high** money laundering risks due to the sector's exposure to the proceeds of political corruption and tax evasion, and persisting regulatory concerns. There is no specific evidence of terrorists using this sector to store or transfer funds and the sector is assessed to be exposed to relatively **low** risks for terrorist financing.

Retail banking

4.7 As identified in the 2015 NRA, the universal nature of retail banking transactions, as well as the frequency and speed with which they are conducted, continue to make the sector vulnerable to money laundering and terrorist financing. The exceptionally high speed and volume of transactions in the sector can allow basic products to be abused, with banks often only able to act on this or report suspicions after transactions have gone through.

4.8 The 2015 NRA highlighted the interaction of the retail banking sector with illicit funds both in cash and electronic form. UK-based OCGs are still assessed to process cash in and out of bank accounts, including by using bank quick drop services, as a means of breaking the audit trail of transactions. Retail banking is assessed to be used to launder the proceeds of a wide range of predicate offences, presenting difficulties for detection and prevention due to the speed of money movement and the ability to withdraw funds in cash or transfer funds overseas.

4.9 In addition, insiders in financial institutions can aid the concealment of financial crime, including money laundering. In 2015, 153 organisations identified and recorded 585 confirmed insider frauds to Cifas.[1] Almost 50% of these cases have been identified as potentially involving money laundering. However, where concerns were raised about wrongdoing, 60% of those surveyed said their organisation's response was 'good' or 'excellent'. [2]

Money mules and mule accounts

4.10 In line with the 2015 NRA, UK-based OCGs are still assessed to cash proceeds into and out of bank accounts as a tool to break the audit trail of transactions. Law enforcement agencies view mule accounts, whereby illicit

[1] 'Employee Fraudscape 2016', Cifas, 2016

[2] 'Employee Fraudscape 2016', Cifas, 2016

funds are transferred either wittingly or not through a third party's account, as one of the primary ways through which the proceeds of cyber crime and fraud are laundered.

4.11 To recruit money mules, the NCA has identified criminals advertising fake jobs in newspapers and on the internet often targeting students or recent migrants. The mule will accept money into their bank account before following further instructions on what to do with the funds. Instructions can include transferring the money into a separate specified account or withdrawing the cash and forwarding it on via MSBs.

Box 4.A: Money mules

Case study: Following a money laundering and fraud investigation, a number of people were arrested on suspicion of money laundering. It was discovered that a suspect was contacting vulnerable repeat victims of fraud and persuading them to transfer money into the accounts of money mules, claiming that if they did so they would be able to recover previous losses from investment frauds. Victims' losses from this scheme were estimated to be in the region of £800,000. Enquiries are ongoing.

Alternative banking platforms

4.12 HMRC continues to see the use of alternative banking platforms (ABPs) to conceal money movements in trading fraud. ABPs are a form of shadow banking which makes use of bespoke online software to provide banking services without regulated and audited due diligence checks. HMRC assesses ABPs to pose a significant risk due to the scale of transactions going through them. Internal transactions within an ABP are outside of the regulated banking sector and are therefore difficult for law enforcement agencies and financial institutions to identify.

Box 4.B: Alternative banking platforms

Case study: During a trading fraud, goods originating in the EU were sold into the UK market through a series of fraudulent UK companies in order to avoid paying VAT. Large payments were made by the fraudulent UK companies into an ABP registered in Hong Kong, but with a bank account based in Montenegro. The ABP was used to disguise the ultimate beneficiary of these payments.

Trade-based money laundering

4.13 The FATF defines trade-based money laundering (TBML) as money laundering through the use of trade transactions. Recent work, including by the JMLIT, has suggested that the most common form of TBML to which UK banks are exposed is through the abuse of the open account third party payments system. This is the process by which sellers extend credit to purchasers and ship goods in advance of payment. Third parties can then

make payments to the seller to settle the open account debts, providing a risk of these debts being settled using illicit funds. In addition, banks can be exposed to money-laundering through documentary trade finance, whereby fraudulent documents are used to launder funds through the trade system.

Terrorist financing

4.14 Terrorist financing activity in the UK is usually limited to the activity of UK-based individuals raising low amounts of money to fund a terrorist attack, to fund their personal expenditure, to travel to conflict zones (such as Syria) or to send low amounts of funds to associates located overseas with terrorist groups. Due to the widespread use of retail banking in low-level financial activity, retail banking is assessed to be one of the primary means used to move and store these funds within the UK.

4.15 Terrorists in the UK often operate alone, using small amounts of money (often below £300). Personal bank accounts are often used to transfer funds abroad or between individuals, as well as to make purchases related to terrorist activity such as travel tickets to Syria or weapons. It is often difficult for financial institutions and law enforcement agencies to identify these transactions as suspicious due to the lack of any obvious indicators to highlight suspicious activity on the account.

4.16 As well as retail banking being used to move terrorist funds, it can also be used to raise funds. As highlighted in the 2015 NRA, one means through which terrorists have been observed to raise funds is through card fraud or loan fraud, whereby individuals may falsely claim to have been defrauded (on the expectation that their bank will reimburse them) or where individuals apply for a loan under false pretences.

Wholesale banking and capital markets

Money laundering through markets

4.17 There is a significant emerging risk of money being laundered through capital markets. The FCA sees this as an emerging risk, potentially extending beyond recent high profile cases, cases due to the complexity of many of the activities involved, the cross-border nature of the market and the relative lack of compliance controls.

4.18 In general, the FCA sees banks taking positive approaches towards wholesale banking. However, the risk around poor controls is evidenced by the fine imposed by the FCA against Deutsche Bank in 2017, its largest ever fine for AML/CTF, as set out in the case study below.

4.19 Greater complexities have been identified in relation to capital markets since the 2015 NRA. There is a particular concern about the use of capital markets to facilitate high-end money laundering, which usually involves the laundering of the proceeds of major frauds and serious corruption, transactions of substantial value and the services of skilled professionals. While our understanding of the risks of money laundering though markets has developed significantly since 2015, the scale and extent of this risk remain an intelligence gap. The FCA and UK law enforcement agencies

continue to work together, engaging with international partners, to maintain an up-to-date picture of these risks.

Box 4.C: Money laundering through markets

Case study: In early 2015, Deutsche Bank notified the FCA of concerns regarding its AML framework following an internal investigation into suspicious securities trading involving DB Moscow (its Russia-based subsidiary). These transactions involved 'mirror trades' by customers of the London office and DB Moscow to transfer an amount estimated to be over $10 billion from Russia, through the UK, into bank accounts in Cyprus, Estonia and Latvia. Between 2012 and 2015, the customer in Moscow bought securities from DB Moscow while a related non-Russian customer in London sold the same number of the same securities to the London office for US dollars. The way these trades were conducted, in combination with their scale and volume, was assessed to be highly suggestive of financial crime, and in January 2017 the FCA imposed a fine of around £163 million against the bank. The failings indicated widespread deficiencies in the bank's AML control framework, though the bank is committing significant resources to undertaking remedial action and to improving its controls.

Correspondent banking

4.20 The vulnerabilities for wholesale banking identified in the 2015 NRA were largely around correspondent banking and trade finance. Correspondent banking continues to pose a risk for banks due to the complex and international nature of many of the relationships involved. Banks' risk appetites for correspondent relationships has decreased in recent years, leading to de-risking. While this has decreased the risk profile for the banks involved, the trend may pose wider risks by shifting correspondent relationships to those banks or jurisdictions with weaker compliance. The UK has been at the forefront of international efforts to address this issue, including through the Financial Stability Board and the G20. In April 2015, the FCA published a statement clarifying its regulatory expectations around banks' approaches to risk and stating that "effective money-laundering risk management need not result in wholesale de-risking".[3]

Wealth management and private banking

4.21 The UK wealth management industry manages over £800 billion of wealth for clients across the globe.[4] The 2015 NRA highlighted the vulnerabilities posed by the complexity of wealth management and private banking services, including potentially high risk formation of trusts and companies. These vulnerabilities can be exacerbated by the use of professional intermediaries and the level of anonymity within the sector.

4.22 The 2015 NRA also identified issues within the sector around client risk assessment and enhanced due diligence (EDD). The FCA still sees examples of

3 'De-risking: managing money-laundering risk', FCA, February 2016

4 'Industry Statistics', PIMFA, 2017

ineffective AML systems and controls in some parts of the sector, including cases of poor management of high risk customers. Through consultation undertaken for this assessment, firms in the sector identified particular vulnerabilities around: the inward transfer of assets already being managed by another wealth manager; the provision of execution only brokerage services; corporate vehicles and structures designed to mask beneficial ownership; third party payments into client accounts; and funds being drip fed into an existing portfolio.

Box 4.D: Wealth management

Case study: In 2011, the Financial Services Authority (FSA) conducted a thematic review of how banks were managing money laundering risk in higher risk situations. As part of that review the FSA visited EFG, a UK subsidiary of a global private banking group. The review and further investigation found that the bank had not fully put its AML policies into practice. Of 36 customer files reviewed by the FSA, 17 highlighted significant money laundering risks without sufficient records of how the bank had mitigated these risks. These included 13 files where risks related to corruption, money laundering or other criminal activity. In 2013, the FSA fined EFG £4.2 million for failing to take reasonable care to establish and maintain effective AML systems and controls in relation to higher risk customers.

Politically exposed persons (PEPs)

4.23 Wealth management and private banking firms are judged to be particularly exposed to the risk of being used to launder the proceeds of overseas corruption. The 2015 NRA highlighted ongoing FCA concerns around firms' approaches to higher risk PEPs. To mitigate these risks, the MLRs require firms to apply EDD to PEPs, their family members and their known close associates. However, concern has been raised about the disproportionate application of enhanced measures to lower risk PEPs. The MLRs and guidance therefore require firms to apply enhanced measures in a risk-sensitive way, so that lower risk PEPs are subjected to less intrusive and exhaustive measures than higher risk ones.

4.24 Firms assess the risks from PEPs to be particularly acute in cases where a customer has held a prominent public function in a high-risk third country. In view of recent guidance from the FCA, PEPs who hold prominent public functions in the UK (and their family members and known close associates) should generally be treated as lower risk due to the anti-corruption regime in place in the UK. However, firms are still required to apply more stringent approaches in cases of higher risks, including in relation to PEPs from countries without such regimes in place.

4.25 Investor visa regimes around the world, including the UK's, have been identified as representing a potential avenue for the laundering of the proceeds of corruption.[5] The government has a number of measures in place to reduce the scope for abuse of the UK scheme, including powers to refuse

[5] 'Action plan for anti-money laundering and counter-terrorist finance', HM Treasury and Home Office, April 2016

applications where the applicant is not in control of the funds relevant to their application, where the funds were obtained unlawfully or where there are concerns around a third party providing the funds. In 2015, the government made a change to require that applicants must have opened a UK bank account with an FCA regulated bank for the purposes of making their qualified investment. This measure ensures that prospective applicants will have been subjected to suitable levels of due diligence and the UK's AML/CTF regime before gaining a visa through the route.

Insurance

4.26 As highlighted in the 2015 NRA, the FATF has identified the life insurance sector as at risk of money laundering and terrorist financing. The 2015 NRA flagged that the sector is a known target for fraud, and that Kidnap for Ransom is a known issue from a terrorist financing perspective, but that the level of known money laundering or terrorist financing risk was limited. The FCA assesses there to be risks given the global nature of the London market, but that firms have suitable controls to deal with these risks. Relative to other sectors, the insurance sector in the UK is assessed to be low risk for both money laundering and terrorist financing.

Supervision, compliance and law enforcement response

Supervision and compliance

4.27 The FCA has a key role in creating a hostile environment for criminal money by ensuring financial services firms have adequate safeguards to prevent themselves from being used for financial crime, in particular money laundering. Most banks recognise the importance of strong AML/CTF controls, and the British Bankers' Association (now UK Finance) has estimated that banks spend £5 billion annually on compliance (including CDD, transaction monitoring, sanctions and fraud risk).[6]

4.28 The 2015 NRA highlighted the most common issues in terms of banks' compliance as inadequate governance structures, inadequate risk assessment process, poor IT systems, poor management of transaction alerts, poor identification of source of funds, and poor management of foreign PEPs and correspondent banks. These vulnerabilities in control weaknesses persist, though the FCA recognises the steps the industry is taking to manage most risks as positive and moving in the right direction.

4.29 Common issues the FCA has seen since 2015 have been weaknesses in governance, and longstanding and significant underinvestment in resourcing. This underinvestment may affect the infrastructure underpinning firms' controls, such as transaction monitoring IT systems that are not kept up to date. Managing complex legacy systems remains a challenge for a number of firms, but the FCA is seeing continuing improvements.

4.30 In the course of the FCA's supervision it has seen many firms engaging in extensive remedial programmes, supported by a much clearer tone from the

[6] Written evidence submitted by the British Banking Association on the Criminal Finances Bill, 2016

top on the importance of managing financial crime risk with better understanding by senior management of what is needed to manage risks. The Senior Managers and Certification Regime (SM&CR), adopted in 2016, introduced a prescribed senior management responsibility within a firm for financial crime and is expected to improve senior management engagement further within firms. The SM&CR currently applies to firms that take deposits and the largest investment firms.[7] However, from 2018 the SM&CR will be extended across all FCA regulated sectors. The FCA's new annual financial crime return, introduced at the end of 2016, should further assist the FCA in supervising firms and assessing emerging risks by providing better data on the inherent risks to which firms are exposed.[8]

4.31 Many of the controls financial services firms employ in relation to terrorist financing overlap with their AML measures, covering for example, risk assessment, CDD checks, transaction monitoring, escalation of suspicions and liaison with the authorities. The FCA's assessment of firms' approach to CTF is positive, with effective cooperation in place between compliance staff and law enforcement agencies to prevent or respond to terrorist attacks. The partnership between the banking sector and law enforcement is vital in limiting abuse of the financial system by terrorists and criminals and the JMLIT provides an effective mechanism for the banking sector to be able to work with law enforcement in line with their regulatory requirements.

Law enforcement response

4.32 The law enforcement response to the risks in the financial services sector is characterised by:

- development of intelligence on and investigation of the criminal entities involved
- working with the financial sector to enable Information sharing to improve threat assessments and the development of intelligence to target and disrupt criminal activity
- engagement with international partners to deliver upstream interventions aimed at tackling predicate offending
- taking innovative approaches to the restraint and recovery of criminal assets
- working with other organisations including supervisors to deliver a range of non-judicial disruptions
- working with the regulated sector to improve its assessment of the threat in terms of the money laundering typologies involved

4.33 SARs are one of the primary means of sharing information to produce intelligence. Banks continue to report by far the greatest number of SARs of any reporting sector (submitting 83% of all SARs in 2015/16) with 348,688

[7] The Bank of England operates a parallel regime – the Senior Insurance Managers Regime (SIMR) – for certain senior personnel of insurance companies.

[8] 'FCA anti-money laundering annual report 2016/17', FCA, 2017

SARs submitted by banks in 2015/16. This number has increased year on year since 2007.[9] The NCA has recently worked to clarify understanding of the provisions around DAML SARs to ensure that their use has the greatest impact against threats.

4.34 The 2015 NRA highlighted banks' concerns about poor information sharing between the sector and law enforcement. The government's 2016 AML and CTF action plan responded to these risks through committing to put the JMLIT onto a permanent footing. This has now been completed, including through the establishment of six expert working groups.[10]

4.35 The JMLIT has been key in delivering improved prioritisation of risks by financial institutions and several targeted interventions to disrupt criminal activity. From its inception in 2015 until July 2017, a total of 306 intelligence requests have been submitted to the JMLIT. As a result of this activity, 96 new court orders have been granted, with approximately £8.5 million subsequently restrained, while a total of 88 arrests have been made. Over 650 bank accounts have been closed, disrupting criminal activity and denying criminals the ability to launder the proceeds of their activity. More than 2,100 new bank-led investigations of suspected money laundering activity were initiated to the mutual benefit of public and private sectors. The bank led investigations have also fed into 22 industry alerts issued by the JMLIT expert working groups.

4.36 The public-private partnership will be further enhanced by new provisions in the CFA, creating a legal gateway to allow firms to share information with one another and to submit joint SARs. This will provide law enforcement agencies with a fuller picture of complex and high-end money laundering, and will allow for further opportunities to disrupt and deter criminal and terrorist activity.

4.37 The CFA also creates new civil powers for law enforcement to seize and forfeit funds held in bank accounts where there is reasonable suspicion that it is the proceeds of crime, or will be used in unlawful conduct.

9 'Suspicious Activity Reports (SARs) Annual Report 2017', NCA, October 2017

10 These expert groups are: trade-based money laundering; terrorist financing; modern slavery, human trafficking and organised immigration crime; money laundering through markets; bribery and corruption; and future threats.

Chapter 5

Financial technology

Summary and risks

5.1 Financial technology ('FinTech') includes a wide range of products and services which apply emerging technological solutions to financial services. The products covered here are those currently considered most relevant from the perspective of money laundering and terrorist financing: e-money, digital currencies and crowdfunding. The rapidly developing nature of products and services in this sector puts an imperative on the ability for government, supervisors, firms and law enforcement to respond rapidly to both the opportunities and risks which they pose.

5.2 The 2015 NRA assessed the risks around e-money to be medium for money laundering and low for terrorist financing. Due to the controls in place and the limited scope to use e-money to launder large sums of money (as evidenced by the few known cases of abuse), the money laundering risks associated with e-money are still assessed to be medium. For terrorist financing, the increased evidence of terrorists' intent to use e-money cards as a medium to transfer funds across borders leads to an assessment that e-money has increased to medium risk. The MLRs reduce the thresholds above which CDD must be applied, mitigating the risks of abuse.

5.3 In 2015, the risks associated with digital currencies were assessed to be low for both money laundering and terrorist financing. There remains little evidence of digital currencies being used as an established tool for money laundering, and the money laundering risk is therefore still assessed to be low. However, the link between digital currencies and cyber-enabled crime means that this risk is likely to increase. While digital currencies could in theory be used to facilitate and finance terrorist activity, the lack of evidence of this occurring and the greater attractiveness of other methods mean that digital currencies continue to be assessed as low risk for terrorist financing.

E-money

5.4 The UK has the highest concentration of e-money issuers in the EU, with 103 authorised e-money firms and 21 small e-money institutions listed on the FCA Register.[1] As highlighted in the 2015 NRA, 'open loop' prepaid cards have the potential to become high risk because of the anonymity they can provide, the ease of transportation and vulnerabilities in law enforcement

[1] As of 28 March 2017

agencies' ability to respond.[2] However, they may not be attractive to criminals or terrorist financiers because of the maximum amount which can be stored electronically each month, the maximum limit on monthly payment transactions, the cash withdrawal limit and costs attached to using the cards in ATMs in the UK and abroad. In addition, AML/CTF controls are complemented in many cases by fraud prevention and consumer protection controls implemented by issuers.

Money laundering

5.5 The 2015 NRA found that many of the vulnerabilities around e-money remained theoretical, and that there was an intelligence gap around exploitation of the sector. Since 2015, law enforcement and the FCA have taken steps to gather evidence of their exploitation. This has included cases where e-money institutions, their agents or their e-money products have been used to facilitate money laundering, including examples where e-money institutions have transferred money obtained from overseas criminality into a UK bank account and where prepaid cards have been used to launder the proceeds of crime. Law enforcement agencies have also seen the use of 'twin' cards used to launder proceeds between two countries. The FCA, as one of its priorities for 2017/18, is currently conducting a thematic review on the e-money sector, which should further explore these risks and firms' abilities to mitigate them.

Box 5.A: Money laundering through e-money

Case study: An OCG has used prepaid cards to make purchases of tobacco in Belgium and Luxembourg. This tobacco is subsequently smuggled to the UK via parcel post. The OCG tops up the prepaid card in the UK, using criminal funds from UK bank accounts to transfer balance onto the card. The funds on the card are then used in Belgium and Luxembourg to purchase tobacco.

Terrorist financing

5.6 The 2015 NRA assessed the terrorist financing risk associated with e-money, and specifically prepaid cards, as low. There remains little evidence of prepaid cards being widely used by terrorists to store and move funds. However, prepaid cards have been observed being used to move terrorist funds out of the UK, and were used in preparation for the November 2015 Paris attacks. Prepaid cards remain a potential method for moving terrorist funds or for purchasing weapons or precursors, in particular due to their lower physical bulk than cash. However, prepaid cards as a substitute for cash are judged to be less attractive in the case of terrorist financing than in money laundering; while money launderers are attracted to cards' compactness relative to cash, terrorist financing typically involves lower amounts and therefore a lower cash bulk.

[2] Open loop cards are those which can be used anywhere the card network is accepted, rather than at just one retailer or one set of retailers.

Digital currencies

5.7 The vulnerabilities identified in the 2015 NRA were largely around the anonymity and cross-border exposure of digital currencies, as well as the lack of interaction with the regulated sector. Digital currencies have only become marginally more mainstream since 2015, but the market is diversifying and growing with other currencies (many of which have enhanced anonymity) taking market share from the historically dominant Bitcoin.[3]

Money laundering

5.8 The NCA has assessed the risk of digital currency use for money laundering to be relatively low; although NCA deems it likely that digital currencies are being used to launder low amounts at high volume, there is little evidence of them being used to launder large amounts of money.

5.9 By contrast, from a cyber crime perspective, the threat posed by digital currencies is higher, owing to their role in directly enabling cyber-dependent crime. This is evident in three areas: firstly, digital currencies directly facilitate victim payments to cyber criminals. This includes malware attacks such as ransomware, and cyber crimes-as-an-extortion, in which victim ransom payments are predominantly requested to be paid in Bitcoin. Secondly, digital currencies aid the growth of cyber crime-as-a-service. They constitute the primary method of payment for criminal-to-criminal payments and for the purchase of illicit tools or services sold online in the cyber criminal marketplace. The ease with which such tools can be bought through digital currencies lowers the barrier to entry for low-sophistication cyber criminals, directly contributing to the growth of cyber-crime-as-a-service. Thirdly, digital currencies play a vital role in laundering the proceeds of cyber-dependent crime, directly facilitating cyber criminal financial flows.

5.10 Analysis of SARs submitted between May 2016 and July 2017 highlighted 1,584 referring to digital currencies, with the number of reports increasing month-on-month. Of these SARs, a number indicated that the suspicion was raised because of the involvement of digital currencies, rather than any suspicion of money laundering or terrorist financing. The reporting and detection of suspicious activity is likely to increase when exchanges and custodian wallet providers become regulated through the EU Fifth Anti-Money Laundering Directive (5MLD), as outlined below.

5.11 These risks are expected to grow as digital currencies become an increasingly viable and popular payment method. As the number of businesses accepting digital currency payments grows, there is an increasing risk of criminals using the currencies to launder funds without needing to cash out into non-digital, or 'fiat' currencies.

Terrorist financing

5.12 The 2015 NRA assessed that digital currencies are not typically a method with which terrorists move funds in or out of the UK. As with money laundering, the scope for terrorist financing to occur through digital

[3] Between March 2017 and July 2017, Bitcoin market share fell from around 80% to under 50%.

currencies has so far been limited by their lack of widespread use. The use of digital currencies to buy and sell illicit goods more widely may mean that digital currencies may be used in order to purchase items which could be used in an act of terror (such as firearms) or used to fund an act of terror (such as stolen card details), but there is no evidence of this occurring to date in the UK. Terrorist use of digital currencies is assessed to be unlikely to increase significantly in the next five years.

Crowdfunding

5.13 The main categories of crowdfunding are: donation or reward platforms; investment, equity or debt platforms; and loan-based or peer-to-peer platforms. The 2015 NRA did not consider crowdfunding. Economic crime risks have been identified where platforms can be used to launder money, while other crowdfunding activities could facilitate fraud. From 14 November 2013 to 25 October 2015, there were estimated to have been 24 SARs relating to crowdfunding. For the majority, the reference to crowdfunding was contextual and not the subject of the suspicion. Crowdfunding, in particular peer to peer lending or donation sites, also has the potential to be used as a terrorist financing tool, though this has not been observed to date in the UK.

Supervision, compliance and law enforcement response

5.14 The 2015 NRA reported that supervision of e-money was challenging due to cross-border business models and the rapid development of the sector. In addition, complex business models, including 'white label' products and secondary cards, can result in weakened AML/CTF controls. So far there has been no specific enforcement action by the FCA for breaches of AML/CTF requirements by e-money institutions. Law enforcement agencies also face challenges in identifying the ownership and value of prepaid cards at the point of detection. However, this anonymity is limited by the electronic record of card activity: every transaction is traced to the point of use, and industry have invested heavily in the creation and continual improvement of transaction monitoring systems to prevent fraud and money laundering. The MLRs represent a significant tightening of the regulation of e-money. The MLRs lower the thresholds at which due diligence should be applied to prepaid cards and exempt e-money products from certain due diligence measures only when an appropriate risk assessment demonstrates that a strict set of conditions is met.

5.15 In November 2014, the government published a call for information to gather evidence on the regulation of digital currencies. In March 2015, the government published its response, highlighting the key benefits and risks associated with digital currencies and setting out policies to help mitigate risks and maximise the benefits of the sector. The government announced at this point that it would look to bring digital currencies within scope of the AML/CTF regime. The UK therefore supports the intention behind bringing digital currency exchange firms and custodian wallet providers into AML/CTF regulation as part of 5MLD, in line with the risk-based approach that FATF standards require. The government's call for information concluded that

greater use of horizon scanning and investment in research and training will be needed to augment law enforcement agencies' ability to mitigate the threat, including taking advantage of the opportunities offered by the blockchain ledger to tackle digital currency risks proactively. The Home Office leads a multi-agency group focused on digital currencies, seeking to address these knowledge and skills gaps across law enforcement.

5.16 More broadly, FinTech also offers opportunities for mitigating financial crime if applied correctly. One example of this is the FCA's regulatory sandbox platform, launched in 2014. It allows FinTech firms to test innovative products, services, business models and delivery mechanisms in a live regulatory environment. The aim is to provide innovators, large or small, with a 'safe space' where businesses can test innovative products, services, business models and delivery mechanisms while maintaining the same standards of AML/CTF regulations.

5.17 Many applications to the FCA's sandbox have been from businesses with new ideas about RegTech, a sub-set of FinTech that focuses on technologies that may facilitate the delivery of regulatory requirements more efficiently and effectively than existing capabilities. Implementation of existing solutions has so far been seen to be constrained by the current legal framework around reliance, as well as wider technological and operational challenges faced by banks around incorporating these alongside older legacy systems. However, RegTech may help regulated firms mitigate risks going forward, including alleviating the difficulties firms face in verifying customer information.

Chapter 6

Accountancy services

Summary and risks

6.1 The 2015 NRA assessed the key risks around the accountancy sector to be: complicit accountancy professionals facilitating money laundering; collusion with other parts of the regulated sector; coerced professionals targeted by criminals; creation of structures and vehicles that enable money laundering; provision of false accounts; failure to identify suspicion and submit SARs; and mixed standards of regulatory compliance with relatively low barriers to entry for some parts of the sector.

6.2 Accountancy services remain attractive to criminals due to the ability to use them to gain legitimacy, create corporate structures or transfer value. While the 2015 NRA identified intelligence gaps around the role of professionals in high-end money laundering, recent work by law enforcement has helped significantly to develop our understanding of this area. Some of those accountants involved in money laundering cases are assessed to be complicit or wilfully blind to money laundering risks, though the majority of these cases are likely to involve criminal exploitation of negligent or unwitting professionals.

6.3 The 2015 NRA assessed accountancy services to be at high risk of exploitation for money laundering. The inherent risks and vulnerabilities of accountancy services remain due to the value of these services to those engaging in high-end money laundering, and these services remain prevalent in cases identified by law enforcement, though there are strict controls in place in certain areas. There is therefore still assessed to be a **high** risk of money laundering for accountancy services. Accountancy services are not judged to be attractive for terrorist financing, and there is no specific evidence of these services being abused by terrorists, so the terrorist financing risk associated with the sector is assessed to be **low**.

6.4 Accountants can be engaged in a range of activities and services and can be supervised by various bodies. Recent work by law enforcement has helped to identify in greater detail those services at greatest risk of being exploited. In 2016, the UKFIU reported that the most common areas identified by SARs were the creation and operation of companies, facilitating financial transactions (including through client accounts) and tax evasion. These areas are judged as being at highest risk of being exploited for money laundering.

Law enforcement agencies assess the highest risk situations to be those where a combination of these services is provided.[1]

6.5 The 2015 NRA reported that in 2014 there were over 23,000 firms carrying out accounting, bookkeeping and auditing activities and tax consultancy in the UK. In 2016 this figure was over 24,000, with 87% employing less than ten employees.[2]

6.6 The term 'accountant' is not a protected term, and qualifications are not required to offer accountancy services. Both professional body supervised and HMRC supervised accountants may have a variety of qualifications, though HMRC also supervises a greater proportion of accountants without qualifications. It is not possible to clearly delineate distinct risk profiles along these lines. Overall, investigations feature cases where money laundering has been facilitated by a range of both professional body supervised and other accountants, though some national agencies currently only have investigations focusing on professional body supervised accountants. Law enforcement agencies assess that accountants with professional body status are attractive for those seeking to engage in high-end money laundering due to the credibility that their services can confer.

Company formation and termination

6.7 The involvement of accountants in company formation and other company services, whether in the UK or overseas, is assessed to be the accountancy service at highest risk of exploitation. Company formation continues to be exploited by criminals to mask the ownership of assets or transfer these assets between persons. Company formation services are assessed to pose higher risks when offered by accountants than when offered by specialised company formation agents, as criminals may also access and exploit the accountant's wider services. These risks apply to a select group of accountants, with under 25% of those accountancy firms supervised under the MLRs estimated to provide trust or company services (ranging from company formation, company secretarial services and registered office services).[3] These services are estimated to be offered by a greater proportion of professional body supervised accountants than HMRC supervised accountants.

[1] The largest accountancy firms provide the full range of services, though are generally assessed to have mature controls in place including through division of responsibility within the firm. Smaller firms which nonetheless provide a range of services are assessed to remain at high risk.

[2] 'Business population estimates 2016', Office for National Statistics, October 2016

[3] Precise proportions cannot currently be calculated as some supervisors do not record whether their members conduct TCSP activities.

Box 6.A: Accountancy services and company formation

Case study: A professional body supervised accountant was a joint director of a UK-registered company, together with a Russian national. Using this company, the accountant established structures to move over $60 million through jurisdictions including Russia, Cyprus, Latvia, the Czech Republic and the British Virgin Islands. The stated purpose of the company was to provide high-end leisure services. The accountant and their co-director intended to use the company and associated company structures to provide money laundering opportunities to sanctioned individuals in Russia, and more generally to assist illicit asset movement from Russia.

6.8 Company liquidation and associated services (including insolvency practice, which may be conducted by certain accountancy professionals) also pose a risk of criminals masking the audit trail of money laundered through a company and transferring the proceeds of crime. The scope for abuse of insolvency services is mitigated to some extent by the licensing of practitioners, the strict set of obligations through the Insolvency Act and recent changes through the Small Business, Enterprise and Employment Act 2015. However, there remains evidence of insolvency and wider company liquidation services being abused.

Box 6.B: Accountancy services and company liquidation

Case study: A substantial food manufacturing company was acquired by individuals connected to an OCG through abuse of insolvency procedures. The company was acquired, through the assistance of a professional body supervised accountant, using funds from suspicious sources involving creditor write-offs exceeding £1 million. Once acquired, the company was suspected of being used to launder criminal cash. There was evidence indicating that the company was managing large sums of cash on-site using two distinct safes in a manner that supported this suspicion. The accountant was subsequently expelled as a member by the relevant professional body supervisor in respect of matters arising from this acquisition.

False accounting

6.9 Accountancy services have also been exploited to provide a veneer of legitimacy to falsified accounts or documents used to conceal the source of funds. For example, law enforcement agencies have observed accountants reviewing and signing off accounts for businesses engaged in criminality, thereby facilitating the laundering of the proceeds. In many cases accounts have been falsified by criminals and unwittingly signed off by accountants, while in others accountants have been assessed to be complicit.

6.10 The risk of false accounting can arise in relation to both high-end and cash-based money laundering, with accountants involved in the account preparation or review processes for both small and large businesses. Some

services, such as audit, are assessed in general to be at lower risk of exploitation because of a strict set of statutory obligations and the small group of registered practitioners who offer the service. For smaller companies, criminals may seek an accountant to sign off their accounts to fulfil reporting requirements imposed by their bank or by Companies House.

Box 6.C: False accounting

Case Study: A multi-million pound fraud was conducted through the selling of unregulated self-invested personal pension products to UK investors. Within this main fraud, a smaller, sub-fraud was perpetrated using a double invoice scheme to enable one UK based sales agent to take a 65% commission from each investment to allow the payment of pension 'cash-back' to certain investors. A professional-body supervised accountant, responsible for the company's accounts and payroll, routinely signed off duplicate invoice payments to UK and overseas bank accounts in the name of that sales agent and of an off-shore sales agent under a false identity. In reality, the off-shore sales agent was in fact the UK based sales agent, and the off-shore company and account belonged to the UK based sales agent. The accountant also set up the payments of false invoices into the suspect company director's overseas bank accounts, some of which were then paid into the accountant's personal UK bank account. The case uncovered serious accounting irregularities within the company. The company director, the chief commercial officer and the chief executive were convicted of conspiracy to commit fraud, conspiracy to furnish false information, fraudulent trading and offences under the Bribery Act 2010, though the accountant himself was ultimately acquitted. As such this case demonstrates the risk of accountants being exploited by others to enable the illicit movement of money.

Misuse of client accounts

6.11 Law enforcement agencies have observed misuse of accountants' client accounts for money laundering. There is a risk posed by accountants performing high value financial transactions for clients with no clear business rationale to be involved, allowing criminals to transfer funds through bank accounts with little scrutiny as a means to complicate the audit trail. Most accountancy firms rarely hold client money, and most supervisors have strict rules in place around the use of client accounts in addition to the MLRs. For example, several supervisors introduced new regulations in 2017 to ensure that firms' client accounts are only used in relation to relevant accountancy services.

Box 6.D: Misuse of accountants' client accounts

Case study: In the case of a multi-million pound investment fraud, a professional body-supervised accountant allowed an individual (who has since been convicted of fraud) to use the accountant's bank accounts to receive money from private investment clients deceived by the fraudster. On

instructions, the accountant paid money out of these accounts to the fraudster's personal bank accounts.

Tax services

6.12 Tax services are unlikely to be used to launder the proceeds of other crimes, but law enforcement agencies do observe accountancy services being used to facilitate tax evasion and VAT fraud. Practitioners in the sector accept the risk that prospective clients may be looking to engage in tax evasion and to launder the proceeds, and there is ongoing work among professional bodies (for example through the guidance on Professional Conduct in Relation to Taxation, developed in collaboration between the accountancy sector and HMRC and updated in March 2017) to promote wider responsibilities around tax in the accountancy sector.

Box 6.E: Tax services

Case study: A client purchased a company, with a debt in the region of £8 million included in the company purchase. A direct settlement of the debt would have resulted in a large tax liability applicable, totalling approximately £3 million. The accountant devised a scheme by which settlement of this debt could take place outside of the UK, thereby circumventing the UK tax system and payment to HMRC.

Supervision, compliance and law enforcement response

6.13 The 2015 NRA identified risks in the sector relating to inconsistent supervision of accountancy firms (despite good practice in areas) and some examples of poor AML/CTF compliance by practitioners. While these risks remain, the government is taking action to promote more effective supervision through the introduction of OPBAS, which will oversee the adequacy of all AML/CTF supervisory arrangements of professional body supervisors in the UK.

6.14 The 2015 NRA assessed that the number of SARs submitted by the accountancy sector was relatively low, and numbers have continued to decline with accountants and tax advisers submitting 4,254 SARs in 2015/16.[4]

6.15 Since 2015, the UKFIU has forged a stronger relationship with supervisors with the ambition of enabling better information sharing. The UKFIU participates in quarterly meetings with the accountancy sector through the recently established Accountancy Engagement Group. The group consists of those organisations submitting the highest numbers of SARs in the sector and shares information on accountancy SAR trends and patterns. The group is currently developing an accountancy SAR template, tailored to the

[4] 'Suspicious Activity Reports (SARs) Annual Report 2017', NCA, October 2017

different types of services provided and offering examples specifically from that sector.

6.16 The need for systems, procedures and staff in place to handle sensitive information has historically constrained cooperation between supervisors and law enforcement. However, cooperation has improved since 2015, for example through supervisors developing an accountancy risk assessment methodology with input from law enforcement, and the Home Office's 'Flag it up' campaign run over the last two years to increase firms' understanding of money laundering risk and reporting obligations. Law enforcement agencies report that the new written risk assessment obligation and approval test (to check key personnel for relevant criminal convictions) introduced through the MLRs will further strengthen the sector's compliance and risk.

Chapter 7
Legal services

Summary and risks

7.1 The 2015 NRA highlighted the main risks around legal services as: complicit legal professionals facilitating money laundering; the use of legal professionals by criminals to purchase property; the misuse of client accounts by complicit or negligent professionals; mixed compliance with the MLRs and POCA; and challenges in supervising a large sector with a high number of small firms and sole practitioners.

7.2 Legal services remain attractive to criminals due to the credibility and respectability they can convey, helping to distance funds from their illicit source and integrate them into the legitimate economy. While the 2015 NRA identified intelligence gaps around the role of professionals in high-end money laundering, recent work by law enforcement has helped to significantly develop our understanding of this area. While some proportion of those legal service providers involved in money laundering cases are complicit, the majority of these cases are likely to involve those who are either wilfully blind or negligent.

7.3 The 2015 NRA assessed legal services to be at high risk of exploitation for money laundering. Due to the attractiveness of legal services to criminals and their continued prevalence in high-end money laundering (including some instances of complicity), there is still assessed to be a **high** risk associated with abuse of legal services in money laundering. These risks vary by area, and the specific areas assessed to be at greatest risk are outlined below. Legal services are not judged to be attractive for terrorist financing, and there is no specific evidence of these services being abused by terrorists, so the terrorist financing risk associated with the sector is assessed to be **low**.

7.4 The 2015 NRA reported that in 2014 there were over 14,000 firms providing legal services. In 2016 this figure remained at over 14,000, with 72% employing fewer than ten employees.[1] The 2015 NRA identified an intelligence gap around the types of legal service and professional involved in money laundering. Recent analysis of SARs and law enforcement cases to date has helped to fill this gap, suggesting that the services at highest risk of exploitation are trust and company formation, conveyancing and client account services. Solicitors may offer any or all of these services and are

[1] 'Business population estimates 2016', Office for National Statistics, October 2016

therefore at greatest risk, while other legal professionals including barristers, legal executives and notaries are assessed to be exposed to lower risks.[2]

7.5 NCA investigations show that criminals may use a combination of legal services to add layers of complexity to a transaction and hamper effective due diligence. Criminals may also deliberately compartmentalise work between or within firms to avoid scrutiny – the Solicitors Regulation Authority (SRA) has identified a risk of those involved in large-scale money laundering using multiple firms to frustrate investigations.[3]

Trust or company formation

7.6 The creation of trusts and companies on behalf of clients is assessed to be the legal service at greatest risk of exploitation. Investigations by law enforcement often feature trusts and companies being used to facilitate high-end money laundering by hiding beneficial ownership, undermining due diligence checks and frustrating law enforcement investigations. This is often used in conjunction with other services (in particular the purchase of property, as detailed below) to facilitate money laundering.

Box 7.A: Legal services and company formation

Case study: Immediately prior to a property being acquired by a development company, shares in the development company were acquired by another company owned by a solicitor in a high risk country. Funds for completion of the purchase were provided from the solicitor in the high risk country to the seller's solicitors. While the solicitor in the high risk country was to become the beneficial owner of the property, the contract for the purchase of the property, was in the name of someone else. Law enforcement agencies suspect that the funds involved were the proceeds of corruption.

Conveyancing

7.7 The involvement of legal professionals in purchasing property is assessed to be another primary risk area for the sector. NCA analysis of SARs related to the legal sector in 2016 revealed that 50% were linked to the property market. Purchase of property provides an opportunity to launder a substantial sum in a single transaction, is a store of value (and often provides a capital gain) and can also be used to enhance criminal lifestyle. Cases encountered by law enforcement agencies continue to evidence the involvement of legal services (whether unwitting, negligent or complicit) in the purchase of property through overseas companies linked to the proceeds of crime, including high profile fraud and international corruption.

[2] In Scotland and Northern Ireland barristers and advocates are barred from direct public engagement, while barristers in England and Wales can only engage directly with the public following a strict authorisation process. Barristers in each jurisdiction are prohibited from executing transactions, conducting conveyancing and offering client account services. These factors are also judged to mitigate the risks involved.

[3] 'Cleaning up: Law firms and the risk of money laundering', Solicitors Regulation Authority, November 2014

Box 7.B: Conveyancing

Case study: A solicitor was instructed by two individuals in relation to a purchase of a commercial property in the region of £4.5 million. The funds came from the sale of shares held in an overseas trust, along with the sale of various property companies owned by a further company. The ultimate beneficial owner of this company was never disclosed, but the director was one of the solicitor's clients. The funds for the deposit were received by the solicitor from another company, also with an unknown ultimate beneficial owner, in various instalments. Law enforcement agencies assess that it was likely that the funds were the proceeds of corruption.

Misuse of client accounts

7.8 Misuse of client accounts represents a further risk around legal services. The majority of cases observed relate to abuse of the property market. Legal service providers often use client accounts to hold and move money on behalf of their clients for related legal services. Money may move through these accounts rapidly and in large sums to third parties. The majority of client account transactions are subject to the MLRs, and in accordance with professional regulations must be in respect of an underlying transaction rather than in lieu of regular banking transactions.

7.9 Law enforcement agencies have observed client accounts being exploited by criminals to transfer funds to third parties, effectively breaking the audit trail to launder funds. The SRA has observed cases of solicitors not carrying out full due diligence on each transaction or facilitating client account transactions before the completion of CDD. Criminals have entered apparently legitimate relationships with legal service providers, securing access to a client account, then changed their arrangements unexpectedly and with little explanation in order to pass funds to a third party.

Box 7.C: Misuse of solicitors' client accounts

Case study: A potentially corrupt and complicit solicitor was identified as being involved in transferring funds with no underlying legal services. The clients for whom the solicitor acted were both foreign PEPs and were strongly suspected of being linked to overseas money laundering, bribery and corruption. The law firm received a total of over £100 million into its client accounts in relation to these clients.

Supervision, compliance and law enforcement response

7.10 The 2015 NRA identified mixed standards of compliance within the sector, as well as challenges in supervision arising from the high number of sole practitioners and small firms. Many of these challenges remain. The SRA's 2015 thematic review found broad compliance but some weaknesses, including relating to the allocation of Money Laundering Reporting Officer

(MLRO) responsibilities and appropriate completion of CDD.[4] Innovation within the legal services market may pose a further supervisory challenge, as criminals could identify new opportunities to access legal services without engaging a supervised firm.

7.11 In addition, some instances of lawyers falsely claiming legal professional privilege continue to occur, posing a risk to the law enforcement response to money laundering. While the law is clear that communications and associated documents are not legally privileged if they are part of the furtherance of crime or fraud, lawyers may claim that legal professional privilege applies to those documents which no-one else has seen. Law enforcement agencies have identified cases where lawyers have claimed legal professional privilege incorrectly (for example, trying to assert the existence of privileged material to prevent the disclosure of other, non-privileged material), frustrating investigations. The government recognises that legal professional privilege is a vital part of the UK's legal system and that ensuring that it is applied correctly in all circumstances is important in mitigating money laundering risk.

7.12 Despite these challenges, improvements since 2015 have been noted across the sector, and the SRA's thematic review concluded that most law firms visited had effective compliance frameworks in place. Law firms have reported to the SRA that understanding of SARs obligations has improved over recent years, and that firms are increasingly refusing to act on behalf of a client where there are suspicions.[5] The improved understanding of risk since 2015 may be in part due to improved supervisory activity and the Home Office 'Flag it up' campaign, run over the last two years to increase firms' understanding of money laundering risk and reporting obligations. Some supervisors have increased the priority of AML/CTF and strengthened their expertise in the area since 2015. Remaining challenges to supervision will be addressed through the introduction of OPBAS, which will oversee the adequacy of all AML/CTF supervisory arrangements of professional body supervisors in the UK.

7.13 The 2015 NRA assessed that the number of SARs submitted by the legal sector was relatively low, and numbers have declined since that stage with independent legal professionals submitting 3,447 SARs in 2015/16.[6] The UKFIU has engaged with the certain parts of the legal sector with a view to improving relationships and the quality of SAR submissions in the sector.

7.14 In addition, the government has taken steps to address the risks arising from links between legal services and the property market through the introduction of Unexplained Wealth Orders in the CFA. Through this measure, those suspected of serious criminality can be required to explain wealth that appears disproportionate to their income, providing law enforcement with an additional tool for investigations around high-end money laundering. The new MLRs and introduction of OPBAS will present a

4 'Anti Money Laundering Report', Solicitors Regulation Authority, May 2016

5 'Anti Money Laundering Report', Solicitors Regulation Authority, May 2016

6 'Suspicious Activity Reports (SARs) Annual Report 2017', NCA, October 2017

range of further measures which should help to further mitigate the risks of exploitation of legal services. These include requiring legal supervisors to conduct approval tests (to check key personnel for relevant criminal convictions), limiting the circumstances in which simplified due diligence can be applied for pooled client accounts and one-off company formation, and requiring operational independence for professional bodies' supervisory functions where this doesn't already exist.

Chapter 8

Property and estate agency services

Summary and risks

8.1 The 2015 NRA looked at the abuse of estate agency services in money laundering, while this report also looks more widely at abuse of the property market including where other professionals are involved.

8.2 The key risks in the estate agency sector identified in the 2015 NRA were: criminals and professionals using estate agents to help buy and sell property to launder funds; complicit estate agents helping criminals buy or sell property, sometimes in conjunction with other complicit professionals; perceived low understanding of money laundering and terrorist financing risks in the sector, and low compliance with the MLRs.

8.3 These vulnerabilities are assessed not to have changed significantly since 2015, though recent reforms to prevent the misuse of corporate structures and trusts should mitigate the risks where property is held by these vehicles. In addition, recent awareness-raising activity by HMRC among the estate agency sector should help to mitigate the risks.

8.4 When separating the exploitation of property from the involvement of estate agency services, abuse of property is assessed to pose a **medium** risk while the services of estate agents themselves pose a **low** risk. Property continues to be an attractive vehicle for criminal investment, in particular for high-end money laundering. While effective and comprehensive due diligence on all parties by estate agents can help mitigate the money laundering risks around property (especially by providing useful intelligence to law enforcement), much of the risk lies with those closer to the client and their funds, such as legal professionals.

8.5 Neither estate agency services nor property are judged to be attractive for terrorist financing, and we have seen no evidence of these areas being abused for terrorist financing, so the terrorist financing risk associated with the sector is **low**.

Abuse of property

8.6 Property can be used by criminals as an investment, for lifestyle benefit and to integrate proceeds of crime into the legitimate economy. It presents particular appeal to high-end money launderers looking to conceal large sums in few transactions, often with beneficial ownership hidden through the use of corporate vehicles or overseas trusts.

8.7 In an analysis of SARs linked to property, 27% highlighted the presence of companies and trusts in property transactions, 36% highlighted attempted use of professional intermediaries and 17% reported high cash payments. The key typologies identified from SARs were unusual transactions relating to the same property in rapid succession (often involving the use of cash or third party intermediaries), and the use of companies or overseas trusts to conceal property ownership. A 2015 report identified that over 75% of investigations involving land and property by the Metropolitan Police Service's Proceeds of Corruption Unit (now the NCA's International Corruption Unit) involved companies registered overseas, primarily in UK Crown Dependencies or Overseas Territories with financial centres.[1]

8.8 There is assessed to be a particularly high risk in super-prime property in London and Edinburgh. Super-prime property is a commonly identified feature within current investigations into grand corruption and money laundering being conducted by the NCA's International Corruption Unit. A significant amount of intelligence about possible proceeds of corruption in London is generated by transactions relating to the acquisition or sale of such super-prime property.

8.9 In Northern Ireland, there is evidence of criminals (particularly those with links to dissident Republican groups) investing illicit proceeds in property south of the border to create additional complexity for law enforcement investigations, as well as evidence of criminals using illicit funds to build property on legitimately owned land to avoid scrutiny.

8.10 Residential property is assessed to pose a greater risk than commercial property: client turnover is higher, the property is easier to sell on, and it can be lived in using criminal funds. However, the commercial sector also poses risks. Complex, opaque company structures are less likely to raise suspicions in the commercial sector than in the residential market. Furthermore, commercial property may be purchased by criminals as premises for cash intensive businesses involved in money laundering or predicate offences, such as human trafficking.

8.11 Certain jurisdictions are noted as particularly high risk as sources of property purchase due to high levels of anonymity, and it is likely that these jurisdictions are used by criminals in the UK or a third country to purchase UK property.

Box 8.A: Purchase of property through companies

Case study: An investigation into a corrupt foreign government official revealed a complex system of shell companies designed to disguise the ownership of money (generated from bribes) and registered by an overseas solicitor. Funds from one of the companies were used to purchase a London property for over £9 million. Unravelling the complex system of shell companies led to the uncovering of an additional sum of over £4 million,

[1] 'Corruption on your doorstep: how corrupt capital is used to buy property in the UK', Transparency International, February 2015. It should be noted that the prevalence of jurisdictions in investigations may be attributable to a number of drivers, and is likely to be greater where there is closer cooperation between law enforcement agencies in that jurisdiction and in the UK.

which was seized. The official was convicted of corruption and money laundering offences and was given a custodial sentence.

Estate agents

8.12 The number of estate agents registered under the MLRs has risen from around 8,000 in 2014 to around 9,500 in 2016. Most of these are small businesses, though restructuring within the sector has led to the number of large firms increasing from 17 in 2015 to 77 in 2016.[2] There are limited barriers to entry to the sector beyond registration with HMRC. Compliance standards vary, with some best practice (especially in large firms) and some poor performance observed, though standards are improving. Recent changes in the sector may lead to further improvements, through smaller businesses being acquired by larger firms and HMRC working with larger businesses to encourage the use of centralised compliance teams, especially where complex ownership structures are involved.

8.13 Due to the relatively limited involvement of estate agents in their customers' affairs, estate agents themselves are assessed to be unlikely to be complicit in facilitating money laundering. Those cases where estate agents have been observed to facilitate money laundering highlight that the general risk in the sector is around negligence or wilful blindness allowing the criminal abuse of property, rather than complicit facilitation of criminal activity.

Supervision, compliance and law enforcement response

8.14 The 2015 NRA identified that a large number of estate agents were not thought to have registered for AML/CTF supervision due to lack of awareness. However, HMRC became the supervisor for estate agents in 2014 and has taken action to significantly increase registration rates.[3] Though HMRC continues to see examples of low awareness of AML/CTF obligations, it works closely with trade bodies and firms to raise awareness, including use of face-to-face visits and webinars. In addition, HMRC has improved the quality of its guidance, which was praised by the government's 2017 Cutting Red Tape Review of the AML/CTF regime.

8.15 Estate agents are key facilitators of property transactions, and have a relationship with both the buyer and the seller at an early stage in the transaction. The 2015 NRA reported that it was common for estate agents not to conduct due diligence themselves, often relying on other regulated firms (sometimes improperly, i.e. without seeking consent) to do so. Poor application of due diligence has also been observed where corporate structures are involved, where identifying beneficial ownership is difficult, or where competition and prospective fees are particularly high. Estate agents were previously only obliged to carry out due diligence on their customer, often interpreted as the seller unless the buyer is independently represented. The MLRs address the risk that criminals may be able to purchase property

[2] Large firms are defined as those with over 50 premises and annual property sales throughput of £50 million or higher.

[3] 7,500 businesses were registered in April 2014, increased to over 10,000 by April 2017.

without being subject to scrutiny by clarifying that estate agents must carry out due diligence on the buyer as well as the seller of a property.

8.16 SAR reporting for the estate agency sector is assessed to be relatively low, with 514 SARs submitted by the sector in 2015/16.[4] However, this represents a 187% increase on 2013/14 figures. This increase is assessed to be due recent work by HMRC and the UKFIU. HMRC has worked to increase registration rates and awareness of money laundering risk in the sector. The UKFIU has engaged with the sector, with the ambition of exploiting better info sharing opportunities and with an emphasis on sharing good practice and signposting guidance. This increase should continue as more activity now falls within the scope of the MLRs. In 2014/15, 21% of estate agent SARs related to property in the London area while 13% had a link to a foreign jurisdiction.[5]

8.17 The risks relating to abuse of property are most acute where property is owned anonymously through corporate structures or trusts. Recent reforms preventing the misuse of corporate structures and trusts will also mitigate the risks where property is held by these vehicles. These measures include the introduction of the publicly accessible register of people with significant control in companies, the requirement through the new Common Reporting Standard (CRS) for banks to provide HMRC with information on assets held in trust, and the introduction of Unexplained Wealth Orders through the CFA.

4 'Suspicious Activity Reports (SARs) Annual Report 2017', NCA, October 2017

5 'Suspicious Activity Reports (SARs) Annual Report 2015', NCA, 2015

Chapter 9

Trusts and corporate structures

Summary and risks

9.1 The 2015 NRA highlighted that companies and trusts (and similar structures) are known globally to be misused for money laundering. As a global financial centre, with individuals and businesses from all over the world choosing to invest and do business here, the UK is particularly exposed to criminal exploitation of otherwise legitimate economic activities and structures. As such, corporate structures and trusts are used in almost all high-end money laundering cases, including to launder the proceeds of corruption. There is insufficient evidence to quantify the exact extent of money laundering through corporate structures and trusts (both UK registered and overseas), though the vast majority of UK trusts, companies and partnerships are assessed to be used for legitimate purposes.

9.2 The UK has implemented a series of reforms since 2015 to increase the transparency of UK incorporated legal persons and arrangements, and to prevent their misuse for illicit purposes. These reforms include, but are not limited to, the introduction of the publicly accessible PSC register; the abolition of bearer shares; the introduction of a register of trusts with tax consequences; and the introduction of Unexplained Wealth Orders. It is too early to measure the impact of many of these reforms, but we expect these measures to go some way towards preventing the misuse of companies and trusts and assisting law enforcement agencies in their investigations where misuse does occur.

9.3 Certain vulnerabilities around both overseas and UK registered corporate structures and trusts make them attractive to money launderers. These include the ability for criminals to create complex and opaque structures, comprising multiple legal entities and arrangements across multiple jurisdictions, which can be used to obscure who really owns and controls assets. Companies, partnerships and trusts can be set up and dissolved with relative ease and low cost and used to transfer large sums of money at less risk of detection from law enforcement or the regulated sector. While the 2015 NRA identified these features as common vulnerabilities of both corporate structures and trusts without applying specific risk scorings, this assessment specifically compares the risks of abuse.

9.4 Law enforcement agencies have identified very little evidence of UK trusts (those governed by UK law and/or administered in the UK) being abused for money laundering purposes. The risk of criminals exploiting UK trusts to launder money is therefore assessed to be low. The precise extent of abuse

of UK trusts remains an intelligence gap. However, there are significantly higher risks associated with overseas trusts. There are no known cases of UK trusts being abused for terrorist financing, and the risk for terrorist financing is also assessed to be **low**.

9.5 While the vast majority of companies and partnerships are used for legitimate purposes, law enforcement agencies assess that criminals seeking to hide wealth or enable money laundering are likely to use companies and partnerships in order to do so. The risk of criminals seeking to launder money through UK and overseas corporate structures is therefore assessed to be **high.** There is assessed to be a **low** risk of UK companies being used by terrorists to move or raise funds.

9.6 The 2015 NRA assessed TCSPs as medium risk for money laundering.[1] While trust and company services pose a relatively high risk, the risks are assessed to be greatest when provided in conjunction with other financial, legal or accountancy services, and the use of TCSPs outside these sectors continues to be assessed as **medium** risk for money laundering. The risk for terrorist financing is assessed to be **low**.

Trusts

9.7 The 2015 NRA estimated that the UK is home to 1.5–2 million trusts, though there remains little reliable data against which to verify this. The great majority of these are used for ordinary and legitimate reasons and pose very low risks of abuse. Common reasons for establishing trusts include people seeking to: manage assets on behalf of vulnerable persons; jointly hold property; ensure inheritance is distributed in accordance with a person's last will and testament; perform commercial activity; and conduct charitable work.

9.8 As noted in the 2015 NRA, however, the misuse of trusts is known to be a global problem. The risk profile around trusts is not assessed to have changed since 2015; trusts remain vulnerable to abuse because they separate legal ownership from beneficial ownership, meaning that a criminal may disguise their interest in an asset by transferring legal ownership to a trustee. Trusts can be used to frustrate law enforcement efforts in obtaining accurate details of who owns an asset.

9.9 Law enforcement agencies rarely encounter abuse of UK trusts in high-end money laundering. However, there are known higher risks posed by abuse of overseas trusts. Overseas trusts feature in many of the SFO's investigations. By placing an asset in an overseas trust, a criminal can simultaneously disguise their interest in it and place it beyond the UK AML/CTF regime and the investigatory powers of UK law enforcement.

9.10 During the NRA exercise, several cases were identified involving UK criminals abusing overseas trusts. These cases involved trusts established in a range of

[1] This does not include the risks of these services when provided by financial institutions, accountants or lawyers, which are assessed to be higher and are covered in separate chapters.

jurisdictions, including UK Crown Dependencies and Overseas Territories with financial centres.[2]

Box 9.A: Abuse of overseas trusts

Case study: A criminal who committed mortgage fraud laundered the proceeds through a trust in the British Virgin Islands (BVI) which was administered by a lawyer in Switzerland. The trust's beneficiaries were the criminal's children and a charity. However, the trust also controlled over 50 BVI-incorporated companies, each of which held luxury assets across the UK and Europe (including artwork, a yacht and a private jet). Most of the companies were held through bearer shares. The criminal received a conviction for fraud and was required to repay proceeds from the assets held in the trust.

9.11 Industry sources have identified a number of indicators for trusts being abused, including a trust being created by a settlor for the benefit of an unconnected party, if a trust had multiple settlors or if it formed part of a complex ownership chain, particularly if that chain crossed national borders.

9.12 Many trustees are trained, licensed and regulated professionals. However, there is no requirement for a settlor to use a professional trustee, and several cases encountered by law enforcement have featured laypersons as trustees. The MLRs require all UK trustees (regardless of whether or not they are professional trustees) to keep accurate and up-to-date records of the identities of all beneficial owners and to provide this information upon request to law enforcement.

9.13 Several branches of government maintain trust registration systems that can help law enforcement agencies to link an asset to the relevant parties.[3] In July 2017, HMRC launched an online beneficial ownership register for trusts with tax consequences. This is expected to cover 160,000–170,000 trusts by the end of January 2018. Information held on this register is available to law enforcement agencies, delivering an increased ability to identify and interrupt suspicious activity involving the misuse of relevant trusts.

9.14 The CFA introduced Unexplained Wealth Orders, which can be used to require individuals whose assets are disproportionate to their known income to explain the origin of their wealth. This will help law enforcement agencies tackle suspicious wealth directly, rather than pursue the audit trail, including where the assets are held by a corporate structure or in a trust.

9.15 Under the CRS – the new global standard for tax transparency – financial institutions must provide HMRC with information on non-UK residents with bank accounts or investments in the UK. This includes accounts or investments held in a trust. The CRS will be complemented by a new UK-led

[2] It should be noted that the prevalence of jurisdictions in cases identified may be attributable to a number of drivers, and is likely to be greater where there is closer cooperation between law enforcement agencies in that jurisdiction and in the UK.

[3] The UK's various land registries record the legal ownership of any land or buildings owned through a trust; charitable trusts are supervised by charity regulators in England and Wales, Scotland and Northern Ireland; and the Pensions Regulator has oversight of occupational pension trusts.

initiative to systematically share beneficial ownership information internationally. Over 50 jurisdictions have signed up to this initiative, including every Crown Dependency and Overseas Territory with a financial centre. In addition, the new PSC register records where a trust is a beneficial owner of a company, with the trustee's name appearing on the register.

Corporate structures

9.16 The 2015 NRA outlined the general company landscape in the UK: as of February 2015, 3.4 million companies and 60,000 limited liability partnerships (LLPs) were on the UK company register. As of March 2017, there were over 3.8 million companies on the register, almost 96% of which are private companies limited by shares.[4] The vast majority of these companies are used for legitimate purposes.

9.17 Law enforcement agencies assess that corporate structures are being created by criminals or on their behalf both in the UK and overseas, frequently using the services of regulated professionals, with the intention of subsequently using the structure to hide wealth or enable money laundering. The incorporation of the company may be done in a way that conforms with the applicable legal requirements and in such a way as to minimise suspicion.

9.18 Companies and LLPs are particularly attractive to criminals due to their separate legal personality, the relative ease and low cost with which they can be incorporated and dissolved (intended to fulfil the needs of a wide range of legitimate businesses) and the ability to use business accounts to merge legitimate and illegitimate funds. Many of these features are common to companies and company incorporation systems around the world.

9.19 Criminals can also be attracted to the ability to terminate a company or partnership easily, and have been observed setting up sequences of limited companies ('phoenix companies') for illicit purposes, then winding them down before being required to submit accounts.

9.20 There is a small risk that UK companies could be used, wittingly or unwittingly, by terrorist actors to raise or move funds, or to procure items for terrorist groups, though intentional abuse of companies is unlikely to represent an attractive or efficient route for terrorist financing.

Risks associated with different corporate forms and structures

9.21 The 2015 NRA highlighted law enforcement agencies' concern around the risks posed by limited partnerships (LPs) in particular due to limited reporting obligations. The availability of useful intelligence for law enforcement when investigating partnerships is undermined by the fact that there is no general requirement to submit annual accounts to Companies House. Accounts may be required by HMRC for tax purposes, and corporate partners are required to submit accounts for the partnership alongside their own annual accounts. Due to the regulatory requirements involved, criminals are assessed to be highly unlikely to set up Public Limited Companies to launder funds.

4 'Incorporated companies in the UK January to March 2017', Companies House, April 2017

9.22 Scottish limited partnerships (SLPs) are governed by Scottish law. They are particularly attractive to criminals due to the fact that under Scottish law the partnership is a distinct legal personality, separate from the partners and is subject to fewer reporting and transparency obligations than most other corporate forms. [5] This has allowed OCGs to disguise their involvement by establishing SLPs with partners, based in the UK or overseas, limiting law enforcement agencies' ability to investigate.

Box 9.B: Abuse of Limited Liability Partnerships

Case study: One Eastern European based bank deliberately sought to increase its number of UK LLP clients. This was driven by a desire to reduce the number of clients domiciled in jurisdictions included on a 'blacklist' of jurisdictions, maintained by the Ministry of Finance in the bank's home country. The UK is a country on the Ministry of Finance's 'white list', enabling the movement of money without scrutiny. It is highly likely that no LLP clients of the bank had any business activities in the UK and that the LLPs were merely vehicles to help move the clients' money, with business activity taking place entirely in Russia or former Commonwealth of Independent States (CIS) countries. The sixteen most profitable LLPs for this bank are believed to have been used to facilitate the movement of at least €1.5 million through the UK over the course of a six-month period in 2013 by filing falsified records and accounts with Companies House.

9.23 In light of concerns that different forms of partnership are being used for criminal activity, the Department for Business, Energy and Industrial Strategy (BEIS) published a Call for Evidence in 2017 on a Review of Limited Partnership Law to consider those aspects of the framework that may enable criminal activity. BEIS will analyse all the submissions and a government response will be published shortly. One part of the response will confirm that LPs and SLPs are a very attractive structure for legitimate businesses across the economy, in particular for financial and pension structures.

9.24 Following the previous Prime Minister's commitments on corporate transparency at the 2013 G8 summit in Lough Erne, the government introduced a public register in 2016 of people with significant control in companies. The register imposes a requirement on all companies and LLPs to disclose the details of any people with significant control in a company or partnership. From June 2017, reporting requirements for those within scope of the register were increased, and the existing regime was expanded to include more corporate forms including all SLPs. The companies register was accessed over two billion times in 2016/17, the first year that PSC information was available, and users are encouraged to report any information they believe to be incorrect.[6] This should mitigate the risks associated with company abuse and support law enforcement investigations.

[5] This does not apply to LPs registered elsewhere in the UK.

[6] 'Companies House Annual Report and Accounts 2016/17', Companies House, 2017

Overseas companies

9.25 Overseas companies are used as a tool for UK criminals to launder their funds or for criminals elsewhere to use corporate vehicles to invest in the UK. In April 2016, the International Consortium of Investigative Journalists released the 'Panama Papers', involving over 11 million documents relating to hundreds of thousands of overseas entities, a number of which involved UK persons and are likely to have been facilitating illicit activity. This has further highlighted the risk posed by the abuse of overseas companies.

9.26 Following the release of the Panama Papers, a cross-agency taskforce was created, led jointly by the NCA and HMRC with the SFO and the FCA as key partners. The taskforce established the Joint Financial Analysis Centre (JFAC) to analyse all information available from the data leak and investigate individuals involved. Using data and intelligence gathered from across the taskforce, and co-located officers from all four agencies, JFAC is developing cutting-edge software tools and techniques to exploit all available financial intelligence, together with other datasets held by government and open source data.

9.27 Overseas financial centres can allow the creation of complex and layered ownership structures quickly, at low cost, and with limited transparency requirements, hindering law enforcement agencies' abilities to identify money flows. Some countries do not require companies to disclose the identity of officers and directors, with no requirement to appoint a locally resident director. This has been identified as a potential money laundering risk, as it is possible for a person to control an offshore holding without disclosure of the director.

Trust or company service providers

9.28 While companies can be registered directly with Companies House, criminals continue to make use of third party TCSPs, to establish the structures within which illegitimate activity subsequently takes place. The 2015 NRA identified the greatest risks around the TCSP sector to be: negligent or complicit TCSPs facilitating money laundering; criminal abuse of companies and trusts set up by TCSPs; inconsistencies in approaches to supervision; and the mixed standard of implementation of the MLRs across the sector. All of these vulnerabilities remain key factors behind the risks in this sector.

9.29 The highest risk TCSPs are assessed to be UK TCSPs which offer a wide range of services (including nominee directors, registered office services, and banking facilities) which are used in conjunction to mask beneficial ownership whether through complicity, wilful blindness or negligence.

Supervision, compliance and law enforcement response

9.30 The 2015 NRA highlighted that those providing TCSP services could be supervised by one of a number of supervisors, depending on whether also acting as an accountant or legal professional or an FCA authorised person. Under the MLRs, all TCSPs are subject to fit and proper testing. The introduction of OPBAS will help address inconsistencies in supervision of TCSPs. In addition, HMRC has a register of TCSPs, which is searchable by the

public via a 'look up' facility and should help build understanding of the sector.

9.31 TCSPs submitted 74 SARs in 2015/16, with a year-on-year decline since 2013/14 likely to reflect inconsistent supervision and mixed compliance standards across the sector.[7] The 2015 NRA identified a mixed quality of CDD across the sector, and the perception among some TCSPs that company formation constitutes an 'occasional transaction' rather than a 'business relationship', leading to insufficient CDD being conducted. The government has addressed this gap through the MLRs, which clarify that one-off company formation constitutes a business relationship.

9.32 While most companies are registered through a third party, the remainder are registered directly with Companies House.[8] Companies House is a registrar, not a regulator, and ensures fulfilment of disclosure requirements in exchange for limited liability. Once registered, companies must provide updates if certain details change and must provide annual sets of accounts and annual confirmation statements for basic information (this replaced the annual return in 2016). There are penalties attached for non-compliance, ranging up to a two-year prison sentence. Companies House has a statutory duty to incorporate a company if all relevant information has been legally provided. While data checking by Companies House is not a guarantee of accuracy, public and commercial access also help to keep accuracy in check. Companies House works with law enforcement agencies to help them identify suspicious activity, files SARs when it forms suspicions, and has powers to impose civil penalties or prosecute when compliance is not achieved.

9.33 Recent reforms preventing the misuse of corporate structures and trusts should mitigate the risks in these areas. These measures include the introduction of the publicly accessible PSC register, the requirement through the new CRS for banks to provide HMRC with information on assets held in a trust, and the introduction of Unexplained Wealth Orders through the CFA.

7 'Suspicious Activity Reports (SARs) Annual Report 2017', NCA, October 2017

8 'UK national risk assessment of money laundering and terrorist financing', HM Treasury and Home Office, October 2015

Chapter 10
Cash

Summary and risks

10.1 The 2015 NRA identified the main vulnerabilities around cash as: the use of high denomination notes to conceal or disguise the origins of funds; the movement of criminal proceeds, in the form of cash, within and across borders; the use of cash rich businesses to conceal or disguise the origins of funds, and to place large sums of criminal cash into the banking system and other parts of the regulated sector; and the use of foreign currency by criminal groups to pay suppliers overseas. Cash is inherently high risk due to it being untraceable, readily exchangeable and anonymous. Evidence from law enforcement agencies and others suggests that these vulnerabilities remain largely unchanged since 2015, and use of cash remains a **high** risk for both money laundering and terrorist financing.

10.2 Cash remains the most popular payment medium in the UK; while its general use is declining (45% of all payments in 2015 were in cash, reduced from 64% in 2005 and forecast to fall to 27% by 2025[1]) it is assessed to remain an attractive tool for criminals. The widespread use of cash for legitimate as well as criminal purposes makes it very difficult to assess the overall extent of its use in money laundering or terrorist financing. Law enforcement agencies' knowledge of cash-based money laundering is generally strong, given a long history in tackling this risk, and the limited number of ways in which cash-based laundering can occur. Cooperation with international partners is also particularly strong in combating this form of laundering, with good intelligence sharing and common cash seizure powers.

10.3 As UK banks' and financial institutions' risk appetites have decreased, there is assessed to have been an increase in the movement of illicit cash via the non-bank financial system, including MSBs and cash smugglers, and the use of mobile stores of value such as gold. The CFA created new civil powers to enable the forfeiture of these mobile stores of value, such as precious metals and works of art.

Cash intensive businesses

10.4 As highlighted in the 2015 NRA, cash intensive businesses remain one of the primary mechanisms through which domestic OCGs launder illicit cash into ostensibly legitimate earnings, and pose risks to several other parts of the

[1] 'Debit cards to overtake cash payments by 2021', Payments UK, May 2016

regulated sector with which they interact – in particular banks and accountancy firms.

10.5 The 2015 NRA highlighted that scrap metal wholesalers, nail bars, takeaways and storage warehouses represented particularly attractive opportunities for criminals. Other firms in parts of the regulated sector (such as MSBs) may also deal intensively in cash themselves and therefore pose attractive business propositions for criminals looking both to launder funds through cash earnings and to use the business' wider activities to transfer or disguise their assets.

Box 10.A: Cash intensive businesses

Case study: A car trader was suspected of keeping cars on his forecourt which were not on the business' books and had been purchased using criminal cash. Customers then purchased these cars from the business using cash or cheque. When a customer bought one of these cars with cheque, a false history relating to the original acquisition of the car was created in the business records. This included the invention of a false vendor and the making of a payment out of company funds to reflect the purchase, which was diverted to the private account of the proprietor's girlfriend. The car dealer was convicted for money laundering on the basis of the evidence of the manipulation of the business books and records.

High denomination notes and cash at the border

10.6 The 2015 NRA highlighted the criminal need for foreign currency to transfer cash overseas and pay overseas suppliers. This risk remains high. Cash is typically transported overseas by heavy goods vehicles, passenger vehicles and air travel, often via commercial airlines. The 2015 NRA estimated that between April 2012 and March 2014, over £6 million was seized and forfeited at the UK border. From 1 January 2017 to 28 February 2017, Border Force seized over £11.5 million of suspected illicit cash being transported through the UK border. A recent multi-agency operation covered three weeks of proactivity at ports, seizing around £1 million in cash with destination countries including Albania, Belgium, Brazil, Netherlands, Thailand and Turkey.

Box 10.B: Cash at the border

Case study: An ongoing HMRC operation is investigating the laundering of illicit proceeds of crime via the physical exportation of cash through UK borders. Three MSBs were identified exporting cash in freight, and in total these businesses exported over £20 million during a three-month period. Investigations are ongoing into identifying the level of illicit activity within this movement, and HMRC is now leading a joint law enforcement project to tackle the identified threat.

10.7 At the border in 2014 and 2015, 23% of cash seized was in foreign currency, with euros and dollars being the most prevalent. Evidence from law enforcement suggests that euro currency is often smuggled in the form

of €500 notes. In 2016, the European Central Bank announced that it would discontinue production of the €500 with effect from the end of 2018. UK wholesale currency institutions already have a voluntary agreement not to issue €500 notes within the UK.

10.8 High denomination notes are seen as attractive to criminals for transferring funds due to their high ratio of value to physical volume. However, within UK borders, law enforcement agencies have indicated that domestic cash seizures suggest criminal use of £10 or £20 notes to be much more common than use of the £50 note. The majority of high denomination notes are assessed to be held overseas for legitimate or illegitimate use, and their use in cross-border cash smuggling may be more prevalent than within the UK.

Terrorist financing

10.9 The 2015 NRA identified the use of cash as high risk for terrorist financing, with cash couriering assessed to be the favoured method of taking terrorist funds out of the UK. Cash is thought to remain the highest risk area for terrorist financing, and recent cases continue to demonstrate this. Between 1 April 2012 and 31 March 2017, law enforcement agencies made 79 cash seizures in relation to terrorist financing totalling £495,797.

Box 10.C: Use of cash in terrorist financing

Case study: In 2016, two men were convicted for preparation of acts of terrorism. One of the individuals withdrew over £3,000 through 2014-15, mostly taken from housing benefits, from a bank account set up by a third individual believed to be fighting for Daesh in Syria. The two men then gave the money to a suspect subsequently linked to the March 2016 Brussels terror attack. The funds were given on the assumption that the money would reach the individual believed to be fighting for Daesh.

Law enforcement response

10.10 The inherent anonymity of cash provides obstacles for law enforcement in disrupting or investigating its use for money laundering or terrorist financing. However, cash seizures continue to play an important role in disrupting illicit activity. The UK has a specialist cash seizure team at UK ports, which has the ability to seize cash at the border and actively share information with other government agencies to allow them to act on intelligence relating to individuals who may be suspected of transporting cash out of the UK. The CFA will allow law enforcement agencies to seize a wider range of items under the definition of cash. Existing cash seizure powers are used on a regular basis and have a significant disruptive effect.

Chapter 11

Money service businesses

Summary and risks

11.1 The MSB sector encompasses a range of services relating to the transmission or conversion of funds, including money transmission services, foreign exchange and cheque cashing. The sector is highly diverse, with providers ranging from local convenience stores offering remittance services to large multinational corporations and web-based businesses providing peer-to-peer money transfers. MSBs play an important function in many communities by providing financial services to those without access to banking services. Cross-border remittances facilitated by MSBs have also been shown to play a key role in supporting economic development within developing countries. World Bank data suggests that remittances outflows from the UK were approximately $11.5 billion in 2014, with Nigeria ($3.8 billion) and India ($3.7 billion) the largest beneficiaries.[1]

11.2 The 2015 NRA noted that around 3,000 principal MSBs were registered with HMRC. This number is now just over 2,000, including over 1,300 firms providing currency exchange, over 1,000 firms providing money transmission, and over 500 firms providing cheque cashing services.[2] The structure of the sector is such that while only around 2,000 principals are registered, there are over 45,000 premises on which these services are conducted through both principals and their agents.

11.3 The 2015 NRA judged the risk of MSBs being abused for money laundering to be medium (with significant high risk elements in the sector). Specifically, the report identified that: some MSBs were being used for money laundering on a significant scale; there was control of some MSBs by OCGs; MSBs were being used to place large sums of criminal cash overseas; and MSBs had low levels of compliance with the MLRs. These specific risks largely persist and MSBs continue to be identified by law enforcement agencies as a key enabler in cases where criminal funds are transferred overseas. Due to the persistence of the risks identified in 2015, in addition to recent changes affecting the structure of the sector and leading to firms increasingly looking to operate outside of contact with the regulatory regime, there are now assessed to be **high** money laundering risks associated with the MSB sector. However, there remain certain services offered by the sector (such as cheque cashing) with little or no risks identified. In response to the risks, HMRC has

1 'Migration and Remittances Factbook 2016', World Bank, 2016

2 These subsectors exceed the total as some firms provide multiple services.

continued to target the MSB sector with significant supervisory interventions, including campaigns around principal-agent relationships.

11.4 The 2015 NRA assessed MSBs as high risk for terrorist financing. There is no reason to conclude that this risk has decreased since 2015, and the sector in general continues to be exposed to risks arising from links to high-risk jurisdictions and generally poor compliance outside the largest firms. As such, the MSB sector continues to be assessed as **high** risk for terrorist financing.

11.5 High risks associated with the MSB sector should be managed on a case-by-case basis. The government is concerned about the trend of de-risking, and has been at the forefront of international efforts to raise the profile of the issue. The UK is leading the global agenda on improving remittance providers' access to banking services, chairing a working group of the Financial Stability Board which will report to the G20 Finance Ministers in March 2018. Closer to home, the government has been working with affected sectors in the UK to better understand their experiences and encourage dialogue with the banking sector. This includes working with the banking sector to produce new guidance to help businesses in affected sectors to open a UK bank account, by setting out what information banks will require to comply with relevant regulations.

Money transmission

11.6 The use of the principal-agent model is widespread within the money transmission subsector. Third party businesses, acting as agents on behalf of the principal, typically accept payment and collect identification details from customers, which are then passed on to the principal for electronic transmission. It is the principal's responsibility to ensure their agents' compliance, including the completion of due diligence. HMRC data shows a 21% decline in the number of registered principals between 2014 and 2016, with a slight rise in the number of MSB business premises over the same period, suggesting that a greater proportion of MSBs are operating as agents and a higher agent to principal ratio. It is thought that these changes have been driven largely by banks withdrawing services from MSBs.

11.7 In recent years, many banks have restricted their relationships with MSBs or withdrawn services as part of de-risking activity. A 2016 FCA external research report found that many small MSBs have had difficulties with their banking arrangements, regard their financial situation as precarious, and have felt pressurised to change their business model, for example becoming part of larger networks.[3] It is likely that reduced access to formal banking services has increased the risks in the sector. There is some evidence that this trend has encouraged smaller businesses to avoid interaction with the AML/CTF regime, either through interacting less with regulated businesses or though illicitly acting without supervision.

11.8 HMRC has reported seeing changes in the way that MSBs operate, potentially as a result of the de-risking trend. This includes evidence of MSBs using freight or parcel companies to ship cash out of the country, or

[3] 'Drivers & Impacts of Derisking', John Howell & Co. Ltd. for the FCA, February 2016

establishing courier businesses to transport cash, facilitating anonymous transactions. For example, one operation identified use of a parcel courier to transport £14,000 in suspicious cash from an MSB out of the country. The same sender had previously sent 70 parcels to the same country.

11.9 There is evidence of MSBs seeking to register with banks as different cash-rich businesses or routing their business through third party accounts and other MSBs. HMRC has also found strong evidence that the principal-agent relationship is being exploited to launder criminal funds, including through businesses becoming agents of well-known money transmitters while operating their own separate systems for illicit transactions.

11.10 As highlighted by the 2015 NRA, international controllers are assessed to operate satellite networks from third countries to manage the flow of illicit funds worldwide as a service to money launderers.

Box 11.A: Money transmission

Case study: An operation concerning an MSB with offices in six UK cities highlighted that this business was being used for money laundering by Chinese OCGs. The director operated the MSBs using immigrants trafficked illegally into the UK, who worked for the MSB businesses to pay off their debts to the traffickers. The MSB moved around £1 billion to China, around £300 million of which was assessed to be criminal money. The investigation team seized £1.5 million in cash.

Currency exchange

11.11 The 2015 NRA highlighted that many criminal groups require large amounts of foreign currency to pay their suppliers overseas. Cases involving currency exchange MSBs indicate that criminals use MSBs to convert street cash into higher denominations of foreign notes as a precursor to cash movement or cash smuggling across borders. In Northern Ireland, HMRC has found that currency conversion MSBs near the border are a key enabler of the laundering of funds from cross-border crime, with many performing currency exchange services off the record. HMRC is increasingly taking action against these MSBs in Northern Ireland. These border MSBs have also started to experience de-banking, though the structure of the sector is different to elsewhere in the UK.

Box 11.B: Currency exchange

Case study: An Albanian drug trafficking gang operating in London was using various MSBs to convert sterling into high denomination euro notes. The euro notes were then concealed inside vehicles and driven back to the continent. The OCG had formed a relationship with two Albanian brothers who owned internet cafes in London. The brothers constructed MSB kiosks in their shops and used front men to operate the MSBs on their behalf. When the MSBs' owners were confronted, the premises were quickly closed and emptied and the companies deregistered.

Terrorist financing

11.12 The 2015 NRA identified key terrorist financing risks within the MSB sector as complicit employees involved in remitting funds destined for terrorists, terrorist exploitation of the CDD threshold, and low reporting from the sector in relation to terrorist financing. While the due diligence threshold has been lowered from €1,000 to €0 through the Funds Transfer Regulation 2017, the general risks in the sector remain. The low cost of transferring funds and the ability to reach a wide number of jurisdictions linked to terrorism continue to make MSBs an attractive method for moving terrorist funds in small volumes.

Box 11.C: Use of MSBs in terrorist financing

Case study: In 2014, two UK-based individuals sent over £200 to their nephew who was known to be fighting for Daesh in Syria. The funds were transferred through an MSB to a third party in Turkey, to be transferred subsequently to their nephew. Interrogation of one of the individual's computers revealed communications detailing the nephew's activities in Syria, as well as wider support for Daesh. Both individuals were convicted of terrorist financing offences in 2016.

11.13 In Northern Ireland, there is evidence that MSBs have been used to move the proceeds of fraud or VAT evasion designed to fund or support the operations of Northern Irish Related Terrorism (NIRT). It is important to note that boundaries between criminality and terrorism are blurred in Northern Ireland, reflecting the nature of the groups involved.

Supervision, compliance and law enforcement response

11.14 Two supervisors regulate MSBs. HMRC is responsible for the supervision of most MSBs under the MLRs. HMRC is required by the MLRs to maintain a register of those that it supervises and to conduct a 'fit and proper' test on those who apply to be registered as an MSB.[4] The FCA is responsible for supervising MSB activities only where they are undertaken by a firm regulated by the FCA under FSMA such as a bank or an e-money firm offering payment services as part of its registration or authorisation.

11.15 HMRC has increased its supervisory action against MSBs in recent years. In 2014/15, HMRC undertook a significant programme of compliance work and follow-up visits with the largest network principals, reaching networks which covered over 90% of all remittance agents in the UK. HMRC has recently identified significant poor practice in the sector, including: insufficient scrutiny of agents by principals; inadequate training; failing to conduct CDD; inadequate record-keeping and inadequate monitoring of the source of funds and business patterns. Some cases of complicit agents or employees were also identified.[5] While the largest principal MSBs have

[4] The 'fit and proper' test prevents unsuitable individuals, including people with relevant criminal convictions, from holding, or being the beneficial owner of a significant or controlling interest, or holding a management function within an MSB business.

[5] 'UK national risk assessment of money laundering and terrorist financing', HM Treasury and Home Office, October 2015

sophisticated compliance and systems, HMRC considers that other businesses do not allocate sufficient resource to AML/CTF policies and controls. The MLRs should mitigate some of the risks around MSB agents by requiring principals to take steps to ensure that their agents are fit and proper persons.

11.16 HMRC has used risk intelligence to enable better targeting of higher risk areas and has worked with the remittance industry to provide MSBs with revised guidance. HMRC is taking additional action to address poor practice with individual firms and across the sector. While the number of agents continues to make supervision challenging, early improvements in compliance in this area are noticeable.

11.17 Law enforcement agencies judge that complicit MSBs offering money transfer services are a favoured and readily available money laundering vehicle for OCGs. In 2015/16, 10,091 SARs were submitted by the MSB sector.[6] Most of these SARs are raised by the largest MSB principals, with very few SARs filed by the independent MSB sector. The number of SARs reported by the MSB sector has declined by over 13,000 over the past five years. This decline has come from the money transmission and cheque cashing industries, while the number of SARs submitted by currency exchange firms has increased. Some of this decline is likely to be due to streamlining of reporting practices among the largest SARs reporters in the sector.

11.18 An HMRC Proceeds of Crime Intervention Team (POCIT) was set up in 2015 and mainly focuses on money laundering through MSBs. The team seized £4,955,782 from April 2015 to October 2016. In 2016 the Metropolitan Police Service seized £14.5 million of criminal money in relation to money laundering through MSBs. Civil powers in the CFA to seize funds held in bank accounts will extend the scope for law enforcement agencies to take disruptive action against the criminal misuse of MSBs, including where prosecution is not possible.

6 'Suspicious Activity Reports (SARs) Annual Report 2017', NCA, October 2017

Chapter 12
Non-profit organisations

Summary and risks

12.1 The UK's NPO sector is large and diverse and encompasses over 900,000 organisations. The 'charity' sector is the most significant component of the UK's NPO sector both by income and by profile. As of March 2017, there were around 380,000 charities in the UK undertaking a broad range of activities ranging from the small community groups to national arts galleries and international aid organisations.

12.2 The 2015 NRA did not assess the risk of abuse of the NPO sector for money laundering. While there are a small number of instances where it has been proven that charities have been used to launder the proceeds of crime, the use of NPOs is not assessed to be attractive as a means to launder money, and so the risk associated with money laundering is assessed to be low.

12.3 The 2015 NRA assessed the risk of terrorist financing through the NPO sector to be medium-high. While the risks in the sector are unchanged, government and law enforcement agencies have conducted significant work since 2015 to increase understanding of the sector and the risks that it faces around terrorist financing. In comparison to the overall size of the UK charity sector, the amount of known abuse for terrorist financing is very low. It is unlikely that charities have been set up for the purpose of funding terrorism. As such, we now assess the risk of abuse of NPOs altogether for terrorist financing as low, with certain parts of the sector facing significantly higher risks.

Terrorist financing

12.4 Recent work has suggested that the terrorist financing risk to UK charities is concentrated in the subsector comprising the 13,000-16,000 charities operating internationally, particularly in areas such as Syria and Iraq. The ongoing crisis in this region and the threat from Daesh and other terrorist groups mean that these charities are likely to be exposed to the greatest risk. Over 30% of charities in this group have a declared annual income of under £10,000, and therefore may be more vulnerable to such abuse as they are less likely to be able to access professional advice. They may also make honest mistakes and adopt poor practices which make them more vulnerable to abuse. The geographical risk domestically is assessed to be concentrated around charities operating in London, the Midlands and the North-West of England.

12.5 Where charities are linked to terrorist financing activity, a significant proportion are likely to have been victims of internal abuse by employees, volunteers or trustees, with others being victims of looting in country, or identified as linked to aid convoys. It is likely that where abuse has occurred, the charities involved would have been set up for legitimate purposes, but that individuals within the charities or individuals pretending to be associated with the charities have diverted funds for a terrorist cause.

12.6 Charities operating in high risk areas are assessed to be vulnerable to looting of goods or products intended for humanitarian relief. Looting is assessed to be an opportunistic method used by local terrorist groups overseas to obtain goods and funds, and charities operating in high-risk jurisdictions are likely to have underreported the losses of assets and serious incidents, which may inadvertently have led to terrorist financing.

12.7 Financial aid is increasingly part of the policy and aid response to crises, with many charities highlighting the positive impact of money transfers on empowering choice and creating incentive structures for beneficiaries.

12.8 In recent years, in some jurisdictions many charities have experienced transaction delays or denials or account closures by their banks due to concerns around terrorist financing risk. If this trend persists, de-risking may have the effect of pushing charities out of more intensely regulated areas of activity and into higher risk ways of working, such as transacting through physical cash or unregulated MSBs, thereby increasing the risks in the sector. The potential use of physical cash, particularly in high-risk jurisdictions, may make it challenging to ensure that funds are reaching the intended recipients and not directly or indirectly falling into the hands of terrorists, and presents a higher risk for charities operating this way. Technology is also assessed to be an emerging risk for terrorist financing, with many charities in higher risk subsectors making increasing use of websites, social media and online platforms to elicit donations.

Box 12.A: Terrorist financing through NPOs delivering cash

Case study: On 23 December 2016, Syed Hoque and Mashoud Miah were convicted under TACT for funding terrorism. The court heard that Miah and Hoque used Syria bound aid convoys in 2013 to send funds to Hoque's nephew in Syria, who was linked to the Al Qaida aligned group Hay'at Tahrir Al-Sham (formerly al-Nusrah Front). An initial £3,000 was sent via a convoy in July 2013, and £1,500 was later sent via another convoy in December 2013.

Supervision, compliance and law enforcement response

12.9 Charities are not subject to the MLRs, but they, their trustees, employees and volunteers are subject to POCA and counter terrorism legislation. In the UK, charities are also subject to strict wider civil regulatory regimes by one of three charity regulators - the Charity Commission for England and Wales (CCEW), the Charity Commission for Northern Ireland (CCNI) and the Office of the Scottish Charity Regulator (OSCR).

12.10 The CCEW has an effective outreach programme which focuses on those charities identified as higher risk for terrorist financing purposes, and has issued guidance and various regulatory alerts to charities to advise them of the risks and help them better protect themselves from abuse. This is likely to have an impact on the activities of some charities and reduce the risk of abuse from within charities. The CCEW works closely with law enforcement partners in this area to inform its understanding of the risk of abuse to charities and to take action to protect charitable funds and property. The CCEW, jointly with NTFIU, issued a regulatory alert regarding reporting requirements under section 19 of TACT in September 2015. This acted as a reminder for charities and their staff of the reporting obligations under TACT 2000 to suspicion or belief that a terrorist financing offence has been committed.

12.11 OSCR publishes guidance to help charity trustees understand their legal responsibilities in managing and controlling charities. Recently, OSCR has started to make more active use of social media and the internet to promote key publications and guidance. OSCR also engages with Scottish charities by organising and participating in a range of events aimed at facilitating compliance. Where issues are identified with a group of charities, OSCR will work with any relevant umbrella charity that provides support or guidance to that group of charities. The OSCR risk framework is used to decide on the specific topics covered in events, and identifies organisations working in fragile states as a risk. As a result, OSCR has actively engaged with the Network of International Development Organisations and the International Development department of the Scottish Government on this area.

12.12 Charities registered with the CCNI are primarily domestically focused. The CCNI regulates the sector through a holistic approach including outreach, reviews and regulatory interventions to improve governance, accountability and the application of charity property towards the public benefit. This approach aims to safeguard charities and prevent their property being misapplied, including for terrorist financing.

Chapter 13
Gambling

Summary and risks

13.1 The 2015 NRA identified the main risks in the gambling sector as being: negligent gambling operators allowing money laundering in the sector through poor compliance with the Money Laundering Regulations 2007 and POCA; criminals gaining control of a licensed gambling business and using it as a cover for money laundering; the sector's exposure to criminals' lifestyle spending; criminals using products and services to store and move the proceeds of crime; and cash transactions by anonymous customers. The Gambling Commission's 2016 risk assessment highlights that these risks generally continue.[1] While recognising that the level of money laundering and terrorist financing risk varies across gambling sectors, it notes that a significant proportion of the money laundering that takes place within the industry is by criminals spending the proceeds of crime (including acquisitive crime and the sale of illicit commodities) for leisure rather than 'washing' criminal funds. More specifically, the Gambling Commission's risk assessment notes that betting (non-remote), casinos (non-remote) and remote (casinos, betting and bingo) all carry significantly higher risks than other gambling sectors.

13.2 The 2015 NRA assessed overall that the gambling sector was less attractive to criminals than other sectors and less exploited to launder significant volumes of criminal funds. Due to the continued lack of evidence of the use of the sector for money laundering on a significant scale, the sector continues to be assessed as **low** risk for money laundering. Neither regulated nor unregulated gambling are judged to be attractive for terrorist financing, and we have seen no evidence of these services being abused by terrorists, so the terrorist financing risk associated with the sector is **low**.

13.3 The gambling sector comprises remote and non-remote licensed casinos, remote and on and off-course betting, remote and non-remote bingo and lotteries, and arcades.[2] At the time of the 2015 NRA, there were almost 150 land-based casinos in UK (with a 16% share of the licensed gambling market), 170 remote casino licences and 9,000 licensed betting shops. As of

[1] 'Money laundering and terrorist financing risk within the British gambling industry', Gambling Commission, October 2016

[2] Remote casinos are those offering account-based gambling offered to GB consumers through the use of remote communication such as internet; telephone; television; radio or any other kind of electronic for communication remotely.

2016, there were 147 land-based casinos in the UK, 177 remote casinos and 8,788 licensed betting shops.[3]

13.4 Currently, only remote and non-remote casinos are subject to the MLRs. The government is required to keep the position of other gambling providers under review. All gambling operators are required by POCA to be alert to money laundering and disclose knowledge or suspicions of money laundering to the NCA.

Casinos

13.5 The 2015 NRA reported that both remote and non-remote casinos are vulnerable to criminal control and the ability to use certain elements of casino services to store or transfer funds. The large cash payments element, the relative lack of familiarity between the casino and the customer, the ability to exchange chips between third parties, the ability to open a customer account through which funds can be stored or remitted, and the ability to use foreign exchange and safety deposit services continue to expose the sector to the risk of money laundering including through criminal lifestyle spending. Recent legislative and regulatory changes outlined below should, however, help to mitigate some of this risk.

13.6 The 2015 NRA highlighted the potential risk posed by criminal use of casino chips and of Ticket In Ticket Out (TITO) vouchers, which can be obtained from machines in casinos, arcades or betting shops. Law enforcement agencies have observed TITO vouchers being used to launder tens of thousands of pounds, whereby criminals obtain the vouchers and cash out at a later date to disguise the origin of funds. The CFA included steps to address this risk, introducing powers which will allow law enforcement agencies to seize TITO vouchers and casino chips.

Box 13.A: Casinos

Case study: Over a five year period an individual deposited over £600,000 in cash at five different casinos. In the absence of a bank account, he used the casinos to hold these funds on his behalf. He subsequently gambled and generated winning cheques that were then paid into the bank account of a family member. This individual was subsequently convicted for the offence of money laundering during the relevant period.

13.7 Recent supervisory action has restricted the risks posed by overseas customers. This has included addressing the risk posed by junkets, whereby casino agents take deposits from overseas clients travelling to the UK to play in higher end casinos. However, due to differing levels of regulatory controls, use of overseas remote casinos by UK customers is still assessed to pose a risk.

Retail betting

13.8 The 2015 NRA identified the main money laundering risks faced by the non-remote betting sector as the combination of anonymity and extensive use of

[3] 'Industry statistics: April 2013 to March 2016', Gambling Commission, May 2017

cash in the sector. At a high level, these risks are not thought to have changed since 2015, though as with the casino sector, retail betting remains more exposed to criminal lifestyle spending than being used to integrate criminal funds into the wider economy.

13.9 Those products which include cash payment and a lack of face-to-face interaction pose a greater risk than other areas, though this may be mitigated by cash payment limits. The speed with which funds can be cashed in and out, the high level of footfall, the ability to deposit and withdraw on different dates and locations, the international reach of remote operators and the ease with which customers can move between operators (without information being shared) continue to pose further risks. Law enforcement agencies have also observed criminals using remote gambling sites to transfer illicit funds through peer-to-peer play and to move funds between online accounts and land based betting shops.

Box 13.B: Retail betting

Case study: A criminal gang targeted ATM machines in Scotland for theft. The gang then employed a network to launder the stolen funds through Fixed Odds Betting Terminals (FOBT) in numerous betting shops in England, inserting the stolen notes from the ATM machines into TITO enabled machines. The network played minimally and then cashed out tickets at the betting counter to break the audit trail of the laundered cash.

13.10 The advent of self-service betting terminals, contactless payments and payment cards issued by operators are all areas which may pose emerging risks not identified in 2015. FOBTs have been perceived as a risk, though recent regulatory amendments have somewhat mitigated the risks through encouraging the move towards account-based play, making it easier for operators to monitor play and mitigate the risks.[4]

Supervision, compliance and law enforcement response

13.11 All gambling operators offering services in Great Britain must be licensed by the Gambling Commission, including operators based overseas offering services to consumers in Great Britain. Only casinos are subject to the MLRs. The licensing objectives include the prevention of gambling being used as a source of, associated with or used to support crime or disorder. In 2016, the Gambling Commission amended its licensing conditions and codes of practice for all operators in relation to the prevention of crime associated with gambling, with a particular focus on AML/CTF provisions. While the Gambling Commission's remit does not extend to Northern Ireland, casinos are banned in Northern Ireland and law enforcement agencies in Northern Ireland do not see gambling as a material money laundering risk.

13.12 The 2015 NRA reported that non-remote casinos had some weaknesses in their systems and controls, in particular with respect to CDD, PEPs, SARs and

[4] Evaluation of Gaming Machine (Circumstances of Use) (Amendment) Regulations 2015, Department for Culture, Media and Sport, January 2016

MLRO responsibilities. The Gambling Commission has continued to observe cases of poor practice in record keeping and due diligence checks in non-remote casinos, and law enforcement agencies have observed a recent increase in allegations of corruption in these casinos. The Gambling Commission has recently amended licence requirements for all licensed operators to mitigate these risks, requiring casinos (and others) to conduct an assessment of the risks of their business being used for money laundering and ensure they have appropriate policies, procedures and controls in place.

13.13 Several casino operators and trade bodies have worked with the Gambling Commission in order to establish an effective common approach to operators meeting their responsibilities. The non-remote casino industry has developed guidelines, through the National Casino Forum and with the Gambling Commission's assistance, with the aim of providing the sector with guidance on good practice in AML/CTF controls.

13.14 Retail betting operators are not covered by the MLRs, so are not required to verify or record customer identity, but are required through the Gambling Commission's licensing regime to have regard to guidance issued relating to their compliance with POCA and to prevent gambling being used for crime.[5] The 2015 NRA highlighted the wider licensing obligations faced by betting operators, but suggested that compliance with these requirements was mixed. However, due to increased awareness, the retail betting industry has taken steps recently (including through creation of the Gambling Anti-Money Laundering Group and the subsequent publication of a money laundering risk assessment) to mitigate the risks of money laundering, primarily through improvements in appropriate systems and controls.

13.15 Obligations under POCA apply to all gambling operators. POCA places an obligation on the gambling operator to submit a SAR where operators know or have suspicion that a person is engaged in money laundering. The 2015 NRA identified that SARs from the gambling sector had seen an upward trend due to work by the Gambling Commission and the NCA. These trends have continued, with SARs increasing from 704 in 2013/14 to 1,564 in 2015/16.[6] Between October 2015 and March 2017, the UKFIU participated in a number of workshops with firms and the Gambling Commission to improve knowledge around CDD and SARs. The UKFIU has seen a considerable improvement recently in SAR quality and understanding of the sector's obligations under the MLRs.

[5] The Gambling Commission publishes advice to non-casino operators on complying with POCA, which includes advice on "know your customer" (KYC) checks, but does not mandate these checks. An ordinary code provision within the Gambling Commission's licensing conditions requires non-casino operators to act in accordance with this advice.

[6] 'Suspicious Activity Reports (SARs) Annual Report 2017', NCA, October 2017

Chapter 14
High value dealers

Summary and risks

14.1 An HVD is defined under the MLRs as any business receiving or making high value cash payments of €10,000 or more (reduced from €15,000 under the Money Laundering Regulations 2007) either in a single payment or a linked series, in exchange for goods. There were around 1,300 HVDs registered in 2015. The number of registered businesses is now just over 700. As any business passing HMRC's approval process can become an HVD, it is inherently difficult to assess the extent of under-registration.

14.2 The 2015 NRA highlighted that the services, products and level of cash use in the HVD sector can make HVD businesses attractive to criminals seeking to convert criminal proceeds into high value or luxury portable assets which can be easily moved outside the UK, or used to conceal the origins of criminally derived cash. The risks posed by the sector were assessed in 2015 to be low relative to other sectors due to the limited ability for criminals to use HVDs to facilitate the laundering of large sums of money. The vulnerabilities in the sector persist, but HVDs are not assessed to present an attractive option for laundering large sums of money or moving terrorist funds, and so the sector is assessed as relatively low risk for both money laundering and terrorist financing.

Money laundering through HVDs

14.3 HMRC divides its supervised HVD population into 25 subsectors, but assesses that the three highest risk areas are motor vehicles, jewellery and alcohol, which make up 55% of all registered businesses. HMRC has seen a drop in the number of alcohol businesses registered in recent years; this may be in part due to tighter controls on HMRC's Alcohol Wholesaler Registration Scheme and in part due to more robust checks on HVD applications.

14.4 The risks around the alcohol sector relate both to criminals using legitimate alcohol trade fronts to facilitate money laundering and criminals trading in illicit, non-duty paid alcohol. HMRC has estimated that the illicit alcohol trade results in duty losses of up to £1.3 billion per year, though only a proportion of this is likely to be laundered through the HVD sector.

Box 14.A: High value dealers

Case study: A wholesale alcohol trader used its high value dealer status to launder money. Its bank account was credited with around £3 million in cash deposited at various bank accounts. The funds were then transferred to other business and personal bank accounts.

14.5 Intelligence has indicated that the sector's attractiveness to criminals is increasing, possibly as a result of displacement from the MSB sector, which has been the subject of stronger law enforcement and regulatory action in recent years. In addition, HMRC has recently identified high levels of criminality within the HVD sector with a large number of individuals seeking to register having been convicted or suspected of involvement of criminal activity, leading to an increased risk of businesses being involved in money laundering.

Supervision, compliance and law enforcement response

14.6 Some businesses do not carry out due diligence to a sufficiently high standard before accepting high value payments, and firm risk assessments are not always addressed to the specific risks of the business. HMRC is aware that many businesses have a good level of awareness of the money laundering and terrorist financing risks associated with large cash payments. Many of these businesses have policies in place against accepting or making high value payments in cash. However, in the registered population, many businesses still have insufficient awareness of these risks.

14.7 Recent changes through the MLRs should mitigate some of the risks identified within the sector. The threshold for requiring registration as an HVD has fallen, and will now apply to those businesses making as well as receiving high value payments from €10,000 (reduced from €15,000). The MLRs also introduce an approval test for HVDs, prohibiting registration for supervision by those with an unspent relevant criminal conviction. The risks of money laundering and criminality in specific parts of the sector should also be mitigated through wider supervision, regulatory or economic changes. For example, the Scrap Metal Dealers Act 2013 made it illegal for anyone to buy scrap metal using cash. HMRC has also refined its HVD registration process to scrutinise higher risk applications in more detail before they are approved, to ensure that inappropriate or unsuitable applicants for registration are not admitted onto the HVD register.

14.8 Law enforcement agencies have raised concerns that the low number of SARs (particularly when compared to the number of SARs submitted by other sectors against HVDs) restricts the level of intelligence available on the sector. The number of SARs submitted by the sector in 2015/16 was 152, an

increase compared to the previous year but significantly lower than those submitted in 2012/13 or 2013/14.[1]

[1] 'Suspicious Activity Reports (SARs) Annual Report 2017', NCA, October 2017

Annex A

Methodology

A.1 The methodology used for the 2017 NRA was similar to that used for the 2015 NRA. This follows the three key stages identified in FATF guidance, of identification, assessment and evaluation of evidence within the context of the 'Management of Risk in Law Enforcement (MoRiLE) model. Unlike 2015, the same methodology was used for both the money laundering and terrorist financing elements of this assessment.

A.2 Several key terms used throughout the assessment are defined below:

- Threat – People or activities with the potential to cause harm. Money laundering threats include predicate offences and criminals who commit them, while terrorist financing threats include those groups and individuals conducting terrorist activity.
- Vulnerability - Things that can be exploited by the threat. Vulnerabilities can also be reduced through mitigation.
- Consequence - The impact or harm that money laundering or terrorist financing may cause, including the effect of the underlying criminal and terrorist activity on financial systems and institutions.
- Risk - A function of threat, vulnerability and consequence. Inherent risks can be weighed against mitigating factors to assess net risks.

A.3 The first stage of the assessment, identification, focused on identifying evidence which had emerged since the last NRA was conducted in 2015. This included evidence submitted by law enforcement agencies, government departments, supervisors, firms and non-governmental organisations, as well as other published evidence. After collecting and reviewing this evidence, further evidence was gathered to fill gaps identified. Calls for evidence were issued to all supervisory bodies and firms in all sectors considered, and roundtables or bilateral meetings were held to follow these up where possible. Altogether, this resulted in contributions submitted by over 200 organisations across the different sectors considered, with evidence gathering prioritised according to the risk profiles involved.

A.4 The second stage involved analysing the data provided by stakeholders to establish the risks present, assess the likelihood of them materialising, and understand their impact. Evidence for all sectors, activities or products considered was categorised against one of the following risk factors under the categories of threat, vulnerability, likelihood and mitigation:

- ability to use the product or service to mask the source or ownership of asset
- ability to use the product or service to mask the destination of funds
- level of complexity of the product or service
- level of exposure of the product or service to high risk persons or jurisdictions
- speed with which transactions relating to the product or service can be completed
- typical volume and frequency of transactions relating to the product or service
- accessibility of the product or service
- criminal or terrorist intent to exploit the product or service
- capacity and capability of law enforcement agencies to mitigate the money laundering or terrorist financing risks around the product or service
- capacity and capability of supervisors or regulators to mitigate the money laundering or terrorist financing risks around the product or service
- capacity and capability of firms to mitigate the money laundering or terrorist financing risks around the product or service

A.5 Given the largely hidden nature of money laundering and terrorist financing, the evidence used to assess these risk factors relies on a combination of hard data, case studies and expert judgment from law enforcement agencies, supervisory authorities and those responsible for AML/CTF within firms.

A.6 The final stage of the assessment was the evaluation of the relative exposure of each sector to risk using the identified and assessed evidence. As part of this, areas were ranked by relevant experts from government and law enforcement against the risk factors outlined above, using an adapted Management of Risk in Law Enforcement (MoRiLE) model to establish money laundering and terrorist financing risk rankings for each area. The MoRiLE model evaluates inherent risk, based on vulnerabilities and the likelihood of criminals or terrorists exploiting these, followed by evaluating mitigating factors to calculate the net risk in an area. The consequences of criminals or terrorists successfully moving money through a particular sector or area were also considered throughout this assessment.

A.7 It should be noted that the risk rating is a relative assessment, and a rating of low risk does not mean that there is no risk within a sector. Money laundering and terrorist financing may still take place through low risk sectors at a significant level and all sectors or areas covered are assessed to be exposed to some level of risk.

Annex B

Glossary

4MLD	EU Fourth Anti-Money Laundering Directive
5MLD	EU Fifth Anti-Money Laundering Directive
ACE	Asset Confiscation Enforcement
AML	Anti-money laundering
BEIS	Department for Business, Energy & Industrial Strategy
CCEW	Charity Commission for England and Wales
CCNI	Charity Commission for Northern Ireland
CDD	Customer due diligence
CFA	Criminal Finances Act 2017
CRS	Common Reporting Standard
CSEW	Crime Survey for England and Wales
CTF	Counter-terrorist financing
CTU	Counter-Terrorism Unit
CPS	Crown Prosecution Service
DAML (SARs)	Defence Against Money Laundering SARs
EDD	Enhanced due diligence
EU	European Union
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
GCHQ	Government Communications Headquarters
HMRC	Her Majesty's Revenue and Customs
HVD	High value dealer
JFAC	Joint Financial Analysis Centre
JMLIT	Joint Money Laundering Intelligence Task Force
LLP	Limited liability partnership
LP	Limited partnership
MER	Mutual evaluation report

MLRO	Money Laundering Reporting Officer
MLRs	Money Laundering Regulations 2017
MOU	Memorandum of Understanding
MPS	Metropolitan Police Service
MSB	Money service business
NCA	National Crime Agency
NPO	Non-profit organization
NRA	National risk assessment
NTFIU	National Terrorist Financial Investigation Unit
OCG	Organised Crime Group
OFSI	Office of Financial Sanctions Implementation
OPBAS	Office for Professional Body AML Supervision
OSCR	Office of the Scottish Charity Regulator
PEP	Politically exposed person
POCA	Proceeds of Crime Act 2002
PSC	People with significant control
PSNI	Police Service of Northern Ireland
RART	Regional Asset Recovery Team
ROCU	Regional Organised Crime Unit
SAR	Suspicious activity report
SFO	Serious Fraud Office
SLP	Scottish limited partnership
SRA	Solicitors Regulation Authority
TACT	Terrorism Act 2000
TAFA	Terrorist Asset-Freezing etc. Act 2010
TCSP	Trust or company service provider
UKFIU	UK Financial Intelligence Unit
UNSCR	United Nations Security Council Resolution

HM Treasury contacts

This document can be downloaded from www.gov.uk

If you require this information in an alternative format or have general enquiries about HM Treasury and its work, contact:

Correspondence Team
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

Tel: 020 7270 5000

E-mail: public.enquiries@hm-treasury.gov.uk