HM Treasury

Home Office

UK national risk assessment of money laundering and terrorist financing

October 2015

HM Treasury

Home Office

UK national risk assessment of money laundering and terrorist financing

October 2015

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 978-1-910835-57-9
PU1851

Contents

		Page
Executive summary		3
Chapter 1	Methodology	9
Chapter 2	Legal and regulatory framework	13
Chapter 3	Predicate offences	19
Chapter 4	UK law enforcement	23
Chapter 5	Supervision	29
Chapter 6	Regulated sectors	31
Chapter 7	Legal entities and arrangements	67
Chapter 8	Cash	75
Chapter 9	New payment methods	79
Chapter 10	International exposure	85
Chapter 11	Terrorist financing	89
Annex A	Full list of AML/CFT supervisors	99
Annex B	Glossary	101

Executive summary

This is the UK's first money laundering and terrorist financing national risk assessment (NRA). In conducting this assessment the aim is to identify, understand and assess the money laundering and terrorist financing risks faced by the UK.

Money laundering can undermine the integrity and stability of our financial markets and institutions. It is a global problem. The European Commission's 2013 impact assessment of the EU anti-money laundering/counter terrorist financing legislative framework points to global criminal proceeds potentially amounting to some 3.6% of GDP; around US$2.1 trillion in 2009.[1]

The best available international estimate of amounts laundered globally would be equivalent to some 2.7% of global GDP or US$1.6 trillion in 2009.[2] Both money laundering itself, and the criminality which drives the need to launder money, present a significant risk to the UK.

The laundering of proceeds of overseas corruption into or through the UK fuels political instability in key partner countries. The NCA judges that billions of pounds of suspected proceeds of corruption are laundered through the UK each year.

Money laundering is also a key enabler of serious and organised crime, the social and economic costs of which are estimated to be £24 billion a year.[3] Taken as a whole, money laundering represents a significant threat to the UK's national security. The government's 2013 Serious and Organised Crime Strategy set out plans to make it harder for criminals to move, hide and use the proceeds of crime.[4]

There is a marked overlap between money laundering and terrorist financing – both criminals and terrorists use similar methods to store and move funds. However, the motive for generating and moving funds differs. Terrorists ultimately need money to commit terrorist attacks. Unlike criminal gangs, terrorist groups involve disparate individuals coming together through a shared motivation and ideology.

Finance is an essential aspect of enabling terrorist groups to function, recruit and commit terrorist acts. A lack of funds can have a direct effect on the ability of terrorist organisations and individuals to operate and to mount attacks. There is evidence of terrorist financing activity in the UK and terrorist financing poses a significant threat to the UK's national security.

The UK recognises that countering terrorist financing is important in protecting national security. Countering terrorist financing forms a key part of the UK's CONTEST counter-terrorism strategy with the aim being to reduce the terrorist threat to the UK and its interests overseas by depriving terrorists and violent extremists of the financial resources and systems required for terrorism-related activity.[5]

[1] 'Impact Assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering, including terrorist financing and Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds', European Commission, February 2013

[2] 'Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes: Research report', UNODC, October 2011. This estimate would be within the IMF's original 'consensus range', equivalent to some 2.7% of global GDP (2.1 – 4%) or US$1.6 trillion in 2009.

[3] 'Understanding organised crime: estimating the scale and the social and economic costs', Home Office, October 2013

[4] 'Serious and Organised Crime Strategy', HM government, October 2013

[5] 'CONTEST: The United Kingdom's Strategy for Countering Terrorism', HM government, July 2011

The national risk assessment

The objective of the NRA is to better understand the UK's money laundering and terrorist financing risks, inform the efficient allocation of resources and mitigate those risks. While this assessment should not be relied upon in isolation, the improved understanding it provides should assist the government, law enforcement agencies, supervisors and the private sector in targeting their resources at the areas of highest risk, ensuring that the UK's approach to preventing financial crime is risk-based and proportionate. The Financial Action Task Force (FATF) sets international standards on anti-money laundering and counter financing of terrorism (AML/CFT).[6] Conducting a NRA is an obligation under the FATF recommendations,[7] and the UK is committed to the FATF standards.

This NRA is the product of extensive consultation with law enforcement agencies, UK intelligence agencies, the UK Financial Intelligence Unit, supervisors and private sector representatives. It serves as a stock-take of the collective knowledge of money laundering and terrorist financing, the current intelligence gaps, and the effectiveness of the current response across government, law enforcement agencies and the regulated and private sectors. The relative weight given to each of the areas covered in this report is reflective of the extent of that collective knowledge in relation to the area, and the scale of current intelligence gaps, as well as the availability of information which is not too sensitive for publication. The volume of information provided on an area or sector is not reflective of the government's view of the relative risk within that area.

The findings of the NRA will shape the government's response to money laundering and terrorist financing, and will inform the risk-based Anti-Money Laundering Action Plan that the Home Office and HM Treasury have committed to producing.[8]

The UK is a global financial centre. Trillions of pounds worth of transactions are made each year, and UK banks, and their subsidiaries, operate around the globe. The same factors that make the UK an attractive place for legitimate financial activity – its political stability, advanced professional services sector, and widely understood language and legal system – also make it an attractive place through which to launder the proceeds of crime. In response to this the UK has developed its anti-money laundering and counter financing of terrorism (AML/CFT), regime over a number of years. This regime is well developed in a number of respects, although areas for improvement remain.

Key findings

The UK's law enforcement agencies know most about cash-based money laundering, particularly cash collection networks, international controllers, and money service businesses, although some gaps in knowledge remain. This is a result of the resources that law enforcement agencies have invested over a number of years in tackling cash-based money laundering and the drugs trade (which largely generates proceeds in the form of cash) which has long been recognised, and continues to be recognised, as posing a high money laundering risk.

The size and complexity of the UK financial sector mean it is more exposed to criminality than financial sectors in many other countries, including abuse enabled by professional enablers in

[6] The Financial Action Task Force (FATF) is an independent inter-governmental body that develops global standards to protect the financial system against money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction.

[7] 2012 FATF Recommendation 1 and its interpretative note

[8] 'The UK Anti-Corruption Plan', HM government, December 2014

the legal and accountancy sector. There are significant intelligence gaps, in particular in relation to 'high-end' money laundering. This type of laundering is particularly relevant to major frauds and serious corruption, where the proceeds are often held in bank accounts, real estate or other investments, rather than in cash. UK law enforcement agencies want to know more about the role of the financial and professional services sectors (banks, legal, accountancy and trust and company service providers) in money laundering. They judge the threat in these sectors to be significant, and are still establishing the strength of understanding needed in this area.

The intelligence picture in other areas – such as high value dealers, gambling, and new payment methods – is mixed. This NRA has found that, while in some cases individual agencies or supervisors have a good understanding of the risks in these areas, the collective understanding of law enforcement agencies, supervisors and the private sector is limited. On the basis of what is known, the risks in these areas appear to be lower relative to those posed by cash-based money laundering and 'high-end' money laundering through the financial and professional services sectors.

The effectiveness of the supervisory regime in the UK is inconsistent. Some supervisors are highly effective in certain areas, but there is room for improvement across the board, including in understanding and applying a risk-based approach to supervision and in providing a credible deterrent. The large number of professional body supervisors in some sectors risks inconsistencies of approach. Data is not yet shared between supervisors freely or frequently enough, which exposes some supervised sectors where there are overlaps in supervision.

The majority of those working in the regulated sector are not complicit in money laundering or terrorist financing. However those working in the regulated sector may aid those involved in money laundering, either unwittingly, or through negligence or non-compliance. Non-compliant or negligent professionals have the potential to cause significant harm by facilitating money laundering and causing reputational damage to their profession.

The law enforcement response to money laundering has been weak for an extended period of time. It has not been a priority for most local police forces (although the metropolitan forces appear to provide a more effective response). Since 2012, the government has invested in developing the capabilities of Regional Organised Crime Units (ROCUs).

In 2013, the National Crime Agency (NCA) was launched. Within the NCA, the Economic Crime Command leads the national response to economic crime, including money laundering. The NCA has a programme of work in place to build a better intelligence picture and respond to 'high-end' money laundering. It also chairs the multi-agency criminal finances threat group, which aims to steer a comprehensive response by law enforcement agencies to the threat posed by money laundering, including cash-based money laundering, non-cash money laundering and professional enablers. The NCA's National Intelligence Hub, responsible for producing the authoritative national assessment of the threat posed by serious and organised crime, established a dedicated money laundering threat desk in 2014.

The suspicious activity reports (SARs) regime obliges entities in the regulated sector to report suspicions of money laundering or terrorist financing to the UK Financial Intelligence Unit (UKFIU), which is part of the Economic Crime Command in the NCA. Last year, over 350,000 SARs were filed with the UKFIU, the vast majority of them submitted by the financial sector.[9] SARs form a critical intelligence resource, and enable law enforcement agencies to intervene to prevent suspicious transactions. The SARs regime also provides SARs reporters with a mechanism

[9] 'Suspicious Activity Reports (SARs) Annual Report 2014', National Crime Agency, December 2014

to obtain a statutory defence from a money laundering or terrorist financing prosecution when they report suspicion.

Supervisors and private sector representatives consulted in the course of producing the NRA voiced repeated criticism of the SARs regime. In December 2014 the government committed to reviewing the regime.[10] This will provide an opportunity for individuals and firms in the regulated sector, supervisors and law enforcement agencies to make proposals for improvements to the regime, and in particular to ELMER, the database for suspicious activity reports. ELMER is now reaching the end of its life, which may create risks to the effectiveness of the UK's anti-money laundering regime, and will need to be replaced soon. The government responded to the regulated sector's concerns about their vulnerability to civil litigation as a result of submitting SARs by legislating in the Serious Crime Act 2015 to provide all reporters with statutory immunity from civil liability when submitting SARs in good faith.

The private sector holds much of the data needed to succeed in the fight against money laundering and terrorist financing. The Joint Money Laundering Intelligence Taskforce (JMLIT) pilot, established in February 2015, is a shared endeavour to create an environment in which the financial sector and law enforcement agencies can exchange and analyse information and intelligence. Increasing collaboration between law enforcement agencies, supervisors and the private sector is essential to help prevent and detect money laundering and terrorist financing, and protect the UK from their effects.

Next steps

This NRA shows that the collective knowledge of UK law enforcement agencies, supervisors and the private sector of money laundering and terrorist financing risks is not yet sufficiently advanced. The UK's response is well developed, but more needs to be done to ensure it is commensurate with our status as a well regulated global financial centre.

The government has already committed to publishing an Anti-Money Laundering Action Plan.[11] That action plan will set out how the government will work with supervisors and the private sector to address the risks identified in this NRA. It will build on the 2013 Serious and Organised Crime Strategy and the actions it contains to make it harder to move, hide and use the proceeds of crime.

The overall objective will remain to ensure the financial system is a hostile environment for illicit finance while minimising the burden on legitimate businesses and individuals.

The priorities for the action plan will be:

- plugging intelligence gaps, particularly those associated with 'high end' money laundering through the financial and professional services sectors
- enhancing our law enforcement response to tackle the most serious threats
- reforming the suspicious activity reports (SARs) regime, and upgrading the capabilities of the UK Financial Intelligence Unit (UKFIU)
- addressing the inconsistencies in the supervisory regime that have been identified through this assessment

[10] 'UK Anti-Corruption Plan', HM government, December 2014

[11] 'UK Anti-Corruption Plan', HM government, December 2014

- working with supervisors to improve individuals' and firms' knowledge of money laundering and terrorist financing risks in key parts of the regulated sector to help them avoid getting drawn into money laundering
- transforming information sharing between law enforcement agencies, the private sector and supervisors, building on the progress already made through the JMLIT

The UK is periodically assessed under mutual evaluations by the FATF. The NRA and the action plan will be kept under review and will inform the UK's next evaluation.

The government is committed to ensuring the UK Anti-Money Laundering regime is effective and proportionate, with businesses and regulators taking a risk-based approach to implementation. The Better Regulation Executive is leading a 'red tape' review into the UK Anti-Money Laundering regime, including a call for evidence in September and October 2015 to identify, for example, where companies are confused as to what is required or are undertaking unnecessary activity which diverts attention away from where there are real risks. The results of this review will inform the action plan. Further information can be found here: https://cutting-redtape.cabinetoffice.gov.uk/anti-money-laundering

1 Methodology

1.1 In establishing the methodology for this assessment, the government took into account the models developed by others, including the World Bank and IMF, the approach taken by other countries, the FATF guidance and views expressed in consultation with key stakeholders of the UK's AML/CFT regime. The assessment followed the three key stages identified in FATF guidance, of identification, assessment and evaluation.

1.2 A number of key terms used throughout the assessment are defined below:

- Threat -

  Is a person or group of people, object or activity with the potential to cause harm to, for example, the state, society, the economy etc. Threat is one of the factors relating to risk; typically it serves as the starting point in developing an understanding of money laundering/terrorist financing risk.

- Vulnerability -

  When used in a risk assessment, vulnerability is a concept encompassing things that can be exploited by the threat or that may support or even facilitate its activities. Distinct from threat, vulnerabilities are factors that represent weaknesses in the AML/CFT systems.

- Consequence -

  Refers to the impact or harm that money laundering or terrorist financing may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions.

- Risk -

  Can be seen as a function, or combination, of threat, vulnerability and consequence. For a risk assessment to be distinct from other assessments, for example a threat assessment, a measure of judgement on the threats, vulnerabilities and consequence/impact should ideally be included.

1.3 There is a significant overlap between money laundering and terrorist financing in the methods used by criminals and terrorists to raise, store and move funds. However, the motive of the perpetrators, and so the threat to the UK, from terrorist financing is different. For this reason this document includes a chapter specifically focusing on the financing of terrorism (chapter 11). Those in the regulated sector should be aware that the vulnerabilities set out in rest of the document can apply equally to facilitating money laundering and aiding the financing of terrorism.

Data collection and consultation

1.4 The first stage of the assessment, identification, focused on gathering information through consultation with a broad range of stakeholders. This was in order to identify vulnerabilities and threats. Firstly we held a series of workshops and bilateral meetings with a broad range of stakeholders including firms and industry representatives from the sectors subject to the Money Laundering Regulations, law enforcement agencies, supervisory authorities, other government departments and NGOs.

1.5 Previous assessments conducted by law enforcement and other bodies were used to assist in identifying the main threats to the UK. Business activities presenting risk were identified and prioritised according to the level of risk. Workshops were held with some sectors and questionnaires issued to others. In addition to the annual reporting process for supervisors, they were each asked to complete a questionnaire specifically for this assessment.

1.6 The second stage involved analysing the data provided by stakeholders to establish the risks present, and understand their impact. Given the largely hidden nature of money laundering and terrorist financing, the data used for this assessment is, in places, partial, inconsistent or contradictory. The conclusions of the assessment in this paper draws heavily on expert judgment from law enforcement agencies, supervisory authorities and those responsible for AML/CFT within firms.

1.7 The risks identified were tested through a peer review process with stakeholders. Peer review workshops were conducted on a sector by sector basis, including industry representatives, supervisors and law enforcement agencies. Stakeholders were invited to submit any necessary additional information to support their views.

1.8 As a result this assessment represents the broad views of all those participating in the UK's AML/CFT regime from regulated firms in the private sector, to police forces and national law enforcement agencies, government departments and supervisory authorities. It also reflects input from leading NGOs in this area including Global Witness and Transparency International.

Risk rating

1.9 The final stage of the assessment was the evaluation of the relative exposure of each sector to risk. As part of this, areas were ranked on the basis of risk, using a model developed from the NCA's draft Management of Risk in Law Enforcement (MoRiLE), which was amended to reduce the dependency on quantitative data and include factors for qualitative assessment. The methodologies used by the World Bank and International Monetary Fund were also considered during the development phase. The terrorist financing risks were assessed separately.[1]

1.10 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 may still take place through low risk sectors at a significant level, and, as compliance is one of the factors considered in the risk assessment, sectors still need to invest significant effort to strengthen their AML/CFT controls in order to address the threats and vulnerabilities they face.

1.11 The NRA risk rating model assesses the structural risk within each area, based on a series of factors to indicate the vulnerability of a particular sector to money laundering and the relative likelihood that the threat of money laundering will materialise in that a particular sector, given there is general threat to the UK that criminals will attempt to launder money through some means, and all the sectors covered below can be used to launder money.

1.12 It should also be noted that this model focuses on the risk of businesses in a sector being used by criminals to facilitate money laundering, wittingly or unwittingly, due to the services it offers, rather than the risk that business itself is established as a front for money laundering. The risks with regard to criminal spend, or the use of the business itself to conceal money laundering, may be substantially different.

[1] Chapter 11 focuses specifically on the financing of terrorism.

1.13 The assessment has also looked at means of transferring funds that provide a degree of anonymity, and so present a greater risk than payments through the conventional payment systems that are directly linked to a bank account, such as debit/credit card payments, direct debit or other transactions through bank payment systems.

1.14 A range of factors were considered when assessing the risk within the sectors, including law enforcement agencies' existing knowledge of money laundering through the sector, where a lower level of knowledge represents a vulnerability and so a higher level of risk.

1.15 The factors considered when assessing the vulnerability of a particular sector or area include:

- the relative complexity and reach (national/international) of the services offered by the sector, or the capacity to move money internationally given the nature of the funds (i.e. cash, e-money)
- the relative volume and speed of money movement through firms in the sector, or the volume and speed of money movement given the nature of the funds
- the level of compliance within the sector

1.16 For factors such as complexity, reach and volume, and speed of money movement the ratings are based on the nature of business undertaken by the majority of the sector.

1.17 The factors considered when assessing the likelihood that a threat will materialise in a particular sector/area include:

- the size of the sector or area
- the likelihood that the sector will report suspicious activity to law enforcement, as indicated by the level of SAR submission by the sector
- law enforcement agencies' existing knowledge of money laundering through the sector

1.18 The consequences of criminals successfully laundering money through a particular sector were assumed to be severe for all the areas covered.

1.19 Following the scoring of vulnerabilities and likelihoods, the matrix produces a score for the thematic area's risk, which is then categorised into Low, Medium or High risk levels. The model then considers the mitigating measures in place in terms of UK law enforcement agencies and supervisors' capability and capacity to combat money laundering in that area. The combined mitigation score has the potential to reduce the overall risk level of a thematic area where law enforcement/supervisory activity effectively mitigates the risk. Once applied, an overall risk score for the thematic area is calculated and then categorised.

Table 1.A: National risk assessment on money laundering

National risk assessment on money laundering						
Thematic area	**Total vulnerabilities score**	**Total likelihood score**	**Structural risk**	**Structural risk level**	**Risk with mitigation grading**	**Overall risk level**
Banks	34	6	211	High	158	High
Accountancy service providers	14	9	120	High	90	High
Legal service providers	17	7	112	High	84	High
Money service businesses	18	7	119	High	71	Medium
Trust or company service providers	11	6	64	Medium	64	Medium
Estate agents	11	7	77	Medium	58	Medium
High value dealers	10	6	56	Low	42	Low
Retail betting (unregulated gambling)	10	5	48	Low	36	Low
Casinos (regulated gambling)	10	3	32	Low	24	Low
Cash	21	7	147	High	88	High
New payment methods (e-money)	10	6	60	Medium	45	Medium
Digital currencies	5	3	15	Low	11	Low

2 Legal and regulatory framework

2.1 This section outlines the legal and regulatory framework governing the AML/CFT regime in the UK. Further detail on the legal framework relating to terrorist financing can found in chapter 11.

The Financial Action Task Force (FATF)

2.2 The Financial Action Task Force (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 of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is therefore a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

2.3 The UK was a founding member of the FATF and continues to play a leading role in the development of global standards; the identification of new risks and typologies; the production of guidance and best practice, incorporating a risk-based approach; and the assessment of countries compliance with those standards. In addition, the UK is a Cooperating and Supporting Nation to Caribbean FATF (CFATF) and 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 FATF and represents the UK at the FSRBs, working in collaboration with a number of different government departments, agencies and regulatory bodies, such as the Home Office, Department for International Development (DfID), the National Crime Agency (NCA) and the Financial Conduct Authority, and with technical assistance provided by the Metropolitan Police, Crown Prosecution Service (CPS) and the Charity Commission among others.

2.4 The FATF has 2 important functions: setting the FATF recommendations and monitoring their implementation among members. The UK plays a key role in maintaining suitable pressure on FATF and FSRB members to ensure their compliance with the recommendations and ensure they take appropriate action to rectify their deficiencies. In this role, the UK, in cooperation with FATF and FSRB members, reviews money laundering and terrorist financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures globally.

The European Union

2.5 The EU takes particular account of the FATF recommendations through EU directives that member states transpose into national law. The First Money Laundering Directive was adopted by the European Parliament and Council in June 1991. It applied the FATF recommendations to financial institutions and requirement the criminalisation of money laundering. This directive was transposed into UK law through the Criminal Justice Act 1991, the Drug Trafficking Act 1994 and the Money Laundering Regulations 1993.

2.6 The Second Money Laundering Directive was adopted in December 2001. It extended the anti-money laundering obligations to a defined set of activities provided by a number of non-financial services. Those services included independent legal professionals, accountants, real

estate agents and tax advisors. This directive was transposed into UK law through the Proceeds of Crime Act 2002 and the Money Laundering Regulations 2003.

2.7 After the FATF updated its recommendations in 2003, incorporating nine special recommendations on terrorist financing, the Third Money Laundering Directive was adopted in October 2005. The UK transposed this directive through the Proceeds of Crime Act 2002, the Terrorism Act 2000 and the Money Laundering Regulations 2007.

2.8 The EU Funds Transfers Regulation[1] was adopted in November 2006, transposing the FATF recommendation on ensuring traceability of payment to prevent the financing of terrorism (FATF special recommendation VII).[2] The regulation imposes identification and verification requirements on payers and by payment service providers. For money transfers within the EU, and in line with building and ensuring a single market, Article 6 of the regulation provides what is in effect a simplified due diligence approach. Article 17 provides an authorisation process to treat transfers to or from some non EU countries and territories as though they were transfers within the EU. The regulation took direct effect in January 2007.

2.9 The Fourth Money Laundering Directive and the accompanying Wire Transfer Regulations, 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 European Union on 5 June 2015. This directive will be transposed into UK law within 2 years of the date of publication.

The Money Laundering Regulations 2007 ('the regulations')

2.10 The regulations place requirements on relevant persons for the purpose of preventing and detecting money laundering and terrorist financing. Relevant persons subject to the regulations 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.

2.11 The regulations include (but are not limited to) the requirement relevant persons to:

- conduct customer due diligence (CDD) and identify categories of higher risk customer including Politically Exposed Persons (PEPs)
- appoint a nominated officer to whom knowledge or suspicion of money laundering or terrorist financing must be reported
- have policies and procedures, including for risk assessment and management
- monitor and manage compliance with those policies and procedures
- ensure awareness and training of staff

2.12 Regulation 20 (1) states a relevant person "must establish and maintain appropriate and risk-sensitive policies and procedures" relating to the requirements in the regulations which includes "risk assessment and management". In order to establish a level of risk a relevant person must consider if there are money laundering and/or terrorist financing risks. That will inform what level of customer due diligence (CDD) is required as per regulation 7 (3).

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

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

2.13 All relevant persons subject to the regulations must be effectively monitored for compliance (Regulation 24). The regulations permit supervisory authorities that include professional bodies where possible, as provided for by the EU directive. There are currently 27 supervisors.[3]

Proceeds of Crime Act 2002

2.14 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. It provides the framework for asset recovery in the UK, as well as a number of investigative powers to enable law enforcement agencies to investigate money laundering and develop cases to recover the proceeds of crime.

Money laundering offences

2.15 The money laundering offences in POCA go further than the minimum standards agreed by the FATF. POCA covers all crimes and there is no *de minimis* limit for reporting money laundering. The principal money laundering offences are designed to cover all elements of money laundering and include:

- s 327: An offence is committed if a person conceals, disguises, converts, transfers or removes from the jurisdiction property which is, or represents, the benefit of criminal conduct (i.e. the proceeds of crime) and the person knows or suspects represents such a benefit
- s 328: An offence is committed when a person enters into or becomes concerned in an arrangement which he knows or suspects will facilitate another person to acquire, retain, use or control benefit from criminal conduct and the person knows or suspects that the property is benefit from criminal conduct
- s 329: An offence is committed when a person acquires, uses or has possession of property which he knows or suspects represents benefit from criminal conduct

Suspicious activity reports (SARs)

2.16 POCA requires financial institutions and businesses in the regulated sector to report to the NCA suspicions about money laundering. SARs reporters gain a statutory defence from the money laundering offences if they submit a SAR and receive consent from the NCA to undertake an activity which would otherwise constitute money laundering.

2.17 There are separate offences of failing to disclose money laundering, and include:

- s 330: An offence is committed by those working in the regulated sector if they do not submit a STR to a nominated officer or a SAR to the NCA if they know or suspect, or have reasonable grounds to know or suspect, that another person is engaged in money laundering; and the information came to them in the course of their business in the regulated sector
- s 331: An offence is committed by 'nominated officers' in the regulated sector if they do not submit a SAR if they know or suspect, or have reasonable grounds to know or suspect, that another person is engaged in money laundering; and the information came to them in the course of their role as nominated officer

[3] A full list of supervisors can be found in Annex A.

2.18 In addition under s.332 an offence is committed by other nominated officers if they do not submit a SAR to the NCA when they know certain information and they suspect that another person is engaged in money laundering and the information came to them in consequence of a protected or authorised disclosure.

2.19 POCA gives reporters a defence when undertaking an activity which the reporter believes may constitute one of the three money laundering offences (sections 327-329) if they have appropriate consent. This is achieved by submitting a suspicious activity report (SAR) to the NCA. The reporter runs the risk of committing a money laundering offence if they proceed before having appropriate consent.[4]

2.20 It is also a criminal offence for individuals within the regulated sector to 'tip off' a person that a SAR has been submitted. There were over 354,000 SARs submitted in 2013/14, the vast majority of which came from the financial sector.

Financial investigation powers

2.21 POCA provides financial investigatory powers to the police, officers of HM Revenue & Customs, NCA and non-warranted accredited financial investigators (AFIs) (for example those working at Trading Standards and Royal Mail) who have been trained and accredited by the Proceeds of Crime Centre (POCC) housed in the NCA.

2.22 These powers allow those bodies to investigate and develop cases to recover the proceeds of crime. There are in excess of 3000 trained financial investigators (including AFIs, constables and officers of HMRC) and they have played an integral role in the recovery of assets since POCA came into force in 2003.

Asset recovery

2.23 POCA also sets out the legislative framework for the recovery of criminal assets. There are four routes for recovery of assets:

- criminal confiscation (post-conviction)
- civil recovery (a form of non-conviction confiscation)
- cash seizure and forfeiture
- taxation

Criminal confiscation

2.24 Confiscation proceedings seek to recover the financial benefit that an individual has gained as a result of their offending. It is the most commonly used asset recovery mechanism. Confiscation orders are available following a criminal conviction. The court identifies the value of the benefit in monetary terms that the defendant received, and orders him to pay an equivalent sum, or less if a lower sum is available. If the defendant fails to pay the sum, enforcement action can ensue and the offender can be imprisoned. Confiscation proceedings can be instigated either by the prosecution or by the court and the standard of proof in these proceedings is on the balance of probabilities.

2.25 The confiscation provisions of POCA apply only to offences committed on or after 24 March 2003. The courts initially determine whether or not the defendant has a 'criminal lifestyle'

[4] For more information please see Home Office Circular on Consent (029/2008).

as defined in POCA – this is if a defendant has been convicted of a specified offence in schedule 2 or in the proceedings in which they have been convicted, they were convicted of three or more other offences, each of the additional offences constituting conduct from which he has benefited or they have a certain history and number of convictions. The defendant only has a criminal lifestyle under the latter 2 methods if he obtained relevant benefit of £5,000. If the defendant has a criminal lifestyle, the courts apply certain assumptions about their wealth as being the proceeds of crime and therefore liable to be calculated as benefit from criminality. Lifestyle offences include drug trafficking, money laundering, people trafficking, arms trafficking, counterfeiting and blackmail. If a defendant does not have a 'criminal lifestyle' then a confiscation order is calculated as the benefit derived from the offences of which they were convicted (this is known as 'particular criminal conduct').

2.26 POCA also provides for the making of a restraint order, the effect of which is to restrain a person from dealing with the assets so as to prevent them from being dissipated in advance of a confiscation order being made. A restraint order can be applied for as soon as a criminal investigation has commenced. The Serious Crime Act 2015 has reduced the test for restraint to one of "reasonable grounds to suspect". This is in line with the test for effecting an arrest of a person under the Police and Criminal Evidence Act 1984, and should make it easier to secure restraint orders at the early stages of an investigation. The Serious Crime Act 2015 also amended POCA to strengthen significantly the default prison sentences for those who refuse to pay their confiscation order

Civil recovery

2.27 Civil recovery is the process of recovering the proceeds of unlawful conduct without the need for a conviction, through proceedings in the High Court proved to a civil standard. If a criminal prosecution is not feasible, civil recovery may present an opportunity to deprive criminals of property obtained through unlawful conduct, for example in cases where the criminality took place overseas and cannot be prosecuted in UK courts or where someone has died. It is important to note that civil recovery proceedings are taken in respect of the property itself rather than (as in confiscation) the person responsible for the unlawful conduct. Enforcement authorities do not have to prove that the unlawful conduct was of a particular type or types but they do have to link the asset to the unlawful conduct for it to be recoverable.

Cash seizure and forfeiture

2.28 The cash seizure provisions in POCA allow authorised persons to seize cash[5] suspected of being the recoverable property of unlawful conduct, or intended for use in by any person in unlawful conduct. Cash forfeiture powers are founded on the same conditions: namely that there are reasonable grounds to suspect the cash is either recoverable property[6] or was intended for use by any person in unlawful conduct.

2.29 Cash forfeiture proceedings are civil rather than criminal in nature before the Magistrates' Court, are taken against the cash and not a person, and the standard of proof in these cases is on the balance of probabilities. Specific unlawful conduct does not need to be proved; it is enough to show that the cash is probably related to one of a number of kinds of activity, any one of which would have been unlawful.

[5] Cash is defined in POCA 'as notes and coins in any currency, postal orders, cheques of any kind including travellers' cheques, bankers' drafts, bearer bonds and bearer shares and any other monetary instrument as specified by the Home Secretary.'
[6] As defined in POCA

Taxation

2.30 POCA enables the NCA to adopt the direct taxation functions of HM Revenue and Customs where there is a reasonable grounds to suspect that an individual has received taxable income, gains or profits upon which no tax has been paid as the result of their own or another person's criminal conduct. The income, gain or profit in respect of which the NCA adopts taxation powers may be suspected to be wholly or partly, directly or indirectly as a result of criminal conduct. As a result tax assessments raised by the NCA may cover an individual's untaxed receipts from both legitimate and criminal sources. POCA provides that the NCA does not have to identify the source of the funds that are the subject the tax assessment.

Industry guidance

2.31 In addition to the regulations, the Treasury approves AML/CFT guidance written by and for industry sectors. Treasury approved guidance exists for most supervised sectors and provides detailed assistance to firms on the practical application of legal and regulatory requirements to their business or sector.

2.32 Before being approved by HM Treasury, industry guidance is 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/CFT regime in the UK;. HM Treasury and the Home Office chair meetings of this group 3 times a year. The Treasury only approves guidance that is proportionate and risk-based, and this is therefore an essential part of the UK's risk-based approach.

2.33 The regulations and guidance, when taken together, are a framework for relevant persons and the regulated sector to avoid committing an offence under the Proceeds of Crime Act 2002 (POCA) or the Terrorism Act 2000 (TACT) or the Money Launder Regulations 2007. POCA and TACT require that the Court must consider whether a person followed the guidance, at the relevant time, that has been approved by HM Treasury and issued in an appropriate manner.

3 Predicate offences

3.1 This section describes the nature and scale of offending in the UK which generates criminal proceeds.

3.2 Crime levels in the UK have been on a downward trend for nearly 20 years. Many of the highest volume crimes, such as offences of violence or criminal damage, generate no proceeds.

3.3 The laundering of the proceeds of the larger scale criminal activity of organised crime groups (OCGs) is particularly significant because it relates to high-harm offending, funds further criminal activity, and funds the lifestyles that make organised crime attractive to vulnerable people at risk of getting drawn in to crime. As of 31 December 2014, there were around 5,800 organised crime groups (comprising approximately 40,600 individuals) operating in the UK.[1] The social and economic costs of serious and organised crime are estimated to be £24 billion per year, mostly as a result of drug supply (with a cost of £10.7 of billion) and fraud (with a cost of £8.9 billion).[2] Less is known about cyber and 'hidden' crimes such as Modern Slavery.

3.4 There are intelligence gaps on the size and nature of criminal markets in the UK, but we know from confiscation order data that the offences in the UK that generate the largest scale of proceeds are fraud and drugs supply offences.

Fraud and tax offences

3.5 Fraud and tax offences are the largest known source of criminal proceeds from offending in the UK and involve a wide variety of crime types, victims, and perpetrators. Fraud conducted by organised crime groups is thought to cost the UK £8.9 billion per year.

3.6 Fraud is increasingly conducted online. Non- and under-reporting by individuals and some business sectors makes the true scale difficult to estimate. The number of reported frauds is rising, although this may be a consequence of improved reporting through Action Fraud rather than an actual increase in crime.[3]

3.7 HMRC estimate that £5.4 billion was lost to criminal attacks against the tax system in 2012/13, with a further £4.1 billion lost to tax evasion.[4] Excise duty fraud (particularly targeting tobacco, alcohol and fuel) and VAT fraud are the principal threats.

3.8 The Department for Work and Pensions estimates the total value of fraud against the benefit system to be £1.2 billion (0.7% of total benefit expenditure) in 2013/14.[5]

3.9 The NCA estimates that individuals, the private sector and the charity sector lose billions of pounds each year to fraud, and assesses that cyber-enabled banking and card fraud are widespread. Reported losses to card fraud increased from 2013 to 2014 (up from £216 million in the first 6 months of 2013 to £248 million in the first six months of 2014, an increase of

[1] 'The Serious and Organised Crime Strategy: Annual Report for 2014', HM government, March 2015.

[2] 'Understanding Organised Crime: Estimating the Scale and the Social and Economic Costs', Home Office, 2013.

[3] Action Fraud is the UK's national fraud and internet crime reporting centre. It provides an online reporting tool through which fraud and internet crime can be reported.

[4] 'Measuring Tax Gaps 2014 Edition', HM Revenue and Customs, October 2014

[5] 'Fraud and error in the benefit system: financial year 2013/14 estimates', Department for Work and Pensions, November 2014

15%).[6] The NCA also estimates that insider dealing and market abuse may cost hundreds of millions of pounds per year, although the true scale of the threat is an intelligence gap.[7]

3.10 In the period 2010-2014, approximately 20% of the confiscation orders made related to fraud offences, but they accounted for approximately 45% of the value, indicating that fraud offenders typically generate larger amounts of realisable criminal assets compared to other offenders. Many of the largest confiscation orders made by the UK courts relate to VAT fraud, the proceeds of which are typically laundered out of the UK using complex company structures.

Drugs offences

3.11 Drug use amongst the UK population has fallen in recent years, as has drug use amongst problem drug users (those who abuse opiates and crack cocaine) who commit a disproportionately high number of crimes.[8]

3.12 The UK drugs market remains significant, and is estimated to be worth nearly £4 billion per annum.[9] The number of UK cannabis farms and new psychoactive substances (NPS) detected in the UK has grown, whilst cocaine use remains prevalent and the heroin market remains stable. The source countries and supply routes for cocaine and heroin are well understood, and disruptions of OCGs are regularly achieved.[10]

3.13 In the period 2010 – 14, drugs supply offences accounted for approximately half of the confiscation orders made in the UK and for approximately one quarter of the value of orders made (second only to fraud offences).[11]

Modern slavery

3.14 Modern slavery includes labour and sexual exploitation, domestic servitude and human trafficking and is a largely hidden crime that is difficult to identify.

3.15 The Home Office estimates that there were 10,000 – 13,000 potential victims in the UK in 2013. The National Crime Agency estimates that one third of victims are from UK.[12] The number of referrals of potential victims of trafficking has grown year-on-year for the past 3 years, and the NCA assesses that this trend is likely to continue.[13] There is an intelligence gap on the scale of proceeds of this crime in the UK, but the International Labour Organisation estimates that profits from forced labour worldwide come to US $150 billion per year.[14]

3.16 The fact that this is an underreported crime, in which it is difficult to identify victims and perpetrators – and that victims sometimes do not consider themselves victims – has led to low numbers of prosecutions and asset recovery actions against modern slavery perpetrators historically, both in the UK and across the EU. There has been a sustained increase in detection of modern slavery in recent years, but this may be a result of improved reporting mechanisms and increased priority attached to this crime by law enforcement agencies and others.

---

[6] Financial Fraud Action UK.

[7] 'National Strategic Assessment of Serious and Organised Crime', National Crime Agency (NCA), June 2015

[8] 'Drug Misuse: Findings from the 2013/14 Crime Survey for England and Wales', Home Office, August 2014

[9] 'Understanding Organised Crime: Estimating the scale and understanding the social and economic costs', Home Office, 2013

[10] 'National Strategic Assessment of Serious and Organised Crime', NCA, June 2015

[11] Unpublished Home Office data.

[12] 'Modern Slavery Strategy', HM government, November 2014

[13] 'National Strategic Assessment of Serious and Organised Crime', National Crime Agency, June 2015

[14] 'Modern Slavery Strategy', HM government, November 2014

Acquisitive crime

3.17 Acquisitive crime (covering theft, robbery and burglary) has been on a downward trend in the UK since the mid-1990s. The 2013/14 Crime Survey of England and Wales showed approximately 4.56 million acquisitive crime offences (down from 11.9 million in 1995).[15] The total value of stolen goods in 2013/14, as estimated by the victims, was £1.6 billion, a 75% drop since the estimated £6.9 billion in 1995.[16]

3.18 Recent Home Office research has shown that the decline in the number of heroin and crack-cocaine users from the late 1990s onwards may have been an important factor in the fall in acquisitive crime, accounting for between a third and a half of the fall in thefts.[17] Other factors, such as improvements to the security of vehicles and property, and better policing techniques, have probably also played an important role.

3.19 Most acquisitive crime is carried out by individuals, but organised crime groups are also involved. Whilst the number of armed robberies at banks and buildings societies has declined in the last decade, OCGs target the movement and housing of cash, automated teller machines (ATMs) and jewellery retailers, with high value watches and Asian gold the most sought after products. OCGs are also involved in organised vehicle crime, commodity-based crime (particularly smart phones) and metal theft.[18] The NCA has found that many OCGs involved in organised acquisitive crime operate across a variety of crime types, being involved in drugs supply and economic crime, as well as multiple types of acquisitive crime.[19]

3.20 Most detected acquisitive crime offences generate relatively low value proceeds. In the period 2012 to 2014 over 90% of acquisitive crime resulted in criminal proceeds of under £1,000. In the period 2010–14, burglary and theft offences accounted for between 7 – 10% of all confiscation orders granted but only 1 – 2% of orders by value.

[15] 'Crime Statistics: Focus on Property Crime, 2013/14', Office for National Statistics, November 2014

[16] 'Crime and the Value of Stolen Goods', Home Office, 2015

[17] 'Research Report 79: The heroin epidemic of the 1980s and 1990s and its effect on crime trends – then and now', Home Office, July 2014.

[18] 'National Strategic Assessment of Serious and Organised Crime', NCA, May 2014

[19] 'National Strategic Assessment of Serious and Organised Crime', NCA, June 2015

4 UK law enforcement

4.1 This section outlines the current UK law enforcement landscape, and our law enforcement and prosecution agencies' response to money laundering.

4.2 The UK's law enforcement and prosecution agencies operate at the national, regional and local levels (see table 4.A). All of the law enforcement agencies described below have powers to investigate money laundering (as provided in section 7 of the Proceeds of Crime Act 2002).[1] The National Control Strategy prioritises the threats of serious and organised crime and cross-cutting issues, providing a framework that informs the response across law enforcement. Decisions on what cases to investigate, and what priority to give to particular types of crime (such as money laundering), rest with the law enforcement agencies themselves.

Table 4.A: UK law enforcement and prosecution agencies at local, regional and national level

Local	43 police forces in England and Wales (local policing in Northern Ireland and Scotland is the responsibility of the Police Service of Northern Ireland and Police Scotland).			
Regional	9 Regional Organised Crime Units (ROCUs) in England and Wales, which include Regional Assets Recovery Teams (RARTs) and Asset Confiscation Enforcement (ACE) teams.		Regional Crown Prosecution Service offices (including dedicated asset recovery resources co-located with ROCUs).	
National	HM Revenue & Customs	National Crime Agency	Serious Fraud Office	National Crown Prosecution Service Functions

Local policing

4.3 There are 43 local forces in England and Wales, with Police Scotland and the Police Service of Northern Ireland providing local policing in Scotland and Northern Ireland. There are also a number of non-territorial police forces, such as the British Transport Police.

4.4 There are approximately 128,000 police officers in the UK, supported by a further 13,000 Police Community Support Officers (PCSOs) and 64,000 civilian staff in the 43 forces in England and Wales[2]. The size of forces varies widely, reflecting the size of the force area and its population. The largest force, the Metropolitan Police Service, is 39 times the size of the smallest force, the City of London Police.[3]

4.5 The police have a broad responsibility to prevent and detect crime of all types, from anti-social behaviour to child sexual exploitation and the most serious organised crime, including money laundering. Tackling money laundering is a part of the total police response to crime although it is not a priority for the majority of police forces. In 2013/14, the police, including the Regional Assets Recovery Teams (RARTs), were responsible for the majority of confiscation orders with 5227 orders issued with an approximate value of £125 million and £30 million cash forfeited.[4]

[1] Financial investigation powers have also been granted to a number of other agencies with investigative and enforcement functions, such as Trading Standards and the Environment Agency.

[2] Data as of 31 March 2014. 'Police Workforce, England and Wales', Home Office, July 2014

[3] 'Policing in Austerity: Meeting the Challenge', HMIC, July 2014. Data covers Full Time Equivalent staff "FTE" including police officers, civilian staff and PCSOs

[4] JARD (Joint Asset Recovery Database) data from 1 April 2013 to 31 March 2014.

Regional Organised Crime Units and Regional Asset Recovery Teams

4.6 Police forces in all nine policing regions in England and Wales have collaborated to form Regional Organised Crime Units (ROCUs). These units deliver specialist investigative and intelligence capabilities to all forces within a region, to help tackle serious and organised crime. ROCUs are the primary interface between the National Crime Agency (NCA) and forces and are accountable to their respective Police and Crime Commissioners.

4.7 They support the national coordination and tasking of the effort against serious and organised crime by providing capabilities for the police response to activity with regional impact. They also support local forces, providing specialist resources and tactical advice to support local operations to counter serious and organised crime.

4.8 Within each ROCU is a Regional Asset Recovery Team (RART). The RARTs develop financial intelligence in aid of investigation and disruption of subjects. They utilise financial investigation to conduct money laundering investigations, disrupt subjects and recover assets through POCA legislation. There are approximately 180 staff in the RARTs, all of whom are operational.

4.9 In 2013/14 the RARTs secured approximately £1 million in cash forfeitures and 261 confiscation orders with an equivalent value of approximately £22 million. The regional ACE teams, established in September 2014, recovered approximately £7 million of assets in the first 6 months of operations.

National Crime Agency

4.10 The National Crime Agency (NCA) is the lead agency for the response to serious and organised crime in the UK.

4.11 The NCA's strategic priorities are set by the Home Secretary. The first is to identify and disrupt serious and organised crime including by investigating and enabling the prosecution of those responsible.[5] Its principal functions are to reduce crime and to gather, analyse and disseminate criminal intelligence.[6]

4.12 Money laundering and criminal finance are important areas of work for the NCA. Money laundering, and bribery and corruption which is closely associated with it, have been identified as high priority threats in the NCA National Control Strategy, which prioritises the threats of serious and organised crime.

4.13 The NCA has an intelligence hub which is responsible for gathering, analysing and disseminating information and an Economic Crime Command which is responsible for leading, supporting and coordinating resources to counter economic crime across the UK – including law enforcement, regulatory bodies and the private sector. This includes law enforcement efforts on money laundering, bribery and corruption, asset recovery and asset denial. It also supports partners, for example in the SFO and FCA by providing the NCA's investigative capabilities to tackle high priority economic crime threats.

4.14 The NCA co-ordinates activity through the multi-agency Criminal Finances Threat Group, which has sub-groups on cash-based money laundering (led by HMRC); non-cash based money laundering (led by NCA); and professional enablers (led by SFO).

[5] 'NCA Annual Plan 2014/15', National Crime Agency (NCA), March 2014

[6] As set out in the Crime and Courts Act 2013

4.15 NCA is focussing on money laundering and international corruption to protect the UK as an international financial centre. It is proactively using financial investigation and other law enforcement techniques in intelligence and evidence-gathering to target money laundering, as well as asset recovery tools after the event. It has various tools available to it including:

- intelligence and evidence-gathering
- cash seizure and forfeiture
- restraint and confiscation
- civil recovery and taxation

4.16 On asset recovery the NCA's priority is denying criminals their assets by every lawful means it can, not just recovering them. The focus is on the disruptive value of taking assets away, not the size of the returns. However, in its first year, NCA led and coordinated operational activity that resulted in almost £126 million (£22 million domestically and £104 million internationally) being denied to criminals impacting on the UK. In regards to assets recovered, in its first year the NCA achieved returns of £22.5 million.

4.17 The NCA also works closely with its partners to assist their efforts against criminal finances, for example by working with UK police forces to identify and seize money derived from criminal activity. Since the NCA was established in 2013, its activity has led directly to operational partners seizing over £16 million in cash and making around 150 related arrests.

4.18 NCA has also set up a dedicated Asset Confiscation Enforcement (ACE) team to coordinate activity across the Agency and with its partners, including the police, HMRC, SFO and HM Courts and Tribunal Service. Between 2 December 2013 and 31 December 2014, £40 million was collected by partners on a total of 161 priority cases across law enforcement. Through the work of ACE teams across the UK, law enforcement is tackling unenforced confiscation orders and prioritising the orders of the most serious criminals.

UK Financial Intelligence Unit

4.19 The UK Financial Intelligence Unit (UKFIU) is part of the NCA Economic Crime Command, but is operationally independent of the NCA, meaning that it has the authority and capacity to act autonomously.

4.20 The UKFIU is a law enforcement FIU which receives, analyses and distributes financial intelligence gathered from suspicious activity reports (SARs). UKFIU analyses the SARs to extract strategic and tactical intelligence, and makes all SARs available to law enforcement agencies for investigation (with the exception of SARs in certain sensitive categories). UKFIU receives the largest number of SARs of any EU member state. In 2013/14 UKFIU received 354,000 SARs of which 14,155 were requests for consent. This is an increase of approximately 38,000 reports on the totals for 2012/13.[7]

4.21 The UKFIU works in close partnership with other key international organisations to fight money laundering and terrorist financing. The UKFIU is a fully active member of the Egmont Group (an international forum for FIUs, set up to improve cooperation in the fight against money laundering and the financing of terrorism). Membership allows the UKFIU to seek and receive financial intelligence from other members in order to support law enforcement

[7] 'Suspicious Activity Reports (SARs) Annual Report 2014', NCA, December 2014.

operations and projects. It also acts as the conduit to this resource for the wider UK law enforcement community.

Serious Fraud Office (SFO)

4.22 The 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 the responsibility rests with the Crown Office and Procurator Fiscal Service. Its expert forensic accountants and professional investigators and lawyers investigate and prosecute the most serious or complex instances of fraud and corruption.

4.23 The SFO's Proceeds of Crime Division deals with confiscation investigations, restraint proceedings, money laundering investigations and civil recovery work across the SFO's cases. The Division comprises a multi-disciplinary team of 37 lawyers and financial investigators who work closely with the criminal case teams to ensure that a financial investigation strategy is in place from the outset. The team also deals with incoming requests for mutual legal assistance involving asset freezing and the enforcement of overseas confiscation orders.

4.24 In the period 2014/15 the SFO secured 17 confiscation orders with an equivalent value of £22.7 million and one civil recovery order worth £520. They also recovered £13.8 million in net receipts.HM Revenue and Customs (HMRC)

4.25 HMRC is the UK's tax authority and was established by Act of Parliament in 2005 following the merger of the Inland Revenue and HM Customs & Excise. It is a non-ministerial department reporting to Parliament through its Treasury minister.

4.26 HMRC is responsible for investigating crime involving all of the tax and other regimes it deals with. It uses civil, as well as criminal, procedures as this allows for a greater volume of cases to be pursued, as well as increasing the revenues secured for the Exchequer. HMRC is also a supervisor for some businesses under the regulations.

4.27 Criminals, including organised criminals, seek to attack the UK's tax and duty systems to steal taxpayer's money. To counter this HMRC has similar criminal investigation powers to those that are available to other law enforcement agencies. In addition to the predicate offences, HMRC can also investigate money laundering offences using POCA investigative powers, recover criminal cash through summary proceedings and recover the proceeds of crime through working with the independent prosecutors.

4.28 In the period 2014/14, HMRC secured £1.7 million in cash forfeitures[8] and 171 confiscation orders with an equivalent value of £51.2 million. They also recovered £22.4 million in net receipts.[9]

Crown Prosecution Service (CPS)

4.29 The CPS is headed by the Director of Public Prosecutions (DPP), who is in turn superintended by the Attorney General (AG). It 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

[8] A total of 52 orders were made.

[9] JARD data for period 1 April 2013 and 31 March 2014

the charge in all but minor cases; prepares cases for court; and applies for restraint, receivership and confiscation orders in respect of CPS prosecutions.

4.30 The CPS also obtains restraint orders and enforces overseas confiscation orders on behalf of overseas jurisdictions pursuant to requests for Mutual Legal Assistance (MLA). Recently it has developed and implemented a comprehensive asset recovery strategy in partnership with relevant government departments and other law enforcement agencies. Central to the strategy is the identification and targeting of priority countries where UK efforts can have most impact, and the deployment of dedicated Asset Recovery Advisors (ARAs), funded by the Home Office, to Spain, UAE, and the European and Caribbean regions. These lawyers work with UK and international partners to increase enforcement of existing orders, assist ongoing operations and develop local capability to improve asset recovery and counter illicit finance.

5 Supervision

5.1 The Treasury is responsible for appointing anti-money laundering and counter financing of terrorism (AML/CFT) supervisors. The regulations set out the role of the supervisors[1] and gives them powers to effectively monitor their respective sectors.

5.2 There are currently 27 AML/CFT supervisors[2] in the UK, supervising a range of sectors including credit institutions, financial institutions, auditors, insolvency practitioners, external accountants and tax advisers, independent legal professionals, money service businesses, trust and company service providers, estate agents, high value dealers and casinos. The supervisors are a diverse group including large global professional bodies, smaller professional bodies, and a number of public sector organisations.

5.3 Supervisors are expected to apply a risk-based approach to their supervisory activities. A risk-based approach means considering the likelihood of unwanted outcomes when targeting resources and applying preventative measures, in order to focus efforts in a way that is effective and commensurate to the nature of risks.

5.4 Where permitted by the Third Money Laundering Directive (3MLD), the UK designates professional bodies as supervisors. This approach benefits from the professional bodies' knowledge of their sectors and the broader incentive their members have to meet high professional standards.

5.5 Most supervisors attend the AML/CFT Supervisors Forum which meets three times a year.[3] Supervisors also meet periodically in smaller affinity groups. There are three affinity groups; accountancy, legal, and the public sector group (made up of HMRC, Financial Conduct Authority (FCA), The Gambling Commission and the Insolvency Service).

Vulnerabilities

5.6 This assessment has identified the following vulnerabilities in the UK's supervisory regime.

5.7 Professional body supervisors tend to integrate their AML/CFT responsibilities into their overall supervisory approach; this has advantages in that the supervisors can capitalise on specialist knowledge, information and resource, and can look at wider risks which may also be indicators for AML, such as bribery and corruption. There is no reason why an integrated model should not be able to support a legitimate risk-based approach. However there is a risk that the priority attached to AML/CFT may vary over time as it is prioritised against assessments of compliance in other areas.

5.8 There is a risk that professional body supervision is compromised by conflicts of interests as these bodies represent and are funded by the firms they supervise. However, the evidence gathered through the consultation undertaken as part of this assessment, and through the annual reporting process, does not indicate that this potential conflict of interest is undermining the

[1] The duties of the supervisors are set out in Regulation 24 of the Money Laundering Regulations 2007 http://www.legislation.gov.uk/uksi/2007/2157/contents/made

[2] Full list of supervisors can be found in Annex A.

[3] The AML/CFT Supervisors Forum was set up to encourage the sharing of information and best practice between supervisors. It is also attended by HM Treasury, the Home Office and the National Crime Agency.

effectiveness of supervision. For the legal sector in particular this risk is partially mitigated by the Law Society delegating part of its supervisory responsibility to the Solicitors Regulation Authority.

5.9 Whilst supervisors demonstrate a high level of awareness of the requirement to, and importance of, taking a risk-based approach to their AML/CFT supervision, implementation of the risk-based approach varies, and the level of sophistication of the risk-based models adopted by supervisors vary significantly. Indeed whilst some supervisors devote significant time and resource to designing and implementing the approach, some supervisors have not yet implemented a risk-based approach to supervision. The majority of supervisors also have difficulty in explaining how their assessment of risk translates into the specific monitoring actions they undertake. This could lead to vulnerabilities in the sectors, as supervision may not be sufficiently focussed on those firms presenting the greatest risks

5.10 Supervisors use a range of sources to inform their understanding of risk. The range of sectors and high number of supervisors creates challenges for law enforcement agencies in providing bespoke information. This may contribute to the supervisors' view that information provided to them by law enforcement agencies focuses on banking, and that more information on sector-specific risks in the other regulated sectors would assist their identification and assessment of risk. Cooperation and outreach between law enforcement agencies and the supervisors generally is improving, with more needed. A recent example is the joint work between the Home Office, NCA, Law Society and Solicitors Regulation Authority to raise awareness of the threats firms face.

5.11 Supervisors such as HMRC and the FCA have statutory fit and proper tests for certain sections of their supervisory population. Firms and individuals that are supervised by a professional body are subject to a test as part of the professional standards required to become a member of the body. Further work is required to testify to the adequacy of those tests.

5.12 In the accountancy, High Value Dealer (HVD) and estate agency sectors, supervisors are concerned about the potential number of firms that are not supervised as they may be unaware of the requirement to register with a supervisor, or they may be seeking to avoid supervision.

5.13 Following a review of the regulations, in 2012 the Treasury amended the regulations to provide a legal gateway for supervisors to share information between themselves for the purpose of their AML/CFT responsibilities. This enables supervisors to inform each other of firms or individuals they have struck off or have particular concerns about, in order to help prevent regulatory arbitrage and non-compliant firms from evading proper controls. Supervisors recognise they collectively need to share more information with each other in order to properly mitigate the risks.

6 Regulated sectors

6.1 This chapter sets out the government's understanding of the money laundering and terrorist financing risks present in the regulated sectors. There are many similarities between money laundering and terrorist financing in the way that criminals and terrorists store and move funds, however, the motives for generating funds differ. The terrorist financing threats to the UK are set out in detail in chapter 11, however, many of the vulnerabilities set out below leave the regulated sector equally open to abuse by criminals wishing to launder money and by those wishing to finance terrorism.

6.2 The table below sets out this assessment's conclusions on the risk of money laundering within the regulated sectors. A range of factors were considered when in this assessment, including the nature of services offered by a sector; the compliance within that sector; and law enforcement agencies' existing knowledge of money laundering through the sector (where a lower level of knowledge represents a vulnerability and so a higher level of risk). For the 'overall risk level' the degree to which law enforcement agencies and supervisors have the capacity and capability to mitigate the risk within a sector was also considered.

Table 6.A: Money laundering risk rating (a summary of the methodology used to produce this rating can be found in chapter 1)

Thematic area	Total vulnerabilities score	Total likelihood score	Structural risk	Structural risk level	Risk with mitigation grading	Overall risk level
Banks	34	6	211	High	158	High
Accountancy service providers	14	9	120	High	90	High
Legal service providers	17	7	112	High	84	High
Money service businesses	18	7	119	High	71	Medium
Trust or company service providers	11	6	64	Medium	64	Medium
Estate agents	11	7	77	Medium	58	Medium
High value dealers	10	6	56	Low	42	Low
Retail betting (unregulated gambling)	10	5	48	Low	36	Low
Casinos (regulated gambling)	10	3	32	Low	24	Low

Banking

6.3 London is an international financial hub. It is home to over 250 foreign banks (more than New York, Paris or Frankfurt), and represents the largest centre for cross-border bank lending.[1] As a result of its size and complexity, the UK banking sector is more exposed to criminality than banking sectors in many other countries. The National Crime Agency (NCA) estimates that many hundreds of billions of pounds of international criminal money is almost certainly laundered through UK banks and their subsidiaries each year.[2]

6.4 The variety of ways that criminals may acquire, move, disguise, dispose of or otherwise launder the proceeds of crime makes a full understanding of the threat and vulnerabilities challenging. As well as traditional banking services, banks also provide other services such as trust and company formation, insurance and currency exchange.

6.5 Banks in the UK are subject to the Money Laundering Regulations 2007 ('the regulations'), Terrorism Act 2000 (TACT) and the Proceeds Of Crime Act 2002 (POCA). Banks are dual regulated by the Financial Conduct Authority (FCA) for conduct of business, including financial crime and the Prudential Regulation Authority (PRA) for prudential requirements, such as capital and liquidity. UK authorised banks are also prudentially regulated by the Prudential Regulation Authority (PRA), a subsidiary of the Bank of England. The FCA regulates hundreds of banks incorporated or operating through a branch in the UK for compliance with the regulations.

6.6 The Financial Action Task Force (FATF) identifies three key methods by which criminals and terrorist financiers move money for the purpose of disguising its origins and integrating it into the formal economy. These include the use of the financial system; the physical movement of money (e.g. through the use of cash couriers); and the physical movement of goods through the trade system. All of these methods directly and indirectly involve the banking system.

Threats and vulnerabilities

6.7 There are significant intelligence gaps in relation to the role of banks in 'high-end' money laundering. This type of laundering is particularly relevant to major frauds and serious corruption, where the proceeds are often held in bank accounts, real estate or other investments, rather than cash, and are moved through the banking sector as part of the laundering process. The threat in this sector is judged to be significant, around 60% of current money laundering cases being investigated by HMRC have funds initially moved through banks, compared with around 11% through MSBs. The UK's law enforcement agencies are still establishing the strength of understanding needed in this area.

6.8 The main threats and vulnerabilities in the banking sector are:

- criminals using the banking sector to move and store the proceeds of crime
- proceeds of corruption being moved through the banking sector
- systemic failings in banks AML/CFT control frameworks, as identified by the FCA, mean products and services without adequate controls can facilitate money laundering and terrorist financing

[1] 'Key facts about the UK as an international financial centre', CityUK, June 2014

[2] 'National Strategic Assessment of Serious and Organised Crime', NCA, June 2014

6.9 The vulnerabilities set out here leave the sector open to abuse both by criminals wishing to launder money, and those wishing to finance terrorism.

Retail banking (including business retail banking)

6.10 A current account can be used to place and transfer funds. It can often be accessed easily and remotely, and funds transferred quickly. This can enable criminality and therefore leave a bank vulnerable to being used as a conduit for the proceeds of crime, or as a conduit for terrorist financing. An example of this activity is the use of money mules.[3] A money mule can be complicit, negligent and/or unwittingly become involved in illegal activity. The cumulative nature of money mule activity means that significant sums can be laundered.

6.11 Investigations by law enforcement agencies found criminals using a service offered by UK retail banks, known as 'Bank Quick Drop' to launder the proceeds of crime. This service offers businesses, mainly cash intensive, the facility to "drop off" cash either at the bank directly, or at a third party facility where the money is counted and then transferred to the bank to be deposited. Investigations show complicit MSBs, HVDs and criminal gangs have utilised this system, particularly through the use of counting facilities, to launder the proceeds of crime. The amount laundered in two of the cases accounted for £250 million. In these cases, the criminal cash was accounted for by the MSB, which intentionally gave the false impression that it had come from legitimate sources. This service, without a robust AML/CFT control framework in place, can leave the banks vulnerable to money laundering.

6.12 Retail banks in the UK can accept thousands of new customers every month. This can make it challenging for banks to apply adequate risk sensitive controls. Ensuring all customers are subject to proportionate and adequate controls on a risk sensitive basis is especially difficult for banks, particularly in terms of ongoing monitoring of account activity and business activity. Cash intensive businesses, which due to the nature of their business have a high cash turnover, can in particular present challenges for banks monitoring systems; this can leave the bank vulnerable to money laundering and terrorist financing.

Wholesale, corporate and investment banking

Correspondent banking

6.13 Correspondent banking is an integral part of the international flow of capital and trade. Due to a number of factors such as speed, volume of transactions, accuracy and efficiency, correspondent banking leaves a bank vulnerable to money laundering. The HM Treasury approved Joint Money Laundering Steering Group (JMLSG) guidance for the financial sector sets out that, as the correspondent often has no direct relationship with the underlying parties to a transaction and so has limited information regarding the identity of the underlying party or the nature or purpose of the underlying transactions, firms undertaking such business should apply enhanced customer due diligence measures to their respondents on a risk-sensitive basis.

6.14 In 2011 the FSA conducted a thematic review which included reviewing correspondent banking systems and controls.[4] They found there was a wide variance in standards with some banks carrying out good quality AML/CFT work, while others, particularly among the smaller banks, carried out either inadequate due diligence or none at all on their correspondent banking relationships.

[3] Money mules are individuals recruited by criminals to receive the proceeds of crime into their bank account.

[4] 'Banks' management of high money-laundering risk situations', FSA, June 2011

6.15 Transaction monitoring was recognised as challenging for banks, however during the course of the review, the FSA found instances where banks did not take adequate steps to verify the explanations given for erratic or unusual transactions by respondents. While finding some examples of good practice, the FSA found many banks were leaving themselves vulnerable to financial crimes including money laundering by not having adequate control frameworks in place to identify and assess such activity. In a follow up report in 2014,[5] the FCA found the quality of enhanced due diligence and risk assessments on respondent banks (where it was required) were generally poor.

Trade finance

6.16 The FATF have identified trade finance as a method criminals and terrorist financiers use to move the proceeds of crime. Trade finance often involves complex transactions with multiple participants; many of the processes cannot be automated and it is resource intensive. Banks cannot see the complete transaction; they only view a single segment of the transaction. Operational structures in banks can compound the issue; there are many participants in the bank involved in the transaction. It is important they are joined up in discussions to ensure the bank is identifying and assessing their risks during and after the transaction.

6.17 For banks there are multiple vulnerability points during the transaction – the account opening stage; monitoring activity and obtaining viable information to inform the risk assessment. Further vulnerabilities identified by banks themselves are:

- Links between businesses engaged in this activity and solicitors (registration)
- Links between businesses engaged in this activity and introducers (giving access to the regulated sector)
- Company Formation Agents and perceived lack of information held at Companies House

6.18 The FCA conducted a thematic review in 2013 on banks' systems and controls in relation to trade finance.[6] The report found that while firms had good systems and controls in relation to sanctions checks (but poor for dual use goods), systems and controls to counter money laundering risk were generally weak. The FCA found inconsistent approaches towards risk assessments; most banks' policies did not deal with trade based money laundering risk and as a consequence some banks failed to implement adequate controls to identify suspicious transactions.

6.19 This work, alongside that by law enforcement agencies on MSBs, has brought trade based money laundering to the forefront of UK banks' risk agenda.

Private and wealth management

6.20 Unlike retail banking, private and wealth management is based on the principle of face to face contact and engagement with the customer. It offers complex services and products and has an embedded culture of confidentiality. All of this can attract high risk customers. The banking sector cite tax evasion and capital flight arising from political corruption as two areas where they can be particularly vulnerable to client risk. The threat to the UK from offshore tax evasion is a sizeable one; with greater global scrutiny over the operations of all banks in the global market given the use of their accounts facilities by some for money laundering linked to

[5] 'How small banks manage money laundering and sanctions risk: Update', FCA, November 2014

[6] 'Banks' control of financial crime risks in trade finance', FCA, July 2013

tax evasion, the need for improved awareness is clear across the whole private and wealth management market.

6.21 In a 2014 FCA thematic review, it was found that UK based private banks were generally operating to a higher standard than others in the sample of firms visited.[7] However issues remain around client risk assessment and enhanced due diligence. For example obtaining and understanding a client's source of wealth and source of funds, and ensuring relevant adverse information is taken into consideration when assessing risk and making judgements to ensure the institution is not being used to launder the proceeds of crime.

Supervision

6.22 The FCA has published 2 reports in 2013 and 2014 about its anti-money laundering activities. Both of these publications have highlighted that it continues to see systematic failings in banks' AML/CFT framework.[8]

6.23 The FCA also said in those reports that the following areas were the most common issues identified through its supervisory work:

- inadequate governance structures and oversight of AML/CFT
- inadequate risk assessment processes
- inadequate or poorly calibrated IT systems
- poor management of alerts from sanctions screening and transaction monitoring
- poor identification of source of wealth and source of funds
- inadequate risk management of foreign PEPs
- inadequate due diligence on correspondent banks
- questionable judgements leading to some firms accepting higher levels of money laundering risk

6.24 A risk assessment is the foundation of a proportionate, risk-based AML/CFT framework from which a banks operational environment, policies and procedures, must emanate. Banks must identify and assess their money laundering risks. Knowing what threats they are exposed to, risks they face and where the vulnerabilities are enables a bank to direct its resource accordingly. An inadequate risk assessment will result in poor delivery of key areas such as identification and assessment of risk posed by the customer and by the business.

6.25 Usually there are two types of risk assessment: client and enterprise wide. Banks believe more work is required on understanding and developing AML/CFT risk assessments, both at client and enterprise wide level.

6.26 This is substantiated by findings from thematic supervisory work by the FCA, where the FCA found the quality of banks' client risk assessments to be weak. Many of the banks found with weak risk assessments, both client and enterprise wide, were also found to have little to no understanding of the vulnerabilities in their products, services and distribution lines. Without an

[7] 'How small banks manage money laundering and sanctions risk: Update', FCA, November 2014

[8] 'Anti-money laundering annual report 2013/14', FCA, July 2014

adequate risk assessment to cover the business and the customers' banks on-board, banks leave themselves vulnerable to being used as conduits for money laundering.

Politically Exposed Persons (PEPs)

6.27 Regulated businesses must have systems and controls in place to identify and where necessary verify their customer. If the customer is a foreign PEP, the business is required to carry out enhanced due diligence (EDD). (Businesses may also carry out EDD on other customers, subject to their own risk assessments.) EDD measures include having approval from senior management for establishing a business relationship with that person; taking adequate measures to establish the source of wealth and source of funds; and conducting enhanced ongoing monitoring.

6.28 An analysis of ongoing and recently concluded investigations undertaken by the Serious Fraud Office and Metropolitan Police Proceeds of Corruption Unit highlight that proceeds of crime have been moved and placed through the banking sector. The sums of money in these cases were significant and linked to cases of international corruption and specifically to corrupt PEPs.

6.29 The complexity of these cases varies from transfer of illicit funds into a personal bank account through to more complex laundering processes using corporate vehicles, to conceal beneficial ownership information, and involving overseas jurisdictions.

6.30 There is evidence that banks are leaving themselves vulnerable when it comes to identifying, assessing and mitigating the risks associated with PEPs. In 2011, the FSA published a thematic review into banks handling of high risk situations which included a review into banks handling of PEPs.[9] They found around three-quarters of banks in its sample, including the majority of major banks, were not always managing high-risk customers and PEP relationships effectively with indications some banks were willing to enter into high risk relationships without adequate controls when commercial considerations were factored in.

6.31 The FSA found it likely that some banks were handling the proceeds of corruption or other financial crime. The FCA continues to find similar problems in relation to PEPs and high risk customers. Firms have improved their identification of PEPs since the FSA's 2011 report but concerns persist in firms' on-boarding of high risk PEPs.

Payments systems

6.32 Geographical risk, lack of harmonisation of regulatory and enforcement regimes, and transparency of the service and products used are some of the factors banks consider when assessing risk from payment systems.

6.33 Recent enforcement and supervisory activity have placed correspondent banking and the global payment system under focus, with banks increasing controls and exiting from a number of payment channels. Specifically, banks identify challenges in identifying, assessing and managing the risks around third party payments, wire transfers, correspondent banking and new payment methods. There are concerns from banks that they are expected to know their customer's customer – something which is not required to comply with AML/CFT requirements.

[9] 'Banks' management of high money-laundering risk situations', FSA, June 2011

Communication between law enforcement and the banking sector

6.34 The banking sector has for a long time asserted that poor information sharing between banks and law enforcement agencies limits their ability to put in place effective AML/CFT systems and controls.

6.35 The Joint Money Laundering Intelligence Taskforce (JMLIT) pilot, established in February 2015, involves representatives from the financial sector, NCA, City of London Police, and HMRC based in a single hub, developing an operational level understanding of money laundering risks. It been developed to provide an environment in which the financial sector and law enforcement agencies can exchange and analyse information and intelligence to detect, prevent and disrupt money laundering and wider economic crime threats against the UK.

6.36 JMLIT was set up under the auspices of the Serious and Organised Crime Financial Sector Forum. The Forum is chaired by the Home Office, British Bankers' Association and the NCA, with Director-level representation from leading banks and other financial institutions. The Forum meets three times a year to identify practical opportunities to make the UK's financial sector a more hostile environment for criminal activity, build international cooperation and help to recover the proceeds of crime more quickly and effectively.

Risks

6.37 The nature of the activities that banks undertake mean there is a high inherent money laundering risk within the sector, and law enforcement agencies are still developing the strength of understanding needed with regards to this risk. The money laundering risk within the banking sector is therefore assessed to be **high**. The terrorist financing risk within this sector is assessed to be **medium**.[10] On the basis of this analysis of the threats and vulnerabilities, the following risks are present in this sector:

- The banking sector is targeted by criminals seeking to move and store proceeds of crime, and by those moving funds in order to finance terrorism.
- Convergence of factors, such as systemic weaknesses in banks' control environments, the speed of transactions and the size of the banking sector, can increase the risk to banks of being used as conduits for money laundering and/or terrorist financing.

6.38 Where banks also provide other services covered by the regulations, such as trust or company services, accountancy, legal, MSB or other financial services, the risks set out in this assessment for those sectors are also relevant.

Accountancy service providers

6.39 The Money Laundering Regulations 2007 ('the regulations') place requirements on accountancy service providers (ASPs), including auditors, insolvency practitioners, external accountants and tax advisors, and reflects the requirements of the Third EU Money Laundering Directive. This includes 'statutory auditors' as defined under Part 42 of the Companies Act 2006[11]; 'insolvency practitioners' as defined under section 388 of the Insolvency Act 1986[12]; as

[10] Please see chapter 11 on terrorist financing.

[11] Companies Act 1989 c. 40

[12] Or article 3 of the Insolvency (Northern Ireland) Order 1989

well as any firm or practitioner who provides accountancy services or tax advice to other persons by way of business.

6.40 This assessment focuses on professionals providing the services covered by the regulations. This includes not only accountancy firms, but also firms which offer a range of services including accountancy services, such as large financial institutions. Businesses providing accountancy services may also offer trust or company services, or other services covered under the regulations.

6.41 At the start of 2014 there were over 23,000 businesses in the UK carrying out accounting, bookkeeping and auditing activities, and tax consultancy, more than 87% of which were micro-businesses, employing less than 10 employees. The combined annual turnover of businesses carrying out accounting, bookkeeping and auditing activities, and tax consultancy, was over £22 billion.[13]

6.42 Accountancy, auditing, bookkeeping and tax consulting services are a net export for the UK. In 2013 UK exports of these services were estimated to be worth over £1.4 billion.[14] It should be noted that many professional accountants fall outside of the regulations, as they operate in industry, commerce or the public sector. These activities present different risks to those undertaken by accountants offering services by way of business.

6.43 The regulations specify 13 accountancy professional bodies as AML/CFT supervisors.[15] Those firms and individuals that are not supervised by a professional body must be supervised by HMRC.[16]

Threats and vulnerabilities

6.44 Criminals can use accountants to conceal the origins of criminal funds and/or legitimise accounts in a variety of ways, such as the creation of companies, trusts and offshore corporate structures; providing false accounts; preparation or audit of businesses' annual accounts; insolvency malpractice; and providing advice. Many of the vulnerabilities set out below also leave accountants open to being used, wittingly or unwittingly, to assist the financing of terrorism.

6.45 The key threats and vulnerabilities within this sector identified through this assessment are:

- complicit professionals facilitating money laundering
- collusion with other elements of regulated sector
- coerced professionals targeted by criminals
- creation of structures and vehicles that enable money laundering
- the provision of false accounts
- failure to identify suspicion and submit SARs
- low barriers to entry and mixed standards of compliance with the regulators across the sector

[13] 'Business Population Estimates for the UK and regions: 2014', BIS, November 2014

[14] 'The Pink Book 2014', ONS, October 2014

[15] The Chartered Institute of Public Finance and Accountancy (CIPFA) withdrew from its role as a supervisory authority in January 2015 (The Money Laundering (Amendment) Regulations 2015).

[16] Accountancy bodies: Association of Accounting Technicians, Association of Chartered Certified Accountants, Association of International Accountants, Association of Taxation Technicians, Chartered Institute of Management Accountants, Chartered Institute of Taxation, Insolvency Practitioners Association, Institute of Certified Bookkeepers, Institute of Chartered Accountants in England and Wales, Institute of Chartered Accountants in Ireland, Institute of Chartered Accountants of Scotland, Institute of Financial Accountants, International Association of Book-keepers. Other regulatory agencies: Insolvency Service/DETNI; Financial Conduct Authority; HMRC.

- ASPs not registered under the regulations facilitating money laundering or terrorist financing (wittingly or unwittingly)
- inconsistences in the supervisory framework, and the potential for poor communication between supervisors

Complicit professionals

6.46 There are known instances where accountants have facilitated money laundering through the creation of complex corporate structures and offshore vehicles to conceal the ownership and facilitate the movement of criminal proceeds. In recent examples, an ASP facilitated the receipt and onwards transfer of proceeds from boiler room frauds and in a separate case the ASP helped launder large sums through a client account. Complicit ASPs sign off accounts, books and records for complicit cash rich businesses and there have been instances of suppressing business takings by knowingly providing false accounts.

6.47 Complicit ASPs have been identified as working alongside other professionals, such as solicitors and financial advisers, to facilitate money laundering. In one instance, an accountant provided third party verification on a series of high value criminal transactions overseas. Intelligence suggests that complicit accountants are often found acting independently within a company, where there is little scrutiny over the services they provide and their client base. In one extreme example, an entire accountancy firm was involved in money laundering for a wide range of criminals.

6.48 Supervisors assess that the majority of the sector are compliant. However, non-compliant or negligent professionals have the potential to cause significant harm.

6.49 As with the legal sector, the money laundering risk posed by the ASP sector in recent years has been heightened by a lack of a coordinated response. Work by the NCA and its partner agencies to developing their understanding of professionals who use their position to enable the laundering of criminal proceeds, and take action against them, will be expanded in due course to include ASPs.

Negligent professionals

6.50 Negligent professionals can enable money laundering and terrorist financing through non-compliance or poor compliance with the regulations and POCA. In some cases accountants may be wilfully negligent in order to gain a competitive advantage. Investigations undertaken by the Serious Fraud Office have uncovered instances of accountants with very poor understanding of the regulations; including the customer due diligence requirements, client acceptance and monitoring procedures.

6.51 Law enforcement agencies pursue cases where the accountant is complicit in the money laundering. Regulatory intervention or education may also be appropriate in order to increase awareness and reduce the risk of unwitting or negligent professional enablers. Law enforcement agencies are currently working with regulators to better understand the nature of the threat and work collectively towards tackling those cases where there is greatest risk. The Home Office is leading work with ICAEW, NCA and others on a campaign to increase awareness of money laundering threats within this sector.

Supervision

6.52 Supervisors report that while firms have a reasonable level of technical compliance, they see evidence of poor practices in the ASP sector, particularly among small firms and sole

proprietors. Particular areas of concern among supervisors are the levels of training, and the processes for identification of clients, ongoing monitoring and risk assessment.

6.53 Multiple supervisors supervise ASPs under the regulations. When supervisors fail to share information on firms they have struck off, this increases the risk to the sector and other supervisors. Challenges in applying effective risk-based supervision of sole proprietors and small firms can also be compounded when there are multiple supervisors. A lack of consistency between supervisors is likely to be a vulnerability and supervisors have expressed the need to share more information and best practice procedures to overcome the inconsistencies.

6.54 The 2012 amendments to the regulations introduced a power for supervisory authorities to share information with each other. Information sharing between supervisors has, as a result, improved since 2012 and is expected to continue to improve. The sector would also benefit from greater communication of information on threat and typologies between law enforcement agencies, supervisors and industry.

6.55 There are low barriers to setting up and operating as an accountant in the UK. 'Accountant' is not a protected term in the UK, which can mean anyone can set up and operate as an accountant.

6.56 The majority of ASP supervisors apply a 'fit and proper' process as part of their supervisory regime. The nature of the test varies between bodies and is a professional requirement rather than a statutory one. HMRC does not operate a 'fit and proper' test for ASPs as the regulations do not provide them with the legal powers to do so. They are only able to refuse registration in a limited set of circumstances.

6.57 In describing themselves as 'supervised by HMRC', businesses may also misleadingly imply that HMRC supervises their professional competence, rather than just their AML/CFT compliance. Unlike professional bodies, which supervise their members' professional conduct and AML/CFT compliance, HMRC only supervise the AML/CFT compliance of their supervisory population.

6.58 There is a need for further work to develop understanding on the exposure of UK ASPs to high risk customers. In 2013, UK exports of accountancy services were estimated to be worth over £1.4 billion. It is likely that the sector has exposure to high net worth individuals from overseas that may present a higher risk with access to the services and products provided by the UK market lending legitimacy to criminals.

6.59 ASPs may also provide trust and company formation services. Those that do are required to be registered with a supervisor as a TCSP (Trusts or Company Service Provider) under the regulations. Provision of trust and company services is viewed as an indicator of money laundering risk by accountancy supervisors (the risks present in the TCSP sector are set out later in this chapter).

SARs and law enforcement

6.60 The sector submitted 5,289 SARs for the reporting period 1 October 2012 to 30 September 2013. This total was generated by 1,580 registered reporters.[17] This figure is low compared to the overall size of the sector and nature of the activities it undertakes, which are

[17] Reporters register individually to submit via SAR Online. Therefore it is not possible to establish the number of firms reporting as opposed to multiple individuals per year, this figure could include multiple reporters from one firm.

attractive to those seeking to launder proceeds of crime. [18] Analysis of SARs from the accountancy sector identified that, in 21% of reports, the reason for suspicion was not clearly given and in 50% of the cases the reporter did not make it clear what services they were providing the client when suspicion arose.[19]

6.61 Supervisors report that a significant proportion of enquiries from law enforcement agencies are in relation to members they do not supervise under the regulations because the individuals in question are either not members of, or are not supervised by the professional body or are conducting business which falls outside the scope of the regulations. These enquiries relate to professionals who do not fall within the definition of ASPs in the regulations, for example because they are providing services in-house rather than by way of business, professionals who are carrying out activities which are covered by the regulations but which the individual is not registered to practice, and individuals who are members of, and may be supervised by, a different accountancy supervisor.

Risks

6.62 There are concerns over consistency of supervision of this sector, and the levels of compliance among regulated professionals, as well as the potential for individuals to operate without supervision. In addition, intelligence gaps exist in law enforcement's understanding of 'high end money laundering' involving professionals in this sector. The money laundering risk within the accountancy service providers sector is therefore assessed to be **high**. On the basis of the analysis of the threats and vulnerabilities, the following risks are present in the sector:

- criminals using ASPs, witting or un-wittingly, to provide legitimacy and to enable access to other regulated sectors without detection
- complicit ASPs using their expertise to facilitate money laundering, possibly alongside facilitating the predicate offence

6.63 Where accountancy service providers also provide other services covered by the regulations, such as trust or company services or MSB services, the risks set out in this assessment for those sectors are also relevant.

Legal service providers

6.64 This assessment focuses on professionals providing the services covered by the Money Laundering Regulations 2007 ('the regulations'). It also includes legal services offered by legal professionals from within larger businesses such as financial institutions and accountancy firms. The regulations apply to 'independent legal professionals' (firms or sole practitioners) who provide legal or notarial services by way of business to other persons when participating in financial or real estate transactions. This includes:

- the buying and selling of real estate property or business entities
- the managing of client money, securities or other assets
- the opening or management of bank, saving or securities accounts

[18] It should be noted that the UKFIU places no expectations on the volume of reports from different sectors; it only requires that legislation is followed and that SARs are submitted when it is appropriate to do so. Sectors and their regulators are encouraged by the UKFIU to judge if the volume of SARs submitted is proportionate to the threats their sectors face, and the quality of SARs is paramount as that impacts on their contribution to fighting criminality

[19] 1500 SARs were analysed, the majority of which were from small and medium sized businesses.

- the organisation of contributions necessary for the creation, operation or management of companies; or
- the creation, operation or management, or contributions to the creation, operation or management, of trusts or companies

and for this purpose, a person participates in a transaction by assisting in the planning or execution of the transaction or otherwise acting for or on behalf of a client in the transaction.

6.65 At the start of 2014 there were over 14,000 businesses in the UK carrying out legal services, more than 71% of which were micro-businesses, employing fewer than 10 employees. The combined annual turnover of businesses carrying out legal services was over £26 billion (though not all of this business would be related to the activities set out above).[20]

6.66 Legal services are a net export for the UK. In 2013, exports of these services were estimated to be worth over £3.5 billion.[21]

6.67 There are nine legal supervisors[22] in the UK, which between them supervise over 12,000 firms and 150,000 individuals.

Threats and vulnerabilities

6.68 Many of the services provided by the legal sector are attractive to criminals seeking to conceal the origins of criminal funds, and some legal professionals are acting as enablers to money laundering by providing access to these services. Many of the vulnerabilities set out below also leave legal service providers open to being used, wittingly or unwittingly, to assist the financing of terrorism.

6.69 The key threats and vulnerabilities within this sector identified through this assessment are:

- complicit legal professionals facilitating money laundering
- levels of compliance with the regulations and the POCA are viewed as mixed
- criminals use of legal professionals to secure property with criminal proceeds
- abuse of client accounts facilitated by complicit or negligent professionals
- challenges in supervision, especially in relation to small firms and sole proprietors

6.70 The risks associated with these threats and vulnerabilities are heightened when the volume of illicit proceeds and the complexity of laundering processes are increased.

6.71 It is not possible from the current intelligence picture to confidently assess which individuals within the legal sector present the highest risk. Law enforcement agencies' understanding of the scale of the threat and specific identities of the professionals involved in money laundering is improving (in particular in relation to solicitors), though a complete understanding remains an intelligence gap.

6.72 There is intelligence to show that a number of solicitors are involved to varying extents in laundering the proceeds of crime, although the vast majority of legal professionals are not

[20] 'Business Population Estimates for the UK and regions: 2014', BIS, November 2014

[21] 'The Pink Book 2014', ONS, October 2014

[22] Law Society of England and Wales (LSEW); Law Society of Northern Ireland (LSNI); Law Society of Scotland (LSS); General Council of the Bar (England and Wales) (GCBEW); General Council of the Bar of Northern Ireland (GCBNI); Faculty of Advocates (Scottish bar association) (FoA); Council for Licensed Conveyancers (CLC); Faculty Office of the Archbishop of Canterbury; Chartered Institute of Legal Executives (CILEx)

involved in money laundering and are compliant, or try to be compliant, with their legal obligations under POCA and the regulations.

Complicit professionals

6.73 There are known professional enablers within the legal sector who are facilitating money laundering through the purchase of property with criminal proceeds, and the creation of complex corporate structures and offshore vehicles to conceal the ownership and facilitate the movement of criminal assets.[23]

6.74 Although there are few complicit professional enablers known within the legal sector relative to the size of the sector as a whole, the potential impact they can have on money laundering remains high given their ability to conceal and disguise large sums of criminal money. They also pose a threat to the reputation and integrity of the vast majority in the legal sector who are not complicit in money laundering.

6.75 A recent high profile prosecution linked to the movement of proceeds of corruption highlighted the active involvement of a legal professional in money laundering by a corrupt overseas politically exposed person (PEP). [24] This case saw a complicit solicitor actively assisting in the money laundering process and also acting to conceal the identity of the PEP from other parts of the regulated sector, preventing other professionals from conducting effective due diligence.

6.76 Overseen by the Professional Enablers sub-group of the Criminal Finances Board, the NCA and its partner agencies are identifying solicitors who are associated with serious and organised criminals. Work will take place to disrupt those that present the highest risk, either through criminal, civil, or, in collaboration with the SRA, regulatory means.

Compliance with the regulations

6.77 The government assesses the standards of compliance in the sector to be mixed, with the majority compliant, or seeking to be compliant, with their legal obligations under POCA and the regulations. However, there are incidences of non-compliance and negligence in the sector, and supervisors report that they continue to see evidence of poor practices. Supervisors and law enforcement agencies have expressed concerns around poor customer due diligence (CDD), failures to ascertain source of funds or wealth, failure to gather beneficial ownership information and an absence of documented policies and procedures. Supervisors also report poor use of the reliance provisions under Regulation 17 of the regulations.[25]

6.78 The Solicitors Regulation Authority (SRA) 2014/15 Risk Outlook highlights the risk of having inadequate systems and controls which could leave firms vulnerable to money laundering through, for example, the transfer of money, specifically referencing conveyancing and client accounts.[26]

6.79 In a number of ongoing investigations undertaken by the NCA's International Corruption Unit[27] relating to PEPs and their close associates it has been identified that the regulations were not correctly applied and enhanced due diligence was not conducted appropriately.

6.80 Examples of weaknesses in law firms' CDD processes and policies have also been found in several complex and high profile investigations undertaken by the Serious Fraud Office. These

[23] Risks associated with the provision of trust and company services is covered later in this chapter, and the abuse of corporate vehicles for the purposes of money laundering, is covered in chapter 7.

[24] Case of Bhadresh Gohil solicitor to James Ibori – World Bank STAR (Stolen Asset Recovery) Database)

[25] See glossary for an explanation of the reliance provisions under Regulation 17 of the regulations.

[26] 'Risk Outlook 2014/15: The SRA's assessment of key risks to the regulatory objectives', Solicitors Regulation Authority, July 2014

[27] Formerly the Metropolitan Police Proceeds of Corruption Unit.

cases relate to larger law firms that have diverse specialist areas, for example criminal defence, mergers and acquisitions and conveyancing. In these cases the firm has been aware of a criminal investigation into a client as a result of the contact with the client through the criminal defence team, however, the same firm has then completed mergers or conveyancing on behalf of the same client without submitting a SAR. This has led to identified asset dissipation and, in one case, the defendant fleeing the jurisdiction.

6.81 Failure to comply with the reporting requirements in POCA or the obligations in the regulations is a criminal offence. However, where negligent professionals are identified, regulatory intervention or education may be a more appropriate response in order to increase awareness and reduce money laundering/terrorist financing risk.

6.82 In 2014/15 the Home Office led an awareness campaign within the legal sector in close partnership with the Law Society, Solicitors Regulation Authority and National Crime Agency (NCA). The aim was to increase understanding and awareness in the sector of both the threat of serious and organised crime to the legal profession and also of the profession's legal obligations under POCA and the regulations. A similar campaign, focussed on the accountancy sector, will be launched later this year.

The use of legal professionals to secure property with criminal proceeds

6.83 The purchase of real estate is attractive for money laundering purposes. Recent high profile international corruption cases have demonstrated that corrupt PEPs have obtained property in the UK and elsewhere in the world.[28] Law enforcement cases show that UK criminals invest proceeds in property and property also represents the most valuable asset type held by UK criminals against whom a confiscation order is made.

6.84 The SRA's 2013 'Conveyancing thematic study' found that a quarter of the 100 firms surveyed had experienced a client attempting to use a conveyancing transaction to commit property-related fraud or money laundering.[29]

Abuse of client accounts

6.85 Law enforcement agencies in the UK have seen cases where client accounts have been used to provide personal banking facilities to criminals, move and store large sums of criminal proceeds and to obscure the audit trail of criminal funds.

6.86 The regulation sets out that regulated entities, such as banks, can, under certain circumstances (such as taking on another regulated entity as a client), apply simplified due diligence. In the case of the legal profession, banks who offer client account services (or designated accounts) can apply SDD. The purpose of Regulation 13 is to assist interaction between regulated businesses. However Regulation 13 is dependent on both sides implementing the provisions of the regulations proportionately and appropriately.

6.87 This vulnerability is potentially greater when the legal professional is acting as a sole proprietor, as there will also be no third party internal checks on compliance and proper use of the client account.

---

[28] 'TI-UK response to the National Risk Assessment of Money Laundering and Terrorist Financing', Transparency International UK, May 2014. James Ibori (former governor of Delta State in Nigeria), Diepreye Alamieyesiegha (former governor of Bayelsa State in Nigeria) and Saadi Gaddafi (son of Muammar Gaddafi, former ruler of Libya) all owned property in the UK.

[29] 'Conveyancing thematic study: Full report', Solicitors Regulation Authority, March 2013

6.88 Independent audits of client accounts help to provide assurance and identify anomalies in transactions. The Solicitors Regulation Authority has recently consulted on introducing risk-based criteria that will exempt firms with a certain profile from the requirement to obtain and deliver an accountant's report of client accounts. [30] Doing so could increase the money laundering vulnerability associated with solicitors' client accounts if a risk-based approach is not effectively applied.

6.89 Criminals have also attempted to coerce legal professionals into facilitating laundering by paying funds into client accounts without the consent or knowledge of the solicitor. Criminals then seek repayment of the money in an alternative form, such as a cheque, in order to obscure the audit trail and disguise the origins of the funds.

6.90 Legal professionals should be aware that they are vulnerable to being targeted by criminals because of the skills, services and products they provide which can facilitate money laundering, and the legitimacy they can lend to a criminal's activities.

Reporting SARs under POCA

6.91 Overall reporting in the sector has decreased year-on-year since 2006/2007. The number of reports filed fell by 8% between 2012/13 and 2013/14 (from 3,935 to 3,610) despite the number of registered reporters increasing over the same period. [31] These figures seem low compared to the overall size of the legal sector and nature of the activities it undertakes, which are attractive to those seeking to launder the proceeds of crime.

6.92 The NCA does not prescribe the correct volume of SARs reporting from different sectors; it only requires that legislation is followed and that SARs are submitted when it is appropriate to do so. Sectors and their supervisors are encouraged by the NCA to judge if the volume of SARs submitted is proportionate to the threats their sectors face. The quality of SARs is paramount because that is the most important factor in their contribution to fighting criminality.

6.93 Approximately 75% of all SARs from the legal sector are consent SARs.[32] The NCA's analysis of SARs from the legal sector found that 42% of consent SARs required follow up with firms because the initial report was incomplete. At times, the poor quality of SARs indicated a lack of understanding or compliance with the regulations and POCA by the submitter.

Supervision

6.94 The supervision of sole proprietors and small firms is challenging for supervisors because of the high numbers of firms involved. This can create vulnerability if a risk-based approach to supervision is not effectively applied by the supervisor.

6.95 Over recent years there has been a considerable amount of national co-ordination and engagement between law enforcement agencies, government and legal sector supervisors. This has led to an improved understanding of the risks and a greater focus on money laundering by the supervisors.

Risks

6.96 Services provided by the legal sector, such as conveyancing and client account facilities, mean that they are exposed to a high inherent money laundering risk. In addition, intelligence gaps exist in law enforcement's understanding of 'high end money laundering' involving

[30] 'Proportionate regulation: reporting accountant requirements', Solicitors Regulation Authority, November 2014

[31] 'Suspicious Activity Reports (SARs) Annual Report 2014', NCA, December 2014

[32] See glossary.

professionals in this sector. The money laundering risk within the legal services sector is therefore assessed to be **high**. On the basis of this analysis of the threats and vulnerabilities, the government considers the principal risks in this sector to be:

- complicit legal professionals facilitating money laundering by enabling criminals to access legal services, and by granting them access to the rest of the regulated sector
- the provision of services by negligent or unwitting legal professionals that enable the transfer of funds, particularly through conveyancing and client accounts[33]
- negligent legal professionals' failure to comply with their obligations under POCA and the regulations leading to failure to conduct effective due diligence and identify suspicious activity

6.97 Where legal service providers also provide other services covered by the regulations, such as trust or company services or accountancy services, the risks set out in this assessment for those services are also relevant.

Money service businesses

6.98 The Money Laundering Regulations 2007 ('the regulations') apply to money service businesses (MSBs) who undertake money transmission services, cheque cashing or currency exchange.

6.99 The money service business (MSB) sector is diverse, with participants ranging from large international corporations who operate worldwide to local corner shops offering remittance services to their community. MSBs offer an important service to those who do not use, for a variety of reasons, the traditional banking sector.

6.100 Two supervisors regulate MSBs. MSBs which are not credit and financial institutions must register and be supervised by HMRC under the regulations.[34] The FCA is responsible for supervising money transmission, currency exchange and cheque cashing activities where they are undertaken by a regulated firm, for example a retail bank who offers currency exchange through one of its branches or as a wholesale supplier of currency to other businesses. HMRC is required by the regulations to maintain a register when they are the supervisor and conduct a 'fit and proper' test on those who apply to be registered as an MSB. Approximately 3,000 businesses are currently registered with HMRC as MSBs.

Threats and vulnerabilities

6.101 The nature of the services provided by the sector can make it attractive to criminals seeking to conceal the origins of criminal proceeds by, for example, remitting the funds overseas, or converting them into high denomination foreign notes. The services provided by MSBs can also be attractive to terrorist financiers, who exploit the same vulnerabilities to fund terrorism.

6.102 Although efforts over recent years to enhance the supervision of the sector have produced higher levels of compliance with the Regulations, intelligence indicates that some MSBs are still being used for money laundering on a significant scale.

[33] Provision of trust and company services is covered later in this chapter.

[34] Money Transmitters registered with HMRC under the regulations are also subject to conduct supervision by the Financial Conduct Authority (FCA) for their compliance with the requirements of the Payment Services Regulations 2009.

6.103 Law enforcement agencies report that they have seen some displacement of cash handling activity to other sectors, including high value dealers (HVDs), as a result of supervisory and law enforcement activity.

6.104 The threats and vulnerabilities in the MSB sector are:

- the transfer of criminal funds overseas
- the use of currency exchange services to convert criminal cash into high denomination foreign notes
- the control of MSBs by organised crime groups;
- The use of complicit employees within MSBs by criminal groups
- third party payments
- the transfer of cash into other payment methods such as digital currency and electronic money
- levels of compliance with the regulations and POCA

Transfer of criminal funds overseas

6.105 Many MSBs offer money transmission services, enabling customers to send money overseas for a small fee. MSBs are commonly identified by law enforcement agencies as a key enabler in cases where criminal funds are transferred overseas, and law enforcement agencies judge that complicit MSBs offering money transfer services are a favoured and readily available money laundering vehicle for organised crime groups. The NCA assesses that at least £1.5 billion of UK criminal proceeds go through MSB remittance each year, with the actual figure likely to be significantly higher.

6.106 Criminals have utilised the cover of MSBs to exploit vulnerabilities in the banks' overnight 'bank quick drop' facilities to place criminal cash into the banking system with limited oversight. Once the cash is in the banking system, MSBs are able to transfer it electronically anywhere in the world. The amount laundered in just 2 such cases totalled £250 million. In these cases, the criminal cash was accounted for by the MSB, giving the impression that it had come from legitimate sources.

Control of MSBs by organised crime groups

6.107 MSBs have also been specifically set up and structured to facilitate money laundering for organised crime groups (OCGs). These MSBs may be used by 'international controllers' (professional money launderers, usually based overseas, who operate laundering networks across multiple jurisdictions) to collect and transmit criminal funds around the world.

Third party payments

6.108 Some money transfer MSBs legitimately use third party settlements to balance their books. However, there is evidence to suggest that a small number of complicit MSBs hide their money laundering activities behind these payment methods.

6.109 The methodology sees criminal cash deposited in the UK to facilitate payment of an equivalent amount elsewhere in the world. Such parallel transactions assist money laundering because they are difficult for investigators or supervisors to connect and identify the criminal from the transaction.

Currency exchange

6.110 Many criminal groups require large amounts of foreign currency to pay their suppliers overseas. They also seek to reduce the bulk of the currency they smuggle through borders by using high denomination notes. The risk posed by high denomination notes is set out in detail in chapter 8.

6.111 Examination of money laundering prosecutions by HMRC, the Metropolitan Police Service and the NCA between 2011 and 2013 indicates that a small number of currency exchange MSBs laundered in excess of £500 million per year.[35]

6.112 Cases involving currency exchange MSBs indicate that criminals use MSBs to convert street cash into smaller bundles of high denomination foreign notes to conceal the origins of funds and as a precursor to cash movement or cash smuggling across borders. This activity will not be detected where there is negligence or a lack of compliance on the part of the MSB or other entity.

6.113 It is thought that only a small fraction of criminally-derived funds converted into high denomination notes is seized inland or at UK borders each year, and that criminal groups are successfully smuggling significant amounts of cash out of the UK.

Suspicious activity reporting

6.114 The MSB sector is responsible for the second largest number of reports from across all sectors (MSBs were responsible for 4% of all SARs filed, with banks responsible for 82%). In 2013/14 the number of SARs filed by the MSB sector fell by 30% from the 2012/13 figure, from 21,343 to just 14,990. This may be accounted for in part by the reduction in the number of principal MSBs (those who would file a SAR). HMRC report that the number of principal MSBs has fallen by 21%.[36] This is believed to be partly a consequence of banks exiting MSBs and partly due to HMRC supervisory intervention. In some cases this has led to the expansion of large agent networks and complex supply chains, which in themselves create vulnerabilities.

6.115 Some organisations within the MSB sector do not identify suspicion or file suspicious activity reports (SARs). In some cases, the quality of reporting is deficient, lacking the requisite level of detail. Many SARs from this sector are submitted after the transaction has been processed, which, whilst providing useful information for intelligence purposes, denies law enforcement agencies the opportunity to intervene to prevent the movement of criminal funds.

Threats identified by industry

6.116 The supervisor and law enforcement agencies have worked closely with the sector to reduce money laundering and terrorist financing risk over a number of years. Most of the sector has a well-developed understanding of the threats it faces, drawing on the extensive information provided by the supervisor and law enforcement agencies.

6.117 The MSB sector reports that money transfer services present the highest risk, with criminals making small payments to avoid customer identification and verification checks. The sector also identifies the use of agents as a vulnerability both because of the fraud risk they pose and because agents can be particularly vulnerable to exploitation by criminals. MSBs view e-money products, such as prepaid cards, as enablers for money laundering and terrorist financing because they provide greater anonymity and facilitate the movement of funds.

[35] 'Intelligence Assessment, Criminal Finances: Criminal Exploitation of the Money Service Business Remittance Sector', NCA

[36] 'Suspicious Activity Reports (SARs) Annual Report 2014', National Crime Agency, December 2014

Business model and structure of the sector

6.118 The MSB sector has a wide range of business models. It contains the largest banks and financial institutions with complex corporate group structures, and small single location operators that have small scale MSB services alongside their main retail business in the same shop. The currency supply element of the MSB sector in the UK is structured in the form of a pyramid: four main cash suppliers supply a number of wholesalers, who, in turn, supply hundreds of retail operators. Some of the larger of these retail operators have branches to act as representatives. The Money Remittance sub-sector, outside of the larger banks and other financial institutions, has a range of business structures from small single premise operators up to larger network operators (principals) who deliver remittance services through a network of agents rather than branches.

6.119 The supervisor has noticed changes in the structure of the MSB remittance sector recently, with a reduction in the number of principal business registrations and an increase in the number of those businesses registering as agents of larger (and expanding) remittance network organisations. These changes may be a result of the trend of banks withdrawing services from the MSB remittance sector, a particularly acute manifestation of the broader 'de-risking' trend, which has made it increasingly difficult for retail MSBs to secure banking facilities.

6.120 The relationship between the retailer and agent can create a money laundering/terrorist financing vulnerability, particularly when a retailer employs a large number of agents. Retail MSBs may find it more difficult to maintain effective oversight of their agents, in order to ensure those agents are discharging their legal and regulatory obligations, when the number of agents is greater.

Compliance with the regulations and POCA

6.121 According to HMRC, levels of compliance across the sector are mixed; there are examples of good practice and areas where poor practices persist. The majority of operators in the MSB sector are compliant, or are trying to be compliant, with their legal obligations under POCA and the regulations. Some MSBs are complicit in facilitating money laundering/terrorist financing, some are negligent in due diligence and some ignore obligations under the regulations.

6.122 Unwitting MSBs can assist money laundering and terrorist financing through their non-compliance with the regulations and POCA. Negligent wholesale MSBs can facilitate money laundering/terrorist financing by a criminally complicit retail MSB. A number of wholesale MSBs have relied on simplified due diligence when dealing with smaller retail MSBs, in some cases only conducting a basic check to establish that the owner and business exist. Suspicious transactions may not be identified in cases where the MSB has poor due diligence provisions or misunderstands how to apply the regulations.

6.123 HMRC and the sector itself believe more work is required to improve implementation of the regulations. The business models employed in the sector and a lack of awareness and understanding of legal and regulatory obligations contribute to the challenges faced by the supervisor as it seeks to build on its work to raise standards.

6.124 Failure to implement the regulations effectively leaves the sector vulnerable to exploitation by criminals seeking to launder funds. MSBs face particular implementation challenges with regard to conducting adequate customer due diligence (CDD), record keeping, transaction monitoring, and the appropriate application of simplified due diligence (SDD) on customers. Correctly understanding and applying Regulation 17 of the regulations (under which an MSB will rely on

another MSB's due diligence, with consent) and conducting enhanced due diligence (EDD) on customers that pose a higher risk also pose significant implementation challenges for MSBs.

International regulation

6.125 The lack of regulatory and legal harmonisation internationally creates different expectations in different jurisdictions and can create obstacles when running an international money service business. A lack of consistency in the legal and regulatory framework can increase the possibility of vulnerabilities, for example, in a firm's enterprise-wide risk assessment. These challenges can be compounded within the EU by the legal and regulatory uncertainties around the home state and host state supervision of retailers and agents.

Supervision

6.126 MSBs may be supervised by both HMRC (under the regulations) and the FCA (under the Payment Services Regulations 2009). This means there is a potential for different supervisory approaches to be deployed to a sector that is deemed to be a target for criminals and therefore vulnerable to being used as conduits for money laundering and terrorist financing. The FCA and HMRC have a Memorandum of Understanding (MOU) in place to assist in overcoming any challenges presented by the current supervisory structure.

6.127 Work is underway to identify what additional powers and tools could be used to increase oversight and supervision of the MSB sector and improve compliance with the regulations. In September 2014, HMRC successfully prosecuted an MSB owner for persistent failures under the regulations. He was jailed for 12 months. HMRC has taken significant steps in this area and the regulation and oversight of this sector is undoubtedly improving. HMRC has issued revised guidance to the sector, and published an e-learning product to enhance understanding of obligations in the sector, as well as significantly increasing the number of compliance visits in the sector in 2014/15. HMRC continues to build on this further to strengthen enforcement activity against regulatory breaches.

Risks

6.128 While the MSB sector remains a sector with significant high-risk elements within it, both in exchange and remittance, the capacity and capability of HMRC and the law enforcement agencies to combat money laundering through the sector means that the overall risk is assessed to be **medium**. The terrorist financing risk within the sector is assessed to be **high**.[37] On the basis of this analysis of the threats and vulnerabilities, the following risks are present in this sector:

- complicit money transfer MSBs are a favoured vehicle for money laundering and terrorist financing
- criminals are using currency exchange services offered by MSBs to convert criminally-derived cash into high denomination notes to facilitate cash smuggling, and only a relatively small proportion of smuggled cash is identified and seized
- MSBs in the UK are used by international controllers and play a significant role in international money laundering networks widely used by UK criminals

[37] Please see chapter 11 on terrorist financing.

- negligent MSBs are failing to comply with their legal obligations under the regulations and POCA and are thereby enabling money laundering and terrorist financing
- the changing structure of the MSB sector, with an increase in the number of agents, may create greater challenges for the supervisors and lower overall levels of compliance in the sector

6.129 The risks set out in this assessment for MSBs are also relevant for other regulated entities, such as banks, which provide MSB services.

Trust and company service providers

6.130 This section focuses on professionals and firms that fall within the definition of trust or company service providers (TCSPs), as set out the regulations.[38]

6.131 Under the provisions of the regulations, TCSPs may be supervised by one of many supervisors.[39] Firms such as accountancy, legal and financial services providers may also provide TCSP services. Where an organisation or individual is not supervised by a professional body or an authorised person regulated by the FCA, they must register and be supervised by HMRC. HMRC is required by the regulations to maintain a register when they are the supervisor and conduct a 'fit and proper' test on those who apply to be registered as TCSPs.

Threats and vulnerabilities

6.132 The nature of services provided by the sector, such as the creation of companies, trusts and offshore corporate structures, can be attractive to criminals seeking to conceal the origins of criminal funds or move criminal proceeds overseas. The vulnerabilities set out below can also leave TCSPs open to being used, wittingly or unwittingly, to assist the financing of terrorism.

6.133 Threats and vulnerabilities in the TCSP sector are:

- negligent or complicit TCSP facilitating money laundering
- criminal abuse of companies and trusts set up by TCSPs
- supervisory framework likely to lead to inconsistencies in approach
- the standard of implementation of the regulations across the sector is mixed

Negligent or complicit TCSPs

6.134 Law enforcement agencies investigations relating to the misuse of corporate vehicles, specifically limited companies, limited liability partnerships (LLPs) and limited partnerships (LPs),

[38] The Money Laundering Regulations 2007 ('regulations') provide that the regulations apply to 'trust or company service providers', defined as a firm or sole practitioner who by way of business (and when providing such services) provides any of the following services to other persons: (a) forming companies or other legal persons; (b) acting, or arranging for another person to act: (i) as a director or secretary of a company; (ii) as a partner of a partnership; or (iii) in a similar position in relation to other legal persons; (c) providing a registered office, business address, correspondence or administrative address or other related services for a company, partnership or any other legal person or arrangement; (d) acting, or arranging for another person to act as either a trustee or an express trust or similar legal arrangement or a nominee shareholder for a person other than a company whose securities are listed on a regulated market.

[39] TCSP supervisors include: HMRC; Financial Conduct Authority; Association of Chartered Certified Accountants; Institute of Chartered Accountants of England and Wales; Institute of Chartered Accountants of Scotland; Institute of Chartered Accountants in Ireland; Association of Accounting Technicians; Association of International Accountants; Association of Taxation Technicians; Chartered Institute of Management Accountants; Chartered Institute of Taxation; International Association of Bookkeepers; Institute of Financial Accountants; Institute of Certified Bookkeepers; Law Society.

to facilitate money laundering have found it is likely TCSPs have been used in the setting up of these entities.

6.135 Law enforcement agencies believe it is likely that there are enablers, or complicit professionals, in the TCSP sector facilitating money laundering through the creation of complex corporate structures and offshore vehicles to conceal the ownership and facilitate the movement of criminal proceeds.

6.136 Criminals may also use virtual office, mail forwarding or serviced office services provided by TCSPs, wittingly or unwittingly, to help add another layer of anonymity when laundering criminal finances.

Criminal abuse of companies set up by TCSPs

6.137 A handful of current investigations have indicated TCSPs as nominee directors of a large number of limited companies. Enforcement of directors' roles and legal responsibilities in the UK is weak and may not deter individuals from money laundering and predicate offending. For example, several law enforcement investigations have found TCSPs acting as nominee directors of large numbers of limited companies.

Supervision

6.138 TCSPs may be supervised by one of a number of different supervisors, (financial services providers, legal service providers and accountancy service providers may all be TCSPs). This presents challenges in ensuring supervision of the sector is consistent. For example, ensuring an appropriate and proportionate application of the fit and proper regime, and/or professional requirement certification, across the sector has been raised by supervisors and NGOs such as Transparency International, as challenging.

6.139 The number of TCSPs registered with a supervisor for AML/CFT and operating in the UK is currently unknown as professional body supervisors do not uniformly record whether firms supervised by them for other reasons are also TCSPs.

Compliance with the regulations

6.140 Supervisors report there are examples of good practice in the sector however implementation of the regulations and, in particular, the quality of customer due diligence are reported as being mixed across the sector.

6.141 The 2012 international study 'Global Shell Games' found that 49% of UK TCSPs who responded to email approaches were not compliant with the international 'Know Your Customer' standards. [40]

6.142 TCSPs must carry out customer due diligence (CDD) when establishing a 'business relationship" and/or if in the course of business they assess and/or suspect there is money laundering or terrorist financing risk. Discussions with sector representatives suggest that there is some confusion over what qualifies as an 'occasional transaction' under the regulations. Some believe the formation of a company falls under the 'occasional transaction' provision in the regulations (because there is no ongoing sequence of transactions), not a 'business relationship', and are therefore not carrying out appropriate CDD.

[40] 'Global Shell Games: Testing Money Launderers' and Terrorist Financiers' Access to Shell Companies', Michael Findley, Daniel Nielson and Jason Sharman, October 2012.

6.143 The nature of the services offered by TCSPs mean they do not see the activity of the company once it is formed, unless they subsequently provide further services to that customer. It can therefore be difficult for the TCSP or provider of the service to identify money laundering following the formation of the company. For the TCSP, the onset of the transaction (i.e. being instructed to form the corporate vehicle) is when suspicion would present itself. Therefore having adequate understanding of the regulations, and of the indicators that trusts or companies are being established to facilitate money laundering or terrorist financing, is an important preventative measure for TCSPs.

International exposure to high risk customers

6.144 The highly regarded reputation of the UK business community is used as a commodity by criminals to avoid scrutiny by law enforcement. UK TCSPs advertise their services overseas and can provide corporate structures to international based OCGs which can be used to open bank accounts which facilitate money laundering related criminality, however, the scale of the misuse of services provided by UK TCSPs is an intelligence gap. Industry representatives report that some parts of the sector have exposure to non-resident high net worth customers, and that ascertaining source of wealth for such customers can be a challenge.

6.145 There have been a number of international studies by the FATF and the World Bank into the misuse of corporate vehicles for illicit purposes.[41] Law enforcement agencies have identified cases of UK TCSPs being used to create complex structures to facilitate money laundering.

Risks

6.146 While the misuse of corporate vehicles to facilitate money laundering is a known global problem, the limited interaction most TCSPs have with the finances of the corporate vehicles they form means that the money laundering risk within the sector is assessed to be **medium**. TCSPs may however be used to conceal the identities of those involved in illicit activities, frustrating law enforcement investigations. On the basis of the analysis of the threats and vulnerabilities, the following risks are present in this sector:

- creation of front companies and complex corporate structures for money laundering
- inadequate control environments in place to prevent the misuse of this service by criminals

6.147 Where TCSPs also provide other services covered by the regulations, such as accountancy, legal or banking services, the risks set out in this assessment for those sectors are also relevant.

Estate agents

6.148 The Money Laundering Regulations 2007 ('the regulations') apply to 'estate agents', defined as a firm or sole practitioner who, or whose employees, carry out estate agency work in accordance with section 1 of the Estate Agents Act 1979 (as modified). This assessment focuses on professionals providing the services covered by the regulations.

6.149 At the start of 2014, there were estimated to be over 20,000 businesses (not all covered by the regulations) in the UK carrying out estate agent activities or estate management services

[41] 'Money Laundering Using Trust and Company Service Providers', FATF, October 2010; 'The Misuse of Corporate Vehicles, Including Trust and Company Service Providers ', FATF, October 2006; 'The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It', The International Bank for Reconstruction and Development / The World Bank, October 2011

on a fee or contract basis, more than 85% of which were micro-businesses, employing less than 10 employees. The combined annual turnover of businesses carrying out real estate activities on a fee or contract basis was over £16 billion.[42]

6.150 There were over 1 million residential property transactions in the UK in 2013, worth nearly £254 billion. The non-residential property market saw approximately 59 thousand transactions, worth nearly £86 billion.[43]

6.151 The main categories of estate agency services captured by this definition, and so covered by the regulations, are residential and commercial estate agency services, property or land auctioneering services and relocation agency or property finder services.[44] The regulations were amended in 2012 to include UK estate agents selling property outside the UK.

6.152 The regulations apply to those carrying out services related to the purchase or sale of property. They do not currently apply to businesses which only provide letting agency or property management services.[45]

6.153 Estate agents are required to carry out CDD on their customers; in the majority of property transactions only the seller is a customer of an estate agent. CDD will not be carried out on the buyer by an estate agent unless the buyer is independently represented, and so is therefore a customer of an estate agent, property finder or relocation agent. Legal Service Providers are required to carry out checks on the purchaser side of the transaction as part of the conveyancing process in the majority of cases.

6.154 In April 2014 supervision of the estate agency sector moved from the Office of Fair Trading (OFT) to HMRC. HMRC supervises approximately 8,500 estate agents, applying a risk-based approach.

Threats and vulnerabilities

6.155 The key threats and vulnerabilities within the estate agency sector are:

- complicit professionals negotiating and arranging the purchase of property
- negligent professionals enabling money laundering and terrorist financing through non-compliance with POCA and regulations
- need to increase standards of compliance with the regulations among the registered population
- challenges to ensure those covered by the regulations are registered
- low levels of SARs submitted
- the international exposure of the UK property market; rising prices also increase the attractiveness to criminals of investing in UK property
- HMRC does not operate a 'fit and proper' test for estate agency businesses as the regulations do not provide them with the legal powers to do so

[42] 'Business Population Estimates for the UK and regions: 2014', BIS, November 2014

[43] 'Annual UK Property Transaction Statistics', HMRC, June 2014

[44] The government amended the Estate Agency Act 1979 in 2012 to exempt businesses which act only as intermediaries providing a platform for private sellers to advertise their properties and provide a means for buyers and sellers to communicate.

[45] Money laundering through letting agencies is currently an intelligence gap.

- misuse of third party reliance by estate agents, or use of reliance when the bodies being relied upon may be complicit

Complicit professionals

6.156 Property is a favoured method for criminals to integrate the proceeds of crime into the legitimate economic and financial system, often after layering the proceeds using legal entities and arrangements. This means property may be bought by a company or trust used by the criminal or their accomplice in order to make it more difficult to identify or trace the illicit activity that generated the funds. There are known professional enablers within the estate agency sector who are facilitating money laundering through arranging and negotiating the purchase of property.

6.157 For many estate agents, even if effective due diligence is in place there may be challenges in law enforcement identifying the proceeds of crime. Where there are complicit professional enablers from other elements of the regulated sector acting for the customer with the express intent of concealing the illicit nature of the client's activities (such as a complicit lawyer, financial advisor or mortgage provider), it is more likely that the customer will successfully conceal the source of the funds used even where the estate agent has robust CDD measures in place.

6.158 There are concerns over the quality of reporting from this sector. NCA analysis of SARs from the estate agency sector indicated that SARs lacked clarity in their reason for reporting, indicating a lack of general understanding of the requirement and purpose of reporting.

Negligent professionals

6.159 Estate agents are required by law to identify their customer, generally the vendor. In addition, some estate agents may also conduct due diligence on the buyer, often for commercial reasons.

6.160 The absence of robust CDD processes within some elements of the sector combined with low SARs reporting leads to low levels of information for law enforcement agencies to act on.

Supervision

6.161 HMRC is aware that firms do not always register or otherwise identify themselves for supervision, which presents challenges for them as a supervisor, and it is expected that there is a shortfall of estate agent businesses on the register. The supervisor has a proactive programme in place to identify and contact businesses who may be liable to register, and have already increased estate agent registrations by 10% since taking over supervision from the OFT.

6.162 Among those estate agents that are registered, HMRC and law enforcement agencies report that the standard of AML/CFT compliance needs to be strengthened, and that firms often lack understanding of what is required of them under the regulations and POCA, including applying customer due diligence and submission of SARs. There is also a lack of understanding in the sector as to which entities are covered by the regulations, specifically that the regulations cover not only high street estate agents, but also commercial estate agents, land and property auctioneers, and relocation agents.

6.163 Estate agents are required to register with HMRC for supervision under the regulations, but there is no 'fit and proper' test as there is no legal basis for this.

International exposure of the UK property market

6.164 The UK property market attracts significant amounts of foreign investment, particularly in London. In 2013, estate agents Knight Frank reported that, in London, foreign buyers made up

63% of new build transactions and 42% of prime market transactions.[46] It is likely that some of this investment originates from individuals who may be high net worth, and/or high risk.

6.165 The UK property market is made more vulnerable because property can be purchased through off-shore holding companies which obscure the ownership and residency of those using the properties. Once the property is purchased it is a long and complicated process for law enforcement agencies to investigate, restrain, and recover criminal property.

6.166 Estate agents also report difficulties in ascertaining the ultimate beneficial owner when the property is owned by a trust or corporate entity, particularly when it is a non-UK trust or company.

Reporting of SARs under POCA

6.167 There are concerns over the number and quality of reports submitted by the sector. In 2013/14 there were 179 SARs submitted by the sector, a drop of 17% on 2012/13.[47] This figure is low compared to other sectors, and analysis of SARs submitted in 2012/13 has found that in 10 of the 73 consent SARs submitted the reason for suspicion given was known LEA interest.[48] This highlights the activity was only reported once law enforcement identified an interest to the reporter. However this needs to be balanced against the fact that estate agents do not directly handle any funds.

Third party reliance

6.168 Estate agents do not handle the transfer of money, so property transactions usually involve other regulated bodies, such as legal professionals and financial services providers. Reliance under Regulation 17 of the regulations allows estate agents to rely on a regulated third party (such as a solicitor) to apply CDD measures in certain circumstances, provided that the third party consents to this. In such circumstances the estate agent remains liable for any failure to apply these measures. Reliance is intended to help the regulated sectors to rely on each other, and so to assist the provision of business and services in the UK. However reliance may pose a risk if it is used incorrectly, or if the third party is complicit in the money laundering/terrorist financing.

6.169 The supervisor reports that it is common for estate agents not to conduct due diligence on their clients and instead to rely on that conducted by other regulated firms. They may do so without seeking consent from the firm that has conducted due diligence, or may take false comfort in the fact that another regulated body is dealing with the customer later in the business relationship, and so not conduct proper due diligence themselves. This can leave the estate agent with a poor understanding and knowledge of their client which will make it more difficult for them to identify anything suspicious about the client or the transaction.

6.170 The sector has also reported that when they try to undertake more in depth investigation of their customers the legal professionals involved in the conveyancing process can be unwilling to share any information beyond the minimum legally required.

Risks

6.171 While there are significant concerns about the levels of compliance in the estate agency sector, the capacity for estate agents to be used to launder money without the involvement of other professionals is limited as they do not handle funds. The money laundering risk within the sector is therefore assessed to be **medium**. Investment in real estate is attractive both to

[46] 'International Residential Investment in London', Knight Frank, 2013

[47] 'Suspicious Activity Reports (SARs) Annual Report 2014', NCA, December 2014

[48] In the period 1 October 2012 to 31 September 2013

legitimate customers and those wishing to use the sector for criminal purposes. The expansion of the UK letting industry makes it increasingly attractive to criminals seeking to launder funds, or provide other facilities to support criminality.

6.172 On the basis of the analysis of the threats and vulnerabilities, the following risks are present in this sector:

- criminal use of estate agency professionals and complicit professional enablers to sell or purchase property
- complicit estate agents facilitate sale or purchase of property by criminals, sometime working in conjunction with other complicit professionals
- perceived low understanding of ML/TF impact and risks in the sector, and the need to strengthen compliance with regulations

High value dealers

6.173 The UK's Money Laundering Regulations 2007 ('the regulations') define a high value dealer (HVD) as a firm or sole trader who by way of business trades in goods (including an auctioneer dealing in goods), and receives in respect of any transaction a high value payment (HVP), meaning a payment or payments in cash of at least €15,000.[49] A HVP may be made in a single payment or in a series of payments that appear to be linked. Any firm or sole trader which engages in this activity must be registered with HMRC for supervision under the regulations.

6.174 The €15,000 threshold was set by the EU Third Anti-Money Laundering Directive, which was transposed into UK law through the regulations. The EU Fourth Anti-Money Laundering Directive, which will be transposed into UK law within 2 years of publication in the Official Journal on 5 June 2015, reduces the threshold to €10,000. The regulations will be updated in due course to take account of the new minimum standards.

6.175 Approximately 1,300 businesses have registered with HMRC for supervision. Many registered HVDs are small businesses, with alcohol trading the most common type of business amongst the registered population.

Threats and vulnerabilities

6.176 The nature of services and products the sector provides makes it attractive to criminals seeking to convert criminal proceeds into luxury goods, high value portable assets which can be easily moved outside the UK, or to conceal the origins of criminally derived cash. Intelligence indicates 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.

6.177 Threats and vulnerabilities where high value cash payments are involved:

- criminal use of the sector to purchase luxury and high value goods with criminal proceeds
- HVDs enabling money laundering through complicity, including the use of HVD businesses to transfer large sums of criminal cash into the regulated sector

[49] Businesses selling goods with a turnover in cash of over €15,000 are not HVDs unless they accept high value payments (HVPs).

- negligent HVD operators enabling criminals to launder criminal proceeds or enabling the financing of terrorism due to failures to fully comply with the regulations and POCA
- the challenges inherent in supervising this particularly diverse sector

Criminal use of the HVD sector

6.178 An increasing number of organised crime groups have been identified by law enforcement agencies as being involved in large-scale criminality using trade-based money laundering involving high value goods, using unregistered businesses to bank cash in order to launder the proceeds of crime.

6.179 HMRC sees HVDs used by crime groups involved in alcohol fraud. Organised Crime Groups (OCGs) have been known to register companies as HVDs to provide a veneer of legitimacy, but in many cases the trading companies are used to facilitate money laundering.

Compliance with the regulations

6.180 Over the past 12 months HMRC has conducted intensive supervision of this sector. They found that there are HVDs who comply with their legal and regulatory obligations, and have good control frameworks in place to identify, assess and mitigate money laundering risks, but this is not representative of the whole sector. HMRC report that the HVD sector has a level of complicit enablers which has raised the risk in this sector, though enforcement action has significantly reduced the number of HVDs remaining on the MLR register.[50] As a result of weak levels of compliance the sector can be vulnerable to being used for money laundering/terrorist financing.

6.181 HMRC view alcohol traders as a higher risk group within the sector, with an element of embedded criminality in this group. There are also a significant number of unregistered HVDs who have failed to identify themselves to HMRC and who are currently operating outside the supervisory regime. It is highly likely that some of the unregistered HVDs are enabling money laundering or terrorist financing through negligence and non-compliance with the regulations and POCA obligations.

Criminals targeting HVD businesses

6.182 HVDs can often be largely cash based and have a significant turnover. This can provide cover for the movement of large sums through the banking system, and intelligence indicates that criminals target cash rich businesses such as fine jewellers and luxury car dealerships to provide cover for large sums of criminal proceeds. The same risk applies to cash based businesses who do not accept high value payments and so by definition are not HVDs – large cash turnover could provide cover for criminal cash.

6.183 Of concern is the exploitation by criminals of vulnerabilities in the 'bank quick drop' system (a bank drop box where businesses can deposit their cash and cheques) operated by some retail banks, which can allow businesses to easily deposit cash into the banking system with limited oversight.

Supervision

6.184 Effective supervision of this sector is made more difficult by the number and diversity of businesses that meet the definition of an HVD in the regulations.

[50] HMRC supervises HVDs, accountancy service providers, trust and company service providers, money service businesses and estate agents.

6.185 Under the regulations HMRC must maintain a registry of HVDs. However the regulations do not enable HMRC to conduct a 'fit and proper person' test on those who seek to register as an HVD. From 2004 there was a significant increase in the population of HVDs on HMRC's register. HMRC believes the absence of a fit and proper test creates a low barrier to entry and therefore a potential vulnerability in this sector. Through gaining a better understanding of business models prior to registration, HMRC has introduced a more rigorous programme of registration, which has seen many applications withdrawn and the total number registered steadily declining.

6.186 HMRC indicates that there is a significant challenge to raise awareness amongst businesses selling goods and who accept large cash payments for single transactions as they may be liable to register and to be supervised by HMRC under the regulations. The low number of registered HVDs also makes it more difficult to establish a fully informed risk assessment of the wider sector.

SARs reporting

6.187 HVDs submitted 331 SARs in 2013/14, which represents less than a tenth of 1% (0.09%) of all the SARs filed in 2013/14.[51] It is also a reduction of nearly 10% on 2012/13 figures. This fall may be accounted for by a move away from the use of cash for high value purchases by HVDs' customers, but there is insufficient information available to form a definitive judgment.[52] Whilst the NCA does not prescribe the number of SARs that should be filed by any sector, a figure of 331 seems low and further emphasises the vulnerability created by the low level of registration in this sector.

Risks

6.188 While there are concerns about the level of registration within the HVD sector, and the use of businesses with HVD registration as a front for criminal activity, the limited capacity to launder large volumes of money through a HVD as a customer means that the money laundering risk is assessed to be **low,** in comparison to other regulated sectors**.** On the basis of the threats and vulnerabilities analysed above, the following risks are present:

- HVD businesses are being used to launder the proceeds of crime, exploiting the 'bank quick drop' system
- low levels of compliance with the regulations and POCA by negligent HVD operators are enabling criminals to launder the proceeds of crime
- low levels of SAR reporting across the sector
- the low number of registrations, which suggests there may be a level of under-registration

Gambling operators

6.189 While all gambling operators are subject to the provisions of POCA, the Money Laundering Regulations 2007 ('the regulations') currently apply only to casinos (defined for this

[51] 'Suspicious Activity Reports (SARs) Annual Report 2014', NCA, December 2014

[52] 'Suspicious Activity Reports (SARs) Annual Report 2014', NCA, December 2014

purpose as the holder of a casino operating license issued by the Gambling Commission).[53] This assessment focuses on operators covered by the regulations (both remote and non-remote casinos),[54] and other categories of operator who offer services which may be used to launder money (other remote operators and retail betting operators).

6.190 The gambling sector is highly segmented, with a wide range of operators offering diverse products in different environments to a variety of customers. The sector differentiates into remote (online) and non-remote (premises or land based) gambling. The remote sector consists in the main of casinos, betting (both direct to the customer and betting exchanges), bingo and some lotteries. The non-remote sector also comprises casinos, betting (on and off-course), bingo and lotteries and also includes arcades. Different combinations of product and environment present different types of money laundering risk.

6.191 There are almost 150 land-based (or 'non-remote') casinos operating in Great Britain, holding a 16% share of the whole (licensed) gambling market, making it the third largest sector in the gambling industry. [55]

6.192 As of February 2015 there were approximately 170 remote casino licences issued by the Gambling Commission, up from 27 licences issued in March 2014 (before the Gambling (Licensing & Advertising) Act 2014 came into effect.

6.193 There are over 9,000 licensed betting shops in Great Britain. They represent the largest market within the industry with a 47% market share. The bingo, arcade, and large society lottery sectors make up 20% of the gambling industry.[56]

Legal framework

6.194 Gambling firms operating in Great Britain are licensed by the Gambling Commission under the Gambling Act 2005 (the Act). [57] The Act sets out three licensing objectives, the first of which is to prevent gambling from being a source of crime or disorder, being associated with crime and disorder, or being used to support crime. Responsibility for delivering the licensing objectives falls primarily on licensed businesses. To help businesses achieve required standards, the Gambling Commission attaches a range of conditions, and publishes guidance and advice. In addition the Gambling Commission is the anti-money laundering supervisor under the Regulations for remote and non-remote casinos.

6.195 The Gambling (Licensing and Advertising) Act 2014 requires all gambling operators that offer services to customers in Britain to be licensed by the Gambling Commission, wherever they are based. The number of remote gambling licenses has increased substantially since the Act came into effect in November 2014. The Commission's licence conditions and codes of practice also extend the coverage of the Regulations to operators based overseas, where those operators are offering services to consumers in Great Britain. The impact of this change on the effectiveness of the UK's anti-money laundering regime are currently being assessed.

[53] Gambling operators that do not hold a casino operating licence are not covered by the regulations, this includes arcade, betting, bingo and lottery operators (both remote and non-remote).

[54] See glossary for definitions of remote and casinos and gambling operators.

[55] 'Gambling Commission – Industry statistics April 2009 to March 2014', Gambling Commission, November 2014

[56] 'Gambling Commission – Industry statistics April 2009 to March 2014', Gambling Commission, November 2014

[57] In Northern Ireland gambling activities are licenced by courts and district councils, and the Department of Social Development is responsible for track-betting licences. Casinos are not permitted under Northern Irish law.

Threats and vulnerabilities

6.196 The nature of the services and products the sector provides can make it attractive to criminals seeking to spend criminal proceeds as part of a criminal lifestyle or to conceal or disguise the origins of criminally derived cash.[58] Many of the vulnerabilities set out below can also leave gambling operators open to being used, wittingly or unwittingly, to assist the financing of terrorism.

6.197 The key threats and vulnerabilities in the gambling sector are:

- criminals attempting to gain control of gambling businesses
- cash transactions by largely anonymous customers
- criminals using gambling to conceal the origin of criminal proceeds
- levels of compliance with the Regulations and POCA
- criminals using services and products to move or store the proceeds of crime
- the sector's exposure to criminals' 'lifestyle' spending

Criminal attempts at gaining control of gambling businesses

6.198 A small number of organised crime groups have sought to secure licences to operate regulated gaming establishments. This would give them direct access to a cash rich business through which they could launder their proceeds, or invest illicit funds into a profitable and seemingly legitimate enterprise. This remains a constant threat mitigated by a range of investigations conducted by the Gambling Commission at licensing stage, including financial integrity and criminal background investigations.

Money laundering through casinos and gaming outlets

6.199 While the casino sector is currently subject to the regulations, the vast majority of gambling transactions take place in cash in circumstances where the individual is not known to the gambling operator. The combination of this anonymity and use of cash can conceal the source of funds and with this, generate a vulnerability to money laundering.

6.200 In order to disguise the origins of criminal funds criminal cash has been exchanged for chips in casinos, with individuals then gambling and cashing out after accepting up to a 10% loss. A number of recent cases highlight the use of this methodology to launder large sums through a variety of casinos.

6.201 This methodology is also used in online gambling, where criminals have placed criminal proceeds into online gambling services such as betting or poker, accepted a small loss and exited with the remaining funds. Law enforcement agencies believe criminals have used these value instruments to launder large sums.

6.202 Ticket In Ticket Out (TITO) vouchers from machines in casinos, arcades or betting shops can also be used for money laundering. They can be cashed in at a later date or by third parties and criminals have made use of a range of outlets to cash in and out to conceal and disguise the origins of funds.

[58] Including foreign money exchange, electronic fund transfers and safety deposit boxes.

6.203 The regulator has published the results of a number of cases that indicate weaknesses in the industry's ability to recognise 'lifestyle' spend of criminally derived funds. This stems from what the regulator describes as insufficient curiosity by operators about source of funds, and a tendency for any attempts at due diligence to be satisfied too easily.

6.204 Casinos may also offer additional facilities such as customer accounts, foreign money exchange, electronic fund transfers and safety deposit boxes. In the absence of robust control environments these additional services can be vulnerable to facilitating money laundering. One particular such development is the 'common wallet' being developed by some gambling operators to bring together a customer's activity across a range of products and platforms. Such developments may offer means to move criminal funds. They may also offer opportunities to the industry, regulators and law enforcement to ensure greater visibility of customer activity.

Levels of compliance with the Money Laundering Regulations and POCA

Implementation of the regulations: non-remote casinos

6.205 The supervisor reports that non-remote casinos have policies and procedures in place aimed at delivering compliance with the regulations. However, their casework has highlighted areas of weakness in firms' systems and controls, including customer due diligence (CDD), the identification and management of politically exposed persons (PEPs), SARs reporting and the discharge of Money Laundering Reporting Officers' (MLRO) responsibilities.

6.206 Given the nature of their business, operators report that carrying out CDD, in particular enhanced due diligence, can be challenging. The industry says that this is further hampered by criminals' use of false identification documents, or the use of proxies to play or stake on their behalf, in order to circumvent casinos' CDD measures.

6.207 The industry says that the €2,000 threshold[59] in the regulations can present opportunities for criminals to conduct multiple transactions just below the threshold in order to avoid CDD ('smurfing'[60]). This can be particularly acute if an operator does not have an adequate control environment to identify this type of activity.

Implementation of the regulations: remote operators

6.208 The regulations only apply to remote casino operators that are licensed by the Gambling Commission. The Gambling Commission reports that the level of compliance with the Regulations and POCA by remote casinos, and other remote operators, is yet to be fully assessed given the recent change in the licence regime to include all remote operators that offer a service to British customers.

6.209 The non-face-to-face nature of online gambling can make customer verification challenging.[61] This is reflected in Regulation 14 of the regulations, which requires enhanced CDD to be carried out when the customer has not been physically present for identification purposes. Firms should be aware of the risks present when operating online, and must have systems in place to ensure adequate CDD is carried out in order to mitigate this vulnerability.

[59] Under the regulations casinos must establish and verify the identity of customers either when the customer enters the casino, or when, over a period of 24 hours, the customer: pays to or stakes with the casino €2,000 or more; pays the casino €2,000 or more for the use of gaming machines; or purchase or exchanges chips with total value of €2,000 or more.

[60] Smurfing - breaking up a large amount of money into smaller transactions that are below a threshold.

[61] 'Moneyval Research Report: The use of online gambling for money laundering and the financing of terrorism purposes', Council of Europe, April 2013

6.210 Remote operators can also accept e-money products, which can in some circumstances be purchased without any due diligence; this can make it challenging for the gaming operator to ascertain the true source of the funds and can therefore create a vulnerability.

6.211 However it should be borne in mind that the account based nature of remote gambling, and the inherent auditability of activity may offer advantages in implementing AML and other controls relative to land based equivalent activity. The Gambling Commission reports that the industry is still at an early stage in making the best use of this opportunity.

Suspicious activity reporting

6.212 The number of suspicious activity reports (SARs) submitted by the casino and gaming industry is on an upward trend, with the number of reports made by casinos in 2013/14 up 12% on the year before, and the number of reports received from the unregulated gaming sector up by nearly 80% over the same period. The UK Financial Intelligence Unit ascribes this increase to work by the supervisor and the NCA to encourage appropriate reporting.[62]

6.213 This is a positive development, as recent enforcement activity by the Gambling Commission highlighted cases in which casinos and betting operators had failed to identify suspicion and file SARs. In these cases the undetected criminal proceeds funded high levels of play, which on occasions led to the businesses offering loyalty rewards to the individuals involved.

Retail betting operators

6.214 Retail betting operators are not covered by the regulations. They are not required to verify or record the identity of their customers. This can make monitoring customer behaviour challenging, as systems are reliant on staff recognising customers by appearance or patterns of spend. It can also limit the information that can be provided to the NCA when reporting suspicious activity. The Gambling Commission reports that retail betting operators' compliance with the licence requirement to prevent gambling being used to support crime is mixed. Weak controls of a number of operators have been exploited to launder at times large amounts of criminally derived cash. The Commission is of the view that there remains significant scope in the sector to improve defences against criminal spend in particular.

6.215 The sector operates a business model based on high footfall, high turnover and low margins, where quick cash transactions are the norm. The combination of anonymity and extensive use of cash exposes the betting sector to particular money laundering risks. This can create a tension between commercial imperatives and the need to comply with controls which, if conducted properly, can be time consuming and increase the attractiveness of using black-market operators. It can also lead to suspicious behaviour being missed.

6.216 Operators can offer facilities for customers to deposit cash at a betting premises and collect payments at a later date, and/or at a different location. These services offer customers the ability to transfer and to store money outside of the conventional banking system. If operators are not carrying out due diligence on such customers this can present a money laundering/terrorist financing vulnerability.

Risks

6.217 Due to the substantial work undertaken by the Gambling Commission in recent years, there is a new focus in the sector on the risks of money laundering and the responsibilities of

[62] 'Suspicious Activity Reports (SARs) Annual Report 2014', NCA, December 2014

gambling operators licenced by the Commission to prevent it. Nevertheless, there remains considerable scope for further improvement. However, the scale of the sector is relatively small in comparison to others and as a result the overall money laundering risk in regulated casino sector and the retail betting sector assessed to be **low** in comparison to the regulated sectors.[63] Both sectors are still vulnerable to abuse by money launderers, and so present a higher risk than most sectors in the UK. It should be noted that if the recent efforts by the sector to improve standards were to lapse, or if businesses were to begin offering new products or services that increase the inherent vulnerability within that sector, then the overall risk could rise.

6.218 On the basis of this analysis of the threats and vulnerabilities, the government considers the principal risks in the gambling sector to be:

- negligent gambling operators allowing money laundering/terrorist financing in the gambling sector through poor compliance with regulations and POCA
- criminals gaining control of a gaming operator 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

Insurance providers

6.219 Internationally, the FATF recognises life assurance as being at risk to money laundering and terrorist financing. Life assurance business is covered by the Money Laundering Regulations 2007 ("the regulations").

6.220 General insurance and brokers are not covered by the FATF recommendations and are not covered under the Money Laundering Regulations 2007. At the time of transposing the EU's Third Money Laundering Directive, general insurance and brokers were regarded as low risk of money laundering.

6.221 However, whilst not all of the sector is captured under the regulations, the insurance sector must comply with other legal and regulatory obligations, including the requirement that all FSMA authorised firms[64] must put in place systems and controls to prevent all types of financial crime.

6.222 Insurance providers are dual regulated by the Financial Conduct Authority (FCA) for conduct of business, including financial crime and the Prudential Regulation Authority (PRA) for prudential requirements, such as capital and liquidity. The FCA is also supervisor under the Regulations for life assurance firms. The UK insurance market is third largest in the world, employing over 300,000 people and managing investment amounting to 26% of the UK's total net worth. [65] The insurance sector is one of the UK's biggest exporters with almost 30% of its net premium coming from overseas business.[66]

[63] The assessment of low risk is relative to other regulated sectors, in the specific context of this risk assessment. HM Treasury will separately consider the nature and extent of ML risk in the gambling industry in the context of its work to transpose the Fourth Money Laundering Directive. This assessment will naturally contribute to that work, but is not in itself sufficient to meet the 'proven low risk' test as set out in 4MLD.

[64] Under Section 19 of FSMA, any person who carries on a regulated activity in the UK must be authorised by the FCA (or exempt).

[65] 'UK Insurance Key Facts 2014', Association of British Insurers (ABI), September 2014 (ABI members account for 90% of the UK market)

[66] 'UK Insurance Key Facts 2014', Association of British Insurers (ABI), September 2014 (ABI members account for 90% of the UK market)

Threats and vulnerabilities

6.223 The scale and impact of money laundering and terrorist financing in the insurance sector is an intelligence gap. What is known is that the insurance sector is a target for fraud and, with recent geopolitical developments, Kidnap for Ransom policies have come under the spotlight.

6.224 The vulnerabilities in the insurance sector set out in this assessment are drawn from material gathered from supervisors such as the FCA and Lloyds of London.

6.225 The FCA (and previously the FSA) have conducted a number of financial crime thematic reviews into the commercial insurance sector, specifically reviewing the anti-bribery and anti-corruption systems and controls of brokers. Commercial insurance brokerage is viewed as posing a higher risk to financial crimes such as bribery and corruption and fraud; indirectly affecting the money laundering landscape of the UK.

6.226 The link between AML and anti-bribery and anti-corruption systems and controls is internationally recognised.[67] In 2010 the FSA's report into commercial insurance brokers found that the approach of many firms towards high-risk business was not of an acceptable standard and firms were not able to demonstrate adequate procedures were in place to prevent bribery from occurring. The report identified a number of common concerns across firms such as weak governance and a poor understanding of bribery and corruption risks among senior managers as well as little or no specific training and weak vetting of staff. The FSA found a general failure to implement a risk-based approach to anti-bribery and corruption and weak due diligence and monitoring of third-party relationships and payments.[68]

6.227 In November 2014 the FCA issued a follow up report on commercial insurance brokers assessing how the sector had responded to the specific issues identified in the 2010 report and subsequent actions. The report found most intermediaries did not yet adequately manage the risk that they might become involved in bribery or corruption. While more than half of brokers had commenced work in this area and start to manage bribery and corruption risk, for the majority of these intermediaries this work was still in progress.[69]

6.228 Consultation with stakeholders in the course of the NRA has revealed that issues similar to those found during the FSA's 2010 thematic review continue to persist in the sector; poor governance, weak vetting of staff and limited, poor information going to senior members of the board on AML/CFT issues. In particular the development and implementation of adequate risk assessments continue to challenge the sector.

Risks

6.229 The insurance sector is at risk of being targeted by criminals due to some weaknesses in its control environment and a lack of intelligence, which can enable a criminal to exploit the sector to further and conceal the proceeds of crime. However, there is an intelligence gap with regards to the incidence of money laundering in the sector. The risk of money laundering within the sector has therefore not been rated as part of this assessment.

6.230 Where insurance providers also provide other services covered by the Regulations, such as trust or company services or other financial services, the risks set out in this assessment for those sectors are also relevant.

---

[67] 'Laundering the Proceeds of Corruption', FATF, July 2011

[68] 'Anti-bribery and corruption in commercial insurance broking', FSA, May 2010

[69] 'Managing bribery and corruption risk in commercial insurance broking: update', FCA, November 2014

7 Legal entities and arrangements

7.1 This chapter considers risks associated with companies, other legal entities, trusts and partnerships in facilitating money laundering. It also considers aspects of corporate behaviour that may be open to misuse.

7.2 The number of businesses choosing to incorporate has continued to grow over the years, with February 2015 alone seeing over 50,000 incorporations. As of February 2015 there were over 3.4 million companies (and 60,000 Limited Liability Partnerships) on the UK's central company register.

7.3 Corporate vehicles and legal structures are attractive to those seeking to launder money, conceal the origins of criminal funds and/or move criminal proceeds overseas because it is easier for larger sums of money to be moved between legal entities without attracting attention. Corporate structures can also obscure the ultimate beneficial ownership of companies and assets, including property, making it harder to ascertain whether such companies or assets are linked to criminality.

7.4 The UK is committed to enhancing corporate transparency, increasing trust and tackling the misuse of companies. A package of reforms in the Small Business, Enterprise and Employment Act 2015 ('SBEE Act 2015') addresses complex corporate structures and other known abuses such as the use of bearer shares and nominee directors. The SBEE Act 2015 implements our 2013 G8 commitment to create a public central register of company beneficial ownership information – known in the UK as the "register of people with significant control". We will be one of the first countries internationally to do this.

UK company obligations and oversight

7.5 A company is a legal entity in itself, with an identity separate from those who own or run it. Upon its creation, or as it grows, a business may be registered as one of four main types of company:

- private company limited by shares – the company has a share capital but shares cannot be sold publicly. Each member's liability is limited to the amount unpaid on their shares
- private company limited by guarantee – the company has no share capital. The liability of each member is instead limited to the amount stated to be guaranteed by the members at the time the company is formed
- private unlimited company – the company may have a share capital, but there is no limit to the liability of a member
- public limited company - the company has a share capital and shares may be sold publicly and quoted on stock exchanges. Each member's liability is limited to the amount unpaid on their shares

7.6 In addition, there are several forms of partnership in the UK. The different structures allow partners (also called members) to have different responsibilities and liabilities for any debts the business cannot pay. The partners may elect whichever structure best suits their needs. A partnership may have legal personality (Scottish Partnerships (SPs), Scottish Limited Partnerships

(SLPs) and Limited Liability Partnerships (LLPs)) or no legal personality (Partnerships and Limited Partnerships). Members of partnerships may have unlimited liability (Partnerships and Scottish Partnerships), limited liability (Limited Liability Partnerships), or limited liability only when uninvolved in the business (in Limited Partnerships and Scottish Limited Partnerships, where there must be at least one general partner with unlimited liability and one limited partner).

UK trust obligations and oversight

7.7 Trusts are a common law legal concept and generally ownership of the assets of one party (the settlor) is transferred to another party (the trustee) to look after and use for the benefit of a third group (the beneficiaries). Trusts typically do not have a legal personality in the UK, so the assets held in a trust are not legally owned by the trust. Instead, the assets held in a trust are legally owned by the trustee(s).

7.8 Trusts may be used for personal reasons, including providing family support, protecting vulnerable persons, personal benevolence, or personal inheritance, and for commercial purposes, such as in a private pension scheme. Beneficiaries can be natural persons, or legal persons (such as a company) or arrangements (such as another trust). Trusts are also a commonly used charity structure; these trusts, unlike all other express trusts[1], are not required to have an ultimate ascertainable beneficiary. Conservative estimates place the number of express trusts administered in the UK at 1.5 to 2 million.

7.9 All trustees are required under UK common law to have information on the intent of the trust, the assets that constitute the trusts, and the beneficiaries. This is in line with the FATF recommendation that 'countries should require trustees of any express trust governed under their law to obtain and hold adequate, accurate, and current beneficial ownership information regarding the trust.'

7.10 Any entity regulated under the regulations, such as a financial institution or an accountant, must carry out customer due diligence when establishing a business relationship with a customer. This customer due diligence should include establishing whether the customer is acting as a trustee and will often extend to obtaining and verifying copies of trust deeds and deeds of appointment before a customer can be taken on. The Fourth Money Laundering Directive explicitly requires trustees to declare their status as a trustee in such circumstances, and to provide beneficial ownership information for their trusts.

7.11 Where a UK-administered trust has a domestic tax liability, trustees are also required to disclose a range of information to HM Revenue & Customs (HMRC) including information on trust settlors, trustees and beneficiaries. Under the Fourth Money Laundering Directive, information will be held in a central register, and will be accessible in accordance with the requirements of the directive. Information on trusts administered in other jurisdictions that have potential UK tax liabilities, including information on beneficial ownership and notification of payments made to beneficiaries, will be reported to HMRC through new international tax information exchange agreements.

Threat of misuse of legal entities and arrangements

7.12 The misuse of legal entities and arrangements is a known global problem. Many international banks will move money readily for companies, whereas doing so for individuals would attract attention and suspicion. The Organisation for Economic Co-operation and

[1] An express trust is a trust clearly created by a settlor, usually in the form of a document, for example a written deed of trust.

Development[2] has observed that: *"almost every economic crime involves the misuse of corporate vehicles [i.e. companies]"*. The World Economic Forum[3] has highlighted the increasing number of problematic cases confronting law enforcement agencies involving illegitimate business activity co-mingling with legal business activity, and illicit funds with licit funds.

7.13 While only a small minority of UK legal entities and arrangements are engaged in money laundering, as set out above, the quantity of money involved is significant. Misuse of corporate structures features frequently in law enforcement investigations – of the current money laundering cases being investigated by HMRC over 70% have used company structures for money laundering, moving over £800 million.

7.14 A 2011 World Bank review[4] found that out of 213 grand corruption cases investigated, 150 involved the use of at least one corporate vehicle to hide beneficial ownership. Of those 150 cases, the total proceeds of corruption were approximately $56.4 billion and across the study, 24 UK corporate vehicles were found to have been involved.

7.15 The misuse of companies is an issue in almost every case investigated by the SFO. The SFO has identified a number of instances in which 'off the shelf' companies have been used to facilitate criminal conduct. The following case examples demonstrate the diversity of the issues facing the regulated sector and law enforcement agencies. In some of these cases the presence of a beneficial ownership register, as has now been established under the SBEE Act 2015, would have aided law enforcement agencies in their investigations:

- evidence in a bribery and corruption case identified invoices alleging millions of turnover in a business that declared no assets and no employees; investigation found it was being used as a conduit in the layering and integration process for money laundering
- a bank received significant sums of money alleged to be the sale proceeds of assets purchased and sold within the same financial year yet the accounts submitted to Companies House demonstrate the corporate entity did not purchase or sell the assets in question and the bank had been misled
- a company incorporated directly with Companies House was used to transfer funds into the UK for the benefit of a fraud suspect. Details show the company directors and shareholders bear the same names as relatives of the suspect however it appears false addresses and dates of birth have been provided – it is suspected this is to disguise the relationship to the fraud suspect
- a defendant in a long running fraud case was subject to a restraint order covering all his assets. At confiscation, he was adjudged to hold an interest in a company used to receive rent from several properties. The company was supposedly owned by his wife and he went to great lengths to try to conceal his true role in controlling the company
- the main suspects in a commercial mortgage fraud had a portfolio of UK properties held through a Gibraltar company, which was subject to a restraint order. They set up a UK company with a similar name to the Gibraltar company and then diverted rental income from the properties to an account in the UK company's name and then dissipated it. The UK company filed minimal documentation and was purportedly controlled by the sons of one of the suspects

[2] 'Behind the Corporate Veil: Using Corporate Entities for Illicit Purposes', OECD, 2001

[3] 'Organised Crime Enablers', Global Agenda Council on Organized Crime, July 2012

[4] 'The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It', World Bank, October 2011

- a defendant in a major fraud case utilised an elaborate offshore trust structure to hold a range of assets in the UK and abroad, mostly through offshore entities. However, a significant property in France was nominally held by a UK company which filed little documentation and dormant accounts even though the property was generating large sums in rent. Ownership was never clear and the shareholders at various times included nominees, another company and the defendant's wife

7.16 Some of these cases suggest that the company in question was being used to deliberately conceal criminal activities, and that the regulated sector did not identify these activities, or was complicit in their concealment.

7.17 A main feature in the evidence gathered by this assessment is the use of "shell" and "off the shelf" companies to facilitate criminal conduct. A "shell" company is a company that serves as a vehicle for business transactions without itself having any significant assets or operations and an "off the shelf" company is one created which typically has no activity before being sold on. Both of these are legal structures only detectable sometime after a company has been incorporated. Criminals use existing company structures such as shell companies to launder money, taking advantage of the fact that a company's existing reputation and financial profile will make it less suspicious than a newly-formed company.

7.18 Another feature of these case studies is the use of companies which file dormant accounts for money laundering purposes. The difficulties in identifying if laundering has taken place through dormant companies is also a major issue for law enforcement agencies. A "dormant company" is a company that is registered with Companies House that is not active, trading or carrying on business activity.[5]

Limited Liability Partnerships (LLPs), Limited Partnerships (LPs) and Scottish Limited Partnerships (SLPs)

7.19 Law enforcement agencies report that transparency and scrutiny of LLPs, LPs and SLPs are restricted by the limited reporting obligations that these structures have. Partnerships are generally subject to less scrutiny than companies. Ordinary partnerships need not register other than for tax purposes. Limited Liability Partnerships by contrast are subject to many of the same requirements of Limited Companies and may be investigated under the Companies Act 1985. Limited Partnerships and Scottish Limited Partnerships have to register certain details with the Company Registrar, including the names of the partners and any capital contribution, but do not have to file accounts or returns and cannot be investigated under the Companies Act 1985. The relative freedom from filing obligations enjoyed by partnerships reduces the ability of law enforcement to easily make initial enquiries. This means that law enforcement agencies have a reduced ability to identify whether this type of structure is being used for legitimate or illicit activity. However, these undertakings can still be investigated using general powers of criminal investigation.

Law enforcement response

7.20 The UK's national-level response is currently focussed on tackling the professional enablers (including lawyers, accountants and trust or company service providers) who are involved in the creation of corporate structures for the purpose of facilitating money laundering. This includes the setting up of shell companies, trusts and other instruments in order to provide anonymity for criminals seeking to launder funds.

[5] According to Companies House's Statistical Release in April 2015, there are 3,494,282 companies on the register, of those 3,224,159 are graded as active, meaning that there are a total of 270,123 inactive companies.

7.21 The response is co-ordinated through the multi-agency Criminal Finances Threat Group and its sub-group on professional enablers led by the Serious Fraud Office (SFO). The response includes the analysis of SARs and other intelligence to identify professionals involved in the facilitation of money laundering; and the co-ordination of engagement with relevant regulatory bodies to target unwitting, negligent and complicit professionals through regulatory sanctions.

UK company landscape

7.22 Companies House, an executive agency of the Department for Business, Innovation & Skills, fulfils the registrar's functions, and works closely with law enforcement agencies across government, sharing information and searching/cross referencing its data in support of the UK's activities to detect fraudulent and criminal activity at all levels. The registrar is not a regulator of companies, but ensures they comply with their disclosure requirements in return for limited liability. The registrar carries out a statutory function: only the registrar can legally incorporate a company. He cannot choose not to incorporate a company if the required information has been properly submitted and is legally compliant.

7.23 A company may be incorporated either directly with Companies House or through a third-party such as a Trust or Company Service Provider (TCSP). For the financial year 2012/13, approximately three quarters of overall incorporations were conducted through a third party; the remaining quarter of entities were incorporated directly. When incorporating, a company is required to provide a range of details, such as the registered office address and details of its directors and shareholders. Companies House carries out a number of checks on this information, ensuring it is valid, complete and correctly formatted. The proportion of complaints about companies incorporating directly through Companies House is lower than the proportion relating to companies incorporated by TCSPs.[6]

7.24 Under the Money Laundering Regulations 2007, TCSPs must carry out appropriate customer due diligence (CDD) on their customer when setting up a trust or company, or undertake to act as Company Secretary or to provide Registered Office or Dormant Company services for the company. This can include establishing the source of wealth and source of funds, as well at the customer's intention. This assessment has identified a number of money laundering risks in the TCSP sector (see chapter 6).

7.25 Once incorporated, a company is placed on a register of companies maintained by the registrar. Following its incorporation, a company has an on-going duty under company law to provide updates to certain information upon change (e.g. a director's details), and to provide annually a set of accounts and an annual return of basic information.[7]

7.26 Companies House carries out a number of checks on all information received, ensuring it is valid, complete and correctly formatted, and in compliance with company filing requirements. In 2013/14, Companies House handled 9,000,000 transactions, including 500,000 new incorporations. Over 400,000 filings were rejected. These checks are not a guarantee of accuracy: the obligation to ensure the information is accurate lies with the company and its directors. However, the validation checks serve to help companies get it right. An offence is committed by the company if the information on their registers is inaccurate or incomplete.

7.27 The international standard, as expressed in the 2012 FATF recommendations, is that such information should be "adequate, accurate and timely". [8]

[6] For 2014/15, 83% of complaints (1092/1315) related to incorporations via TCSPs, 17% to direct incorporations.

[7] The annual return process will replaced by a check and confirm process in 2016.

[8] 'International standards on combating money laundering and the financing of terrorism & proliferation, the FATF recommendations', FATF, February 2012

7.28 The UK has amongst the highest rates of compliance with company filing requirements in the world– over 98% of annual returns and 99% of annual accounts are delivered valid, complete and correctly formatted to the central register. Digital services offered by Companies House have a high take-up rate. Approximately 99% of annual returns are filed online and nearly 65% of accounts. The digital services are designed to assist a company in complying with its obligations, and help companies provide good quality adequate and current information. The system automatically carries out checks, for example ensuring the accounts' balance sheet adds up, to help companies provide the right information.

7.29 With respect to ensuring the accuracy of data held, maintaining one of the most open and extensively accessed registers in the world is a powerful tool in identifying false, inaccurate, or possibly fraudulent information. Public registers are not required under international standards. They are strongly backed by NGOs. With many eyes viewing the data, errors, omissions or worse can be identified and reported. This means that the information held on the register can be policed on a significant scale by a variety of users.

7.30 In 2013/14, Companies House received just 9,109 reports. Of these, 2,499 related to potential unauthorised filings and, after analysis and where appropriate, were reported to law enforcement agencies. Companies House itself follows up on all complaints where information is incorrect or incomplete. In 80% of cases where there appears to be a breach of the legal requirements, companies correct the information immediately, suggesting that the cause is likely to be simple error, rather than fraudulent activity.

7.31 Many commercial users also take Companies House information alongside other data sources, and cross-reference these, before highlighting anomalies or errors back to Companies House. There are very simple routes for users to report possible anomalies, all of which are followed up by Companies House or law enforcement agencies. The level of such anomalies reporting is very low, suggesting that the information on the register is consistent with other data sources.

7.32 The register is accessed over 300 million times a year. Companies House bulk data is also extensively used by commercial users, including credit reference agencies and financial institutions. This use of the register's data – and in particular, the reliance by commercial users on Companies House data to conduct their business – is another indicator of general confidence in the usefulness and accuracy of information held.

7.33 There is little available evidence comparing the effectiveness of different jurisdictions' approaches to ensuring register integrity. A recent evaluation on the Netherlands register[9], which has 2.4 million registered entities and operates a notary/ID verification system, indicates that the data relating to main activities was 91-98% accurate. This is comparable to past findings from analysis of the accuracy of UK Companies House data.

7.34 From June 2015, all digital data held on the register are freely available, significantly expanding the scope for public scrutiny and for the scale of such policing to grow.

7.35 Companies House also carries out analysis of the register to identify and tackle companies where information provided may be inaccurate, or otherwise non-compliant. This includes:

- companies defaulting on annual returns or accounts
- patterns of suspicious activity in the filing of company accounts or other company data

[9] Presentation by Netherlands Chamber of Commerce to European Commerce Registers Forum – Rome, June 2014

- companies that have been restored to the register with number but not name
- companies that have been incorporated and dissolved within 12 months

7.36 Additional measures are now under consideration. The introduction of the UK's register of people with significant control in 2016 and implementation of the Fourth Money Laundering Directive in 2017 will provide further information on the public register. In parallel, Companies House and BIS have commissioned research into the effectiveness of other jurisdictions' verification systems. Companies House will introduce further measures to improve the integrity of information on its register.

Enforcement

7.37 The UK favours an approach that encourages transparency of information, followed by scrutiny of company information over its lifetime. In addition to its own work to improve data accuracy, Companies House works closely with other enforcement agencies, such as National Crime Agency and City of London Police, to make best use of registered company information in combating economic crime, sharing data analysis to help them identify suspicious activity and patterns of behaviour.

7.38 Companies House is part of the Government Agencies Intelligence Network (GAIN) and it files suspicious activity reports (SARs) with the NCA when it forms suspicions of money laundering, as well as filing reports with the Insolvency Service and the City of London police. Ahead of the introduction of the register of people with significant control, Companies House is currently working with enforcement agencies on ways to further improve working arrangements in order to identify cases of fraud and other illegal or suspicious activity, and pass this to enforcement agencies.

7.39 As well as its work with law enforcement to identify more serious crime, Companies House works to identify patterns and triggers which might indicate fraud and other potentially suspicious activity.

7.40 The overall aim is to gain compliance. Where compliance is not achieved, Companies House will use powers appropriately to ensure individuals and/or companies are prosecuted. In 2013/14 over 170,000 civil penalties with a value exceeding £80 million were imposed on companies for late filing of accounts. In the same year, Companies House successfully prosecuted over 1,800 directors of over 1,500 companies on behalf of the Secretary of State for not delivering annual accounts and/or annual returns by the statutory due date.

7.41 Cases are also escalated to BIS for further investigation and possible criminal prosecution. Companies House also works closely with Insolvency Service on ensuring compliance of the register with company law. In 2013/14, 168 companies were wound up by the Insolvency Service for a variety of reasons.

7.42 Where it appears to the registrar that a company is no longer in business or operation, the registrar may strike the company from the register. This is a powerful tool for the registrar to "tidy up" the public record. For the period April 14 to March 15 171,012 companies were subject to compulsory company dissolution (strike off), and 198,514 were struck off voluntarily. Provisions in the SBEE Act 2015 will, from October 2015, reduce the time it takes for the registrar to strike companies off the register. For compulsory strike off, the time period will reduce from the current 5-6 months to around 3-4 months.

Company directors

7.43 The SBEE Act 2015 introduced measures to deter opaque arrangements involving company directors, and increase accountability of individuals who have breached their duties as directors, or where individuals unduly seek to influence directors. These should further improve confidence in business and the enforcement regime.

7.44 Specifically, the act provides a power to ban the use of corporate directors (one company as the director of another), with specified exceptions in the UK. The act also clarifies that shadow directors (those controlling all or the majority of a company's directors) are expected to adhere to the same general duties as directors, where they are capable of applying. Failure to do so leaves shadow directors liable to enforcement action in the same way as directors. This strengthens the incentives on those seeking to instruct company boards to act in the best interests of the company.

7.45 With respect to so-called nominee directors, BIS had originally consulted on the suggestion of creating a register of nominee directors and those on whose behalf they operate. The consultation demonstrated that this would be unworkable, and easily circumvented. Instead, the SBEE Act 2015 introduced a new provision to tackle those people who have unduly influenced directors to act on their behalf.

7.46 The SBEE Act 2015 also introduces a new provision to allow disqualification proceedings against those instructing an unfit director. This means that if a nominee director is disqualified, this provision will allow the courts to look beyond the director to disqualify the individual instructing the nominee.

7.47 Finally, in addition to these legislative measures, BIS and Companies House are also seeking to raise levels of awareness amongst directors of their legal duties. This will involve sending readily accessible advice to all newly appointed directors setting out their legal duties (one of which is the duty to act with independent judgement), and the implications of failing to meet those duties.

Bearer shares

7.48 Bearer shares are unregistered shares owned by whoever physically holds the share warrant. This makes them anonymous and infinitely transferable, and an easy means of facilitating illicit activity, including money laundering.

7.49 The SBEE Act 2015 prohibits bearer shares being issued, requires existing bearer shares to be surrendered and exchanged for registered shares, or cancelled and compensated. Existing bearer shares will be abolished by 25 February 2016 in all but the most exceptional circumstances.

8 Cash

8.1 A number of predicate offences[1] generate proceeds in the form of cash (notably the sale of illicit commodities such as drugs and counterfeit tobacco). Cash is also used to complicate the audit trail in money laundering through the regulated sector.

8.2 Cash is attractive for money laundering and terrorist financing because it is relatively untraceable, readily exchangeable and anonymous. The money laundering risk associated with cash is assessed to be **high**, and the terrorist financing risk associated with cash couriering is also assessed to be **high**.[2] Criminals use cash to enable money laundering by:

- using high denomination notes to conceal or disguise the origins of funds or as a precursor to cash movement or cash smuggling
- moving criminal proceeds, in the form of cash, within and across borders
- using 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[3]

8.3 The law enforcement response to cash based money laundering is co-ordinated through a sub-group of the Criminal Finances Threat Group, chaired by HMRC. NCA-led projects are focusing on issues such as MSBs, International Controllers and domestic and cross border cash movements.

8.4 The following chapters set out the government's understanding of the money laundering and terrorist financing risks associated with cash and new payment methods. The terrorist financing threats are set out in detail in chapter 11, however, many of the vulnerabilities set out below leave the regulated sector equally open to abuse by criminals wishing to launder money and by those wishing to finance terrorism.

8.5 The table below sets out this assessment's conclusions on the risk of money laundering associated with payment methods.

Table 8.A: Money laundering risk rating (a summary of the methodology used to produce this rating can be found in chapter 1)

Thematic area	Total vulnerabilities score	Total likelihood score	Inherent risk	Inherent risk level	Risk with mitigation grading	Overall risk level
Cash	21	7	147	High	88	High
New payment methods (e-money)	10	6	60	Medium	45	Medium
Digital currencies	5	3	15	Low	11	Low

[1] Please see chapter 3 on predicate offences.

[2] Please see chapter 11 on terrorist financing.

[3] Please see chapter 6 on HVDs, banking, MSBs and gambling.

Criminal use of high denomination notes

8.6 The use of high denomination foreign currency in small sized bundles of large value is the easiest method of physically moving funds across borders. It requires only limited interface with the UK regulated sector.

8.7 Euro notes and dollars are attractive to money launderers because they disguise the origins of the criminality, whereas large volumes of sterling will indicate to law enforcement agencies that the predicate offending took place in the UK. High denomination notes also assist with reducing the physical size of the consignment being moved. If £10 notes are exchanged for €200 notes, the same value can be carried in just one fifteenth of the space. This makes large sums of criminal cash easier to conceal when moving them across borders. The most popular notes for money laundering are €100 and €200 and $100 notes due to their high ratio of value to size.

8.8 Previously, the €500 note was the most widely used note for money laundering. Law enforcement agencies and supervisors have worked with the financial sector to secure its agreement to withdraw the €500 from sale in the UK.

8.9 However, it is apparent that the €500 note is still being purchased from customers by the UK currency sector. NCA analysis of SARs in 2012 indicated that 158 reports relating to the €500 note, with an overall value of approximately €2.8 million, were received. The majority of these reports were submitted by the remittance sector and casinos. It is not known how many of these notes were sourced from UK based currency exchanges and how many were brought in to the UK from overseas.

8.10 The government judges the actual number of €500 notes in use by UK criminals to be significantly higher both because of the estimated scale of money laundering through the currency exchange sector and because the NCA analysis is only able to draw on instances in which a compliant reporting entity has identified and reported a €500 note.

8.11 As set out in chapter 6, currency exchange MSBs are a key source of supply of high denomination notes. In one case, one MSB service exchanged over £180 million into high denomination notes over a 2 year period, of which only approximately £10 million was recorded in its books and records.

International cash movement: cash couriers and cash smuggling

8.12 Many criminal groups require large amounts of foreign currency to pay their suppliers overseas. They also smuggle proceeds of crime overseas to avoid the reach of UK law enforcement agencies and realise the value of the proceeds elsewhere.

8.13 Cash couriers are used to move criminal cash across borders, whilst protecting the identity of the criminal concerned. In a recent prosecution involving the smuggling of cash to fund insurgency groups in Syria a courier was found carrying €500 notes concealed in her clothing

8.14 Euros, Sterling and US Dollars are the most commonly forfeited notes. Only a small fraction of criminally-derived funds converted into high denomination notes is seized inland or at UK borders each year. It is thought that criminal groups are successfully smuggling significant amounts of cash out of the UK. Between 1 April 2012 and 31 March 2014 approximately £2.17 million, €2.34 million and $788 thousand was seized and forfeited at UK borders.

8.15 The UAE, USA, Spain, Thailand, Turkey, Jamaica, China, France and Pakistan are the outbound destinations where the most undeclared cash is detected at the border. It is likely that a large element of this undeclared cash is linked to criminality. Nigeria, UAE, France, USA, Egypt and China are the routes where most undeclared cash is detected inbound into UK ports and airports. Although law enforcement cooperation and understanding of the threat has increased with joint teams working at key UK borders, further work is required to increase our understanding of the flow of criminal cash at the border and the jurisdictions that pose the greatest threat.

8.16 Given that fast parcels, cargo and freight routes are known to be used by criminals to move illicit commodities such as drugs, firearms and tobacco into and out of the UK, the government judges that these methods are also vulnerable to misuse for moving criminal cash across borders. The scale and nature of money laundering through freight and fast parcels is an intelligence gap. The UK is leading work with the FATF to assess the risks of money laundering through bulk cash movements across borders. It is likely that this work will increase our understanding of the risks in this area.

Cash rich businesses

8.17 Criminals have used cash rich businesses in order to conceal large sums of criminal cash using the cover of the business and by mixing criminal cash with legitimate income to disguise the origins of funds. Law enforcement intelligence indicates that scrap metal wholesalers, nail bars, takeaways, storage warehousing, MSBs, HVDs and short term loan businesses are also being utilised in this way. Criminals have also used the accountancy sector to sign off books and records of complicit cash rich businesses to provide an element of legitimacy.

8.18 Cash rich businesses provide criminals with cover for large sums of criminal cash which they can then deposit into "quick cash drop" services provided by banks. The NCA assess that the cover of the cash rich business combined with the use of the quick cash drop facility has meant that criminals have been able to place criminal cash into the legitimate banking system with minimal oversight.

9 New payment methods

Electronic-money (e-money)

9.1 In the UK e-money[1] issuers are covered by the Money Laundering Regulations 2007 ('the Regulations') and must comply with the provisions in the E-Money Regulations 2011 (EMRs), POCA and the European Wire Transfer Regulations. E-money products which are offered under a commercial agreement with the e-money issuer either within a limited network of service providers or for a limited range of goods or services are not required to comply with the Regulations or the EMRs (for example gift cards for a single retailer or group of retailers).

9.2 The UK has the highest concentration of e-money issuers in the EU with over 60 e-money issuers authorised or registered with the Financial Conduct Authority (FCA). UK banks are also able to issue e-money products, as are a number of EEA entities operating in the UK under the passporting regime. E-Money issuers may make their products available directly to consumers or provide e-money products for other businesses.

9.3 E-money issuers must have adequate systems and controls to identify, assess and mitigate financial crime risks which include, but are not exclusive to, money laundering and terrorist financing. The legal and regulatory responsibility sits with the e-money issuer whether or not they have engaged an agent, distributor or project manager.

9.4 The JMLSG provides guidance to e-money issuers on customer due diligence and related measures required by law.[2] It notes that e-money is susceptible to the same risks of money laundering and terrorist financing as any other retail payment product. In the absence of adequate systems and controls, it poses money laundering and terrorist financing risk.

Threats and vulnerabilities

9.5 The money laundering risk associated with e-money is **medium**, however terrorist financing risk associated with e-money is **low**. The nature of services and products the sector provides can make it attractive to criminals seeking to convert criminal proceeds into other payment methods or stores of value, conceal the origins of funds, remit funds overseas or transfer value between individuals.

9.6 Threats and vulnerabilities identified in the e-money sector are:

- criminal use of closed loop prepaid gift cards to realise proceeds from compromised credit cards
- the nature of the sector presents a challenge to supervisors and law enforcement
- levels of compliance with the regulations are not well known

Prepaid cards

9.7 There is a risk in the availability of open loop cards from overseas suppliers that can be remotely loaded and emptied. Criminals have also used closed loop prepaid gift cards to realise

[1] Electronic money (e–money) is electronically (including magnetically) stored monetary value, represented by a claim on the issuer, which is issued on receipt of funds for the purpose of making payment transactions, and which is accepted by a person other than the electronic money issuer. Types of e-money include pre-paid cards and electronic pre-paid accounts for use online. See http://www.fca.org.uk/firms/firm-types/emoney-institutions

[2] The Joint Money Laundering Steering Group (JMLSG) publishes industry guidance to assist firms in interpreting the Money Laundering Regulations.

the proceeds from compromised credit cards. Examples of ways in which prepaid cards have been used by criminals include:

- cards loaded with refunds for products purchased with the compromised credit cards
- criminals using gift cards to purchase other gift cards which were then sold online
- prepaid cards used to fund the costs of criminal activity; recent examples include cases where drug mules and illegal migrants were given prepaid cards with small loads on them to pay for travel

9.8 E-money issuers recognise that they can be targeted by criminals in the layering and extraction stages in the money laundering process. The industry gave the following examples of significant money laundering threats or indicators:

- funding of a product using one payment method and withdrawn using another
- multiple top ups on a product and/or large or regular top ups followed by multiple ATM withdrawals
- products funded through stolen instruments (e.g. credit cards)

Business model

9.9 The e-money sector offers a variety of products and services. E-money issuers can employ a range of firms to distribute their products and administer their services, such as project managers, agents and distributors. This is commonly referred to as the segmentation of services.

9.10 E-money issuers recognise they can be vulnerable when they use agents and distributors; particularly in relation to complicit activity such as payment terminal fraud. Monitoring the distribution chain, particularly when multiple participants are involved, is important to ensure threats and vulnerabilities are identified and mitigated.

Product risk

9.11 E-money provides accessibility, mobility, convenience and privacy, increased efficiency of transactions, lower transaction fees, and new business opportunities. However, near or absolute anonymity can be readily achieved.

9.12 The functionality of certain products can increase vulnerability to money laundering and terrorist financing. For example, where a product enables cash withdrawals; where there are no limits to usage and load ability of a product; where the product falls under simplified due diligence (SDD) limits and no due diligence is required; or where a product enables third party usage.

9.13 The geographic reach of certain e-money products can also increase vulnerability to money laundering and terrorist financing. For example, oversight and monitoring capabilities may be limited where the issuer, distributor or agent are based in different jurisdictions. Operating in many countries requires compliance with differing regulatory regimes, which can create challenges for e-money issuers when developing enterprise wide control environments to minimise their vulnerability to financial crimes such as money laundering. The cross border nature of certain products can also make it challenging for law enforcement to identify, track and seize illicit funds.

Supervision

9.14 E-money issuers in the UK are supervised by the FCA. In its 2013 AML/CFT Annual Report, the FCA referred to the risks in the e-money sector and emphasised the need for e-money issuers to have adequate AML/CFT systems and controls, and reported the case of one prepaid card/voucher issuer who did not apply systems and controls and who was targeted by criminals.

9.15 The AML/CFT supervision of e-money issuers and their use of agents and distributors can be challenging, due to the cross border nature of many e-money business models and the on-going development of this sector, which may contribute to a gap in supervisors' understanding of the market they are required to regulate.[3]

9.16 This challenge is exacerbated by different national approaches, legal uncertainties and responsibilities in cross border situations in the AML/CFT supervision of e-money issuers, agents and distributors. At the EU level there are discrepancies between the 3MLD and the Second E-money Directive (2EMD). This has led to other EU member states applying discretion in the application of AML/CFT legislation to agents and/or distributors and different rules applying to different entities in the transaction chain.[4] Passporting within the EU can add a further layer of confusion.

9.17 Due to the nature and size of the sector, e-money issuers fall under the FCA's reactive supervisory approach and are not subject to intensive supervision and proactive work.[5]

9.18 Under certain conditions, SDD can be applied to e-money products.[6] SDD is applied differently across the EU and as a result e-money issuers work to different requirements. This can affect consistency in application, particularly when so many UK e-money providers operate, via representatives such as distributors or agents, outside of the UK. Regulation 7 of the regulations requires customer due diligence to be applied if the issuer suspects money laundering or terrorist financing risk, regardless of threshold limits. The levels of due diligence applied must be commensurate with the risks presented.

9.19 Complying with legal and regulatory obligations is an important step to establishing a control environment to prevent and detect financial crimes such as money laundering, and terrorist financing, and thus reduce vulnerability. This sector continues to grow and it is important to ensure legal and regulatory obligations are followed to mitigate any possible weakness in the sector which criminals could potentially exploit.

Law enforcement vulnerabilities

9.20 Understanding criminal exploitation of the e-money sector remains an intelligence gap for law enforcement agencies. This is compounded by operational challenges. For example, in the majority of cases, prepaid cards do not carry a marking to differentiate them from other credit or debit cards. Therefore law enforcement agencies cannot readily identify the cards as being pre-paid and, furthermore are unable to identify the value on the instrument. This can present a low risk of detection for criminals travelling across borders.

[3] Joint Committee report – 'Report on the application of AML/CTF obligations to, and the AML/CTF supervision of e-money issuers, agents and distributors in Europe.', European Banking Authority (EBA), December 2012

[4] Joint Committee report – 'Report on the application of AML/CTF obligations to, and the AML/CTF supervision of e-money issuers, agents and distributors in Europe.', European Banking Authority (EBA), December 2012

[5] 'The FCA's Approach to Supervision for C4 firms', FCA, March 2014

[6] When the e-money products are either non-reloadable and have a total purse limit that does not exceed €250 (or €500 for domestic transactions), or reloadable and are not used to transact more than €2500 in a calendar year or used to redeem more than €1000 to the e-money holder in that same calendar year.

9.21 Law enforcement are unable to seize many e-money products using POCA cash seizure powers because they do not fall within the definition of cash in POCA.

Risks

9.22 It is thought that criminals are using e-money products to launder the proceeds of crime. However the intelligence is low-grade and needs to be further complemented. A number of vulnerabilities stem from theoretical issues, where solid evidence on the domestic issues is a gap but concerns have been highlighted at the EU and international level.

9.23 On the basis of this analysis of the threats and vulnerabilities, the government considers the money laundering risk posed by e-money products to be **medium**.

Digital currencies

9.24 Digital currencies (sometimes referred to as virtual currencies) are defined by the FATF as "a digital representation of value that can be traded on the Internet and functions as (1) a medium of exchange; (2) a unit of account; and/or (3) a store of value, but does not have legal tender status in any jurisdiction".

9.25 Digital currency is distinguished from fiat currency. Fiat currency is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. Digital currency is also distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency—i.e. it electronically transfers value that has legal tender status.

9.26 There are two types of digital currency – centralised and decentralised. The most widely used centralised and decentralised digital currencies can be exchanged for fiat currencies at varying rates of commission through the services of specialist third party exchangers.

9.27 Widespread use of digital currencies is currently limited. This is due to a number of factors such as familiarity and lack of understanding by the general public and limitations on exchange and conversion methods. Digital currencies providers and digital currency exchanges are not subject to the regulations.

9.28 The threats and vulnerabilities from digital currencies (particularly Bitcoin) are:

- criminals are using digital currencies to move criminal proceeds, predominately in the sale and purchase of controlled substances and firearms
- limited understanding of the use of digital currencies for money laundering

Criminal use of digital currencies

9.29 The money laundering risk associated with digital currencies is **low**, though if the use of digital currencies was to become more prevalent in the UK this risk could rise. Digital currencies are currently not a method by which terrorists raise or move money out of the UK (though they remain a viable method for doing so). Intelligence drawn from a limited number of recent cases indicates there is criminal use of digital currencies predominantly on the online market-place for the sale and purchase of illicit goods and services.

9.30 Digital currencies are the preferred method of online payment for illicit commodities including firearms and drugs. The majority of dark web websites have payment systems reliant

on digital currencies because of the perceived anonymity of these types of payment product. Current criminal exploitation of Bitcoin can be divided into two distinct areas: internally against the Bitcoin platform and users themselves, for example theft or fraud; and externally by exploiting the system as a means of exchange, for example money laundering, terrorist financing or the purchase of criminal commodities.

9.31 There are a limited number of case studies upon which any solid conclusions could be drawn that digital currencies are used for money laundering. There are concerns around anonymity, faster payments, and ability to provide cross border remittances and facilitate international trade. These issues are similar to issues identified with many other financial instruments, such as cash and e-money.

9.32 The use of digital currency online by an online criminal almost eliminates the need for complex layering methods for international money laundering. Using this process a criminal can effectively launder proceeds of crime and transfer it internationally without any interface with the regulated sector and often without any suspicious activity being reported to the NCA, although there have been SARs generated at the point of conversation back into fiat currency either by a bank receiving a transaction from an exchanger or from the exchanger themselves.

9.33 Law enforcement agencies have identified a common methodology whereby criminals are moving the proceeds of crime through a variety of channels and then onto a combination of new payment products in order to disguise and move criminally derived funds. Law enforcement agencies have identified, in a limited number of cases, criminals using large franchised MSBs to purchase digital currencies from exchangers. This method, law enforcement agencies believe, has been developed to avoid the retail banking sector.

9.34 Law enforcement currently assess this threat to be principally related to cyber criminals. There is little evidence to indicate that the use of digital currencies has been incorporated into established money laundering techniques (such as trade-based money laundering), through which 'traditional' (non-cyber) criminals and money laundering specialists working on behalf of 'traditional' crime groups currently launder illicit funds.

9.35 There is little evidence to indicate that the use of digital currencies has been adopted by criminals involved in terrorist financing, whether as a means by which to raise funds (crowd funding etc.), to pay for infrastructure (e.g. server rental), or to transfer funds.

Law enforcement activity

An NCA assessment has provided a baseline for law enforcement on the threat posed by the criminal use of digital currencies. An improved intelligence picture will be the basis for operational targeting, and is also being fed into policy makers to inform decision making about government intervention. Capacity building work includes awareness raising with industry and police forces. In addition, much of this activity is being mirrored at the international level, which is important given the cross border nature of the problem.

Call for information

9.36 In August 2014, the government announced a major programme of work on digital currencies, looking into the potential benefits and risks and whether government intervention is required. In November 2014, the government published a call for information to gather views and evidence on these questions.

9.37 In March 2015, the government published its response to the call for information, noting that while digital currencies represented an interesting development in payments technology, the market in which digital currency firms are operating was not functioning as well as it could. The government concluded that there was a strong case for introducing anti-money laundering regulation in order to provide a supportive environment for legitimate digital currency users and businesses, and to create a hostile environment for illicit users of digital currencies. The government said it would formally consult on this proposal in the new Parliament.

10 International exposure

10.1 The UK faces both direct and indirect money laundering threats in the international sphere. The UK is exposed to money laundering threats from other countries, as foreign criminals seek to transfer criminal proceeds into or through the UK, or seek to use UK professional services to facilitate the laundering of the proceeds of crime within and between other countries. UK businesses that operate internationally are also exposed to money laundering threats in the countries in which they operate. The UK is also exposed to the transfer of UK criminal proceeds to other countries, either to frustrate efforts to confiscate assets, as part of 'lifestyle' spending, or to pay for goods and services overseas in support of further criminality (for example, the purchase of drugs overseas for supply to the UK).

10.2 The UK's Serious and Organised Crime Strategy commits the UK to taking steps to improve our capability to recover UK criminal assets from overseas, and to intensify international collaboration.[1] These measures including drawing on wider resources more effectively to disrupt global organised crime, and negotiating asset-sharing agreements with other countries to encourage them to enforce UK orders.

Exposure of the UK to international money laundering threats

10.3 Criminals from other countries seek to launder their criminal proceeds into or through the UK. They are also known to use the UK professional services to launder money within or between other countries, even in cases where the criminal proceeds do not enter the UK itself.

10.4 The UK's status as a global financial centre makes it vulnerable to money laundering threats from other countries. The UK is the world's leading exporter of financial services with a trade surplus of $71 billion in 2013.[2] The UK accounted for 41% of global foreign exchange trading in April 2013, well ahead of the USA, Japan and Singapore. The UK is the single most internationally focused financial marketplace in the world.

10.5 The same factors that make the UK an attractive place for legitimate financial flows can make it attractive for money laundering: its language and central geographical location between the US and Asian time zones; the concentration of financial institutions (London has more foreign banks than any other financial centre); and a consistent, politically neutral legal system that is widely used and understood globally.

10.6 The true scale and origin of criminal proceeds placed in or moved through the UK is an intelligence gap. Some non-governmental organisations estimate that between £23-57 billion is laundered within and through the UK each year. The NCA assesses that hundreds of billions of dollars are laundered through UK banks and their subsidiaries each year.

10.7 International corruption cases involving millions of pounds of assets in the UK are currently under investigation, with alleged predicate offending in Africa, the Middle East and Eastern Europe, and involving financial flows that span the globe. The scale of the laundering of criminal proceeds, despite the UK's leading role in developing international standards to tackle it, is a strategic threat to the UK's economy and reputation. Some of the same financial transfer systems used by serious and organised criminals in the UK are also used by terrorist groups both domestically and overseas.

[1] 'Serious and Organised Crime Strategy', HM government, October 2013.

[2] 'Key facts about the UK as an international financial centre', CityUK, June 2014.

10.8 UK businesses increasingly operate overseas, to the benefit of both the UK and the countries we trade with. However, this can result in an increased exposure to money laundering risk as UK businesses enter countries that have less stringent rules around trade, weak regulation and ineffective law enforcement response to money laundering, or suffer from significant levels of corruption. The list of countries identified by the private sector in their questionnaire returns for this NRA as posing a high risk for money laundering was extensive. Whilst a core list of countries of high risk was identified in many returns, and closely correlates with those jurisdictions that UK law enforcement agencies identify as high risk, most firms face their own unique combination of risks, determined by the countries in which they choose to operate.

10.9 Although the UK has powerful legislation in place to trace and recover the proceeds of crime, and effective law enforcement and prosecution agencies, it is clear that we need to improve our multilateral efforts, working more closely with other countries in which illicit assets have been placed.

Recovering UK criminal assets laundered overseas

10.10 British criminals often transfer the proceeds of their crimes to other countries. In the last 5 years criminal assets with an estimated value of over £600 million have been identified overseas.[3] The true figure will be significantly higher, as this figure only includes identified assets linked to offenders who have been convicted and had a confiscation order made against them. It does not take account of any assets linked to offenders who have escaped detection or conviction. Table 10.A shows the top ten countries in which UK criminal assets have been identified, ranked by estimated value over the period 2010/11 – 2014/15.

10.11 The UK is working with partners, both domestically and internationally to make it even harder for criminals to move, hide and use the proceeds of crime. This includes increased collaboration on international asset recovery agreements. The UK has reached an agreement with Spain to facilitate the recovery of assets and make Spain a more hostile place for UK criminals. The Home Office has negotiated asset-sharing agreements with other countries, including China and the United Arab Emirates, to encourage them to enforce UK orders and hopes to agree more in the future.

Table 10.A: Top 10 countries to which identified UK criminal assets were laundered, ranked by estimated value, 2010/11-2014/15

Rank	Country
1	United Arab Emirates
2	Pakistan
3	Switzerland
4	Spain
5	Liechtenstein
6	Hong Kong
7	Cyprus
8	British Virgin Islands
9	Isle of Man
10	Nigeria
Source: Joint Asset Recovery Database (JARD) data, as at May 2015	

[3] Data from the Joint Asset Recovery Databased (JARD), 2010/11 – 2014/15, as at May 2015.

10.12 UK investigators and prosecutors face difficulties in identifying, freezing and recovering laundered criminal proceeds from other countries for a number of reasons.

10.13 In many jurisdictions, the concept of asset recovery is still relatively new. Different legal systems can create obstacles as the way investigations are carried out are technically and procedurally different. What can or cannot be identified, investigated and then recovered under differing laws varies. For example, often in other jurisdictions a direct link between a criminal act and the actual asset must be proved for it to become accessible, meaning vast sums of potentially illicit finance that would be recoverable in the UK are beyond reach elsewhere. A lack of strong governance, weak regulations, an absence of the rule of law, lack of financial investigation legislation or capacity, a lack of genuine partnership working in certain countries all provide additional challenges.

10.14 Since the publication of the Serious and Organised Crime Strategy in 2013, the UK has taken significant steps to improve its capacity to recover assets overseas by working with international partners to improve and develop the international operating environment for the recovery of illicit assets in priority jurisdictions. Four prosecutors have been posted overseas as dedicated Asset Recovery Advisors (ARAs) to work with the authorities in key jurisdictions to strengthen collaboration and further the UK's ability to recover criminal proceeds. Since the first ARAs were posted to the UAE and Spain in 2014, £300,000 has been recovered from the UAE – the first time UK criminal assets have been recovered from that country – and over £1 million has been confiscated in Spain. The other two ARAs are responsible for Europe and the Caribbean.

10.15 In December 2014 the UK implemented EU measures (the Criminal Justice and Data Protection Regulations 2014) to enable the mutual recognition of freezing and confiscation orders made by the courts in EU member states. This should enable faster and more effective cooperation on the recovery of proceeds of crime, as the measures significantly reduce the grounds on which requested states can refuse to cooperate, set short time limits for orders to be brought before the courts, and incorporate an asset-sharing agreement in all cases with a value of €10,000 or more.

10.16 The Mutual Legal Assistance (MLA) system is time consuming and complex but provides an essential function for the recovery of UK criminal proceeds laundered overseas. The number of MLA requests made to the countries that hold the highest value of criminal funds has not always been commensurate with the scale of the threat, this reflects the practical difficulties faced by prosecutors and investigators in bringing often very different legal systems together to recover funds. The new Proceeds of Crime Unit in the Crown Prosecution Service, coupled with NCA-led multi-agency work to enforce confiscation orders, and the deployment of ARAs, has already led to increases in the requests made, most notably in respect of Spain.

10.17 Civil recovery work is inherently international, as the assets pursued are often held overseas. The enforcement of civil recovery orders outside the UK remains subject to the law of the jurisdiction where the assets are located. This presents difficulties when it comes to realising such property without the co-operation of the respondent to the proceedings. However, in recent times significant inroads have been made in civil code countries such as Luxembourg and Spain where assets can now be frozen and, in the case of Spain, assets can now be recovered following work with the CPS Liaison Magistrate and the Spanish Authorities. NCA is seeking to progress mutual legal assistance in so far as it relates to civil recovery with a number of EU states

11 Terrorist financing

11.1 It is noted that there is a marked overlap between money laundering and terrorist financing – both criminals and terrorists use similar methods to raise, store and move funds. Many of the vulnerabilities set out in earlier sections leave sectors open to abuse not only by money launderers, but also terrorist financers. However, the motive for generating funds differ. Terrorists ultimately want to make, move and use money to commit terrorist acts and unlike criminal gangs, disparate individuals come together through a shared motivation and ideology.

11.2 The greatest threat to the UK is assessed to be from Al Qaida (AQ) Core, AQ Arab Peninsula (AQAP), AQ Islamic Maghreb (AQIM), Islamic State of Iraq and the Levant (ISIL), Al –Nusrah Front (ANF) and those affiliated to these groups. Terrorist attacks in the UK have required minimal finance, however a lack of funds can have a direct effect on the ability of terrorist organisations and individuals to operate and to mount attacks. Terrorists may use any means at their disposal to raise, store and move funds and this can be through use of legitimate means, self-funding, fraud, or other proceeds of crime.

11.3 The UK recognises that countering terrorist finance is important in protecting national security. Countering terrorist finance forms a key part of the UK's CONTEST counter-terrorism strategy, with the aim being to reduce the terrorist threat to the UK and its interests overseas by depriving terrorists and violent extremists of the financial resources and systems required for terrorism-related activity.[1]

11.4 The UK's approach to countering terrorist finance focuses on three main areas: reducing terrorist fundraising in the UK; reducing the movement of terrorist finance into/out of the UK; and reducing the fundraising and movement of terrorist finance overseas.

Terrorist finance legislation

Terrorism Act 2000

11.5 The legal definition of terrorist property is contained in the Terrorism Act 2000 (TACT) section 14. 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.

11.6 Specific offences under Sections 15-18 of TACT, whether committed in the UK or overseas include:

- inviting, providing, or receiving money or other property with the intention or reasonable suspicion that it will be used for the purposes of terrorism
- using or intending to use money or other property for the purposes of terrorism
- being involved in an arrangement which makes money or other property available for the purposes of terrorism

[1] 'CONTEST: The United Kingdom's Strategy for Countering Terrorism', HM government, July 2011

- being involved in an arrangement which facilitates the retention or control of terrorist property by concealment; removal from the jurisdiction; transfer to nominees, or in any other way

Convictions

11.7 There have been 17 convictions under sections 15-18 of TACT between September 2001 and June 2014. However, this is not indicative of the total number of terrorist financing instances that have been disrupted. In cases involving offences which may attract more severe penalties, such as murder, the Crown Prosecution Service may opt to pursue these charges rather than those related to terrorist financing. In addition, non-terrorism legislation can also be used to disrupt terrorist financing activity.

Terrorist Asset-Freezing Act 2010

11.8 The UK terrorist asset freezing regime meets obligations placed on the UK by Resolutions of the UN Security Council (UNSCRs) and associated EC regulations. It is implemented by the Terrorist Asset-Freezing Act 2010 (TAFA 2010).

11.9 There is a two part test to exercise the power to designate a person under TAFA found at Section 2 of the Act: in essence, there must be evidence to support a reasonable belief that the person has been involved in terrorist activity (s.2(1)(a) TAFA) and the asset freeze must be considered necessary for purposes connected with protecting members of the public from terrorism (s.2(1)(b) TAFA).

11.10 Designation under TAFA subjects a person to the following restrictions:

- a prohibition on dealing with any funds or economic resources owned, held or controlled by the designated person (in effect the funds or economic resources must be frozen)
- a prohibition on making funds, economic resources or financial services available to (or for the benefit of) the designated person

11.11 Specific offences under TAFA include:

- dealing with funds or economic resources owned, held or controlled by a designated person
- making funds, economic resources or financial services available to or for the benefit of a designated person
- circumventing the restrictions imposed by those restrictions

11.12 As well as the requirement that both parts of the statutory test are met before a designation can be made, various other safeguards are built into the asset freezing regime to ensure that it is operated fairly and proportionately:

11.13 The Treasury may grant licences to allow exceptions to the freeze for certain payments or categories of payments;

- designations expire after a year unless reviewed and renewed
- a right of appeal against designation decisions (for the designated person) and a right to challenge on judicial review grounds any other decision, for example, licensing decisions for the designated person or anyone else affected by the

decision to the High Court (using specially cleared advocates to protect closed material where necessary whilst ensuring a fair hearing for the applicant)

- individuals are notified, as far as possible, of the reasons for their designation
- the operation of the regime is subject to an independent review by the Independent Reviewer of Terrorism Legislation
- a requirement that the Treasury report to Parliament every quarter on the exercise of its powers under TAFA during that period

Implementation of UNSCRs 'without delay'

11.14 FATF sets international standards, in the form of recommendations, for combatting money laundering and terrorist financing. Recommendation 6 requires freezing 'without delay' of the assets of individuals or entities designated under UNSCRs 1267 and 1373, whilst Recommendation 7 requires freezing 'without delay' of the assets of those listed by the UN under the non-proliferation regimes. 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.

11.15 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 the TAFA 2010 and EU Common Position 931 and Regulation 2580/2001. The assets of individuals designated under UNSCR 1373 in the UK are frozen without delay.

11.16 UNSCR 1267 created a regime that targets individuals and entities associated with Al Qaida requiring states to freeze the assets of persons designated under that regime. The UK implements UN asset freezes by way of EU Regulation which takes direct effect in the UK. It takes three to four weeks on average for the EU to implement UN listings resulting in a delay between the adoption of designations at the UN and their implementation and a possible risk of asset flight.

11.17 The UK continues to actively raise the risks presented by the delay with the European Commission, and is also currently considering legislative options to address the delay between UN terrorism sanctions being imposed and their implementation by the EU.

11.18 On 31 December 2014, £117,000 was frozen across 80 accounts of those designated under the UK's domestic TAFA regime, the UN AQ regime and the EU CP931 regime.

Al Qaida (Asset Freezing) Regulations 2011

11.19 The Al Qaida (Asset Freezing) Regulations 2011 impose the criminal penalties for breaching the UN Al Qaida asset freezing regime that is given effect by EC Regulation 881/2002. This may include circumventing or assisting someone to circumvent their asset freeze, or providing false information for the purpose of obtaining a licence from HM Treasury.

UK law enforcement

11.20 The Home Office is responsible for counter-terrorist finance policy with key government departments and operational partners critical in undertaking activity to disrupt key terrorist finance threats and risks.

11.21 UK Intelligence agencies are responsible for monitoring and assessing the terrorist financing threats to the UK and its interests overseas, and are supported by the National Terrorist Financial Investigation Unit (NTFIU). The NTFIU, part of the Metropolitan Police Service (MPS) Counter Terrorism Command, has the strategic police lead for countering terrorist financing in the UK. It will lead 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) located in England, Scotland and Northern Ireland. Each CTU is responsible for investigating instances of terrorist financing occurring within their geographical regions and for supporting mainstream counter terrorism investigations with financial intelligence support.

11.22 The UK's Financial Intelligence Unit is hosted by the National Crime Agency (NCA) and sits at the heart of the SARs regime, providing information relating to the detection and investigation of terrorist finance. The NCA's Terrorist Finance Team identifies, assesses and exploits SARs submitted under both TACT and POCA. Due to the additional sensitivity arising from potential links to national security, SARs submitted under TACT, or those submitted under POCA which are identified as having a CFT link, are not routinely made available for other end users.

11.23 In relation to terrorist asset-freezing, proposals for designation under TAFA are made to the Treasury by the police and the Security Service, or by other government departments or international governments where there is evidence to support a reasonable belief that an individual or entity is or has been involved in terrorism and that it is necessary for reasons connected to protecting the public from terrorism for restrictions to be imposed. The investigation of breaches are conducted by the relevant CTU, with engagement from government departments including the Treasury and the Crown Prosecution Service.

Regulated sector

Banking

11.24 Within the banking sector, it is assessed that the terrorist financing risks are medium. Intelligence suggests that terrorists use the formal banking system to move funds to a lesser extent than other means of moving money (for example, cash couriering). However, it is clear that there is a risk terrorists will use the banking system to raise, store and move money for the purposes of terrorism.

11.25 Key threats within the banking sector are:

- use of fraudulent identities and supporting documentation to open and run bank accounts
- complicit employees facilitating fraud and terrorist financing
- fraudulent bank loan applications

11.26 Intelligence suggests terrorists have used fraudulent identities to open bank accounts and corrupt bank employees have facilitated fraudulent loan applications. In one case, a number of fraudulent loan applications were made, with one single application totalling £15,000. The use of the banking sector by terrorists remains a threat, in particular in the context of Syria. Individuals can use cash machines/ATMs to withdraw funds in neighbouring countries where there is a formal banking sector and then carry funds into Syria. This is a significant issue given

the threat posed by foreign fighters travelling to Syria to engage in fighting and returning to their country of citizenship/residence.

11.27 SARs submitted under TACT are different in purpose and effect to SARs submitted under POCA. It is not always reasonable to expect a reporter to be able to identify a terrorist association with suspicious activity, when that association is only visible through sensitive government and law enforcement databases. As a result, TACT SARs represent a small proportion of all SARs submitted, but all SARs are considered for terrorist finance associations. It is important for all reporters to identify and articulate their suspicions accurately, to enable any likely terrorist finance associations to be properly assessed in the light of other information.

11.28 SARs from the banking sector can be variable in quality. The determining factor appears to be the source of suspicion; where suspicion is generated following enquiries by law enforcement, the quality is good. In other cases, the quality of suspicion may be tenuous, based on associations with organisations proscribed by other jurisdictions or on text descriptions of transactions. Better awareness within banks, and other reporters, of how associations are made between reported suspicions and terrorist finance may help them maintain better consistency in their reporting.

Money service businesses

1.1 Terrorist financing risks within the money service business (MSB) sector are assessed to be high. Intelligence indicates that MSBs are used to move terrorist financing out of the UK, with some of the funds moving on to countries who do not have a formal banking structure. To some extent, MSBs offer a degree of anonymity for remitters and recipients given funds under the €1000 threshold (in accordance with the EU Wire Transfer Regulations[2]) require the remitter to provide minimal identity documents. Although HMRC, the supervisor of this sector under the Money Laundering Regulations 2007, advises MSBs that they should carry out customer due diligence on all transactions, there is a risk that individuals can send funds below the threshold on a frequent basis using a variety of MSBs.

11.29 Key threats within the MSB sector are:

- complicit employees involved in remitting funds destined for terrorists
- terrorist exploitation of the ability to remit funds under €1000 without providing identification
- low reporting from the sector in relation to terrorist finance

11.30 Most recently, police investigations have shown that MSBs are being used to send funds to Turkey and Egypt, eventually reaching foreign fighters in Syria. Funds are typically broken down into smaller amounts to avoid the need to provide identification and to avoid detection. Intelligence also indicates that employees have been known to facilitate funds to terrorists through their position within MSBs.

11.31 Between 1 October 2001 and 31 September 2013, 16 SARs under the Terrorism Act 2000 were received from the MSB sector. Reporters in decentralised and diverse businesses like MSBs can find it difficult to consistently identify terrorist finance risks to their business. These difficulties may relate to staff turnover, to different customer relationships and different business

[2] Regulation (EC) No 1781/2006 on information on the payer accompanying transfers of funds.

models, or a mixture of all the above, but the overall effect is that abuse of the MSB sector funds could be a key enabler in the movement of terrorist financing.

11.32 The withdrawal of banking services from parts of the MSB sector is perhaps the most advanced and high-profile manifestation of de-risking that we have witnessed in the UK. Whilst the terrorist financing risks within the MSB sector are assessed as high, it is worth noting that there are a number of developing countries, most notably Somalia and Afghanistan, which rely heavily on remittances from the UK and elsewhere largely due to their weak or non-existent formal banking systems. De-risking is having a particularly acute impact on Somalia given the vital importance of remittances to its economic development, the opaque nature of the money transfer process which relies on Hawala (trust-based system) and banks' concerns that the funds could end up in the hands of Al-Shabaab, a designated terrorist organisation. If MSBs are unable to access banking services from UK banks, money remitters will become increasingly reliant on cash, which may increase the terrorist financing risk within the sector.

Charities/non-profit organisations (NPOs)

11.33 Although proven terrorist abuse of the charitable sector is rare, it is assessed that the terrorist financing risks within the charitable sector are medium-high. Terrorists and charities operate in conflict areas and therefore, determining the end destination of funds can be difficult.

11.34 Key threats within the charitable sector are:

- raising funds from the public under the guise of a charity with or without a charity licence or authority
- trustee abuse of charities to divert funds for terrorist financing
- looting of charity assets by terrorists in high-risk jurisdictions
- diversion of charitable goods at the destination by terrorists
- charities being subject to local extortion by terrorists in de facto control

11.35 Two high profile convictions have highlighted that individuals can use the name of a charity to raise funds for terrorist purposes:

11.36 Case 1: on 2 August 2012, Mohammed and Shafiq Ali were convicted of raising money to fund terrorism and were sentenced to three years imprisonment. The brothers carried out street collections supposedly for charity. They pleaded guilty to raising £3,000 which they sent to a family member in Somalia for terrorist training and fighting.

11.37 Case 2: on 21 February 2013, Ashik Ali, Ifran Khalid and Ifran Naseer were convicted of committing acts in preparation for terrorist attacks, included collecting money for terrorism. They raised funds by fraudulently presenting themselves as charity fundraisers using high visibility vests and collections buckets bearing the name of the charity Muslim Aid. Of the approximately £14,000 raised, only £1,500 reached the charity. A genuine Muslim Aid volunteer, Rahin Ahmed, was found guilty of assisting with the plot.

11.38 These cases highlight that charities can be vulnerable to abuse and underlines the need for charities to have appropriate processes in place to safeguard against terrorist abuse. A key vulnerability is the lack of visibility of the end use of charitable funds once they are sent out of the UK. In 2014, the Charity Commission publicly announced the opening of 3 statutory inquiries into charities where there are regulatory concerns as to whether or not the funds applied overseas can be evidenced by the trustees in accordance with their charity law duties.

The charities are Aid Convoy, Children in Deen and Al Fatiha Global. All of these charities operate in Syria and/or neighbouring areas.

11.39 The Independent Reviewer of Terrorism Legislation, David Anderson, has been concerned about the difficulties created by terrorist finance legislation for the provision of humanitarian aid especially in areas under de facto control of terrorist groups since his visit to Israel and the Occupied Palestinian Territories in November 2013. Following a recommendation by David Anderson in his July 2014 report, dialogue has been initiated between NGOs and policy makers to explore how NGOs can carry out their legitimate activities without being impeded by terrorism legislation including offences that relate to terrorist financing.[3]

11.40 Although we understand that NGOs operating overseas in high-risk jurisdictions may come into contact with proscribed terrorist organisations, it is an offence under the Terrorism Act 2000 if any funds or resources are made available to such a group. However, like banks, NGOs are responsible under charity law for ensuring that they conduct due diligence checks and are satisfied with the end use of funds.

11.41 Withdrawal of banking services ('de-risking') has been of particular concern to the charity sector, where banking services are essential for charities to be able to operate safely, effectively and transparently. If charities are unable to access banking services, charitable funds may go underground, increasingly transacted in cash, or moved off-shore via cash couriers or alternative remittance systems. Such activities would make it increasingly difficult for HMG to address and manage the risk of abuse of charities for terrorist financing.

Prepaid cards

11.42 It is assessed that the terrorist financing risk associated with prepaid cards is low. Although the use of pre-paid cards has not been widely used by terrorists to store and move funds, operational partners are aware of a case where terrorists have used multiple pre-paid cards to move money out of the UK, with the intention for use in Syria. There is a risk that pre-paid cards may increasingly feature as a means to move money in terrorist financing investigations.

Unregulated sectors

Cash couriering

11.43 It is assessed that the terrorist financing risks with associated with cash couriering are high. Cash couriering is the favoured method of taking terrorist funds out of the UK given it is a tried and tested method and recipient countries are usually cash-based economies. Cash couriered out of the UK can be couriered by multiple individuals and is smuggled where borders surrounding destination countries are porous. The UK continues to see cash couriering activity in relation to foreign fighters travelling to Syria. The high profile conviction of Amal El-Wahabi[4] in 2014 demonstrates the need for cash and the amounts that can be involved.

Digital currencies

11.44 Although digital currencies are currently not a method by which terrorists seem to raise or move money out of the UK, they remain a viable method for storing and using funds. There is a risk that digital currencies could be used for terrorist purposes given the opportunity they

[3] 'The Terrorism Acts in 2013 – Report of the Independent Reviewer on the Operation of the Terrorism Act 2000 and Part 1 of the Terrorism Act 2006', David Anderson Q.C., Independent Reviewer of Terrorism Legislation, July 2014

[4] Amal El-Wahabi was convicted in 2014 for coercing a friend to carry 20,000 Euros (£15,800) to Turkey in an attempt to fund her husband's jihad for ISIL in Syria.

provide to move funds internationally with a degree of anonymity. Given digital currencies are currently unregulated, oversight and knowledge of their use is limited.

Mobile payment systems

11.45 Mobile payment systems enable secure payments to be made without the disclosure of a bank account number or sort code and this poses a difficulty for financial investigators in the identification of payments. Although mobile payment systems are regulated under the Money Laundering Regulations, the uses of financial mobile telephone applications to transfer money are an emerging issue for operational partners seeking to disrupt terrorist finance.

International exposure

11.46 The UK is a net exporter of terrorist finance and the risk of money flowing into the UK for terrorist purposes is comparatively lower. Funds raised in the UK for terrorist purposes are assessed to be in the millions of pounds per year, with a proportion eventually leaving the UK. Much of the UK's work has focused on stopping funds entering into end use countries. Common vulnerabilities exist with priority countries that surround end use countries (countries where terrorists operate). Porous and unmanned borders allow for the easy movement of funds and goods into end use countries and a lack of or a weak counter-terrorist finance regime means that instances of terrorist financing or not identified, investigated and disrupted.

End use countries

Syria

11.47 The terrorist threat posed by terrorist groups operating in Syria and returning foreign fighters poses a significant threat to the UK. ISIL largely derives funds from the territory it controls through taxation/extortion activities in Syria and Iraq and the sale of oil. ISIL has also received funds through ransoms (an estimated US$35-45 million between September 2013 – September 2014), private donations and the sale of cultural assets. UK funding of terrorist groups and foreign fighters in the Syria context is very low compared to the main ISIL funding streams. There is evidence of abuse of the UK charitable sector, student loans, money service businesses and cash couriering to move funds out of the UK. UK nationals have also raised and moved funds using these methods to enable them to travel and engage in fighting in Syria and Iraq.

Somalia

11.48 Somalia remains a key country of counter-terrorism concern, while Al-Shabaab have lost control of most towns and cities, including Mogadishu (the main destinations for remittances from the UK to Somalia), they do continue to operate in large swathes of the country. There is evidence of money being raised in the UK and moved out to Somalia, as highlighted by the convictions of Mohammed and Shafiq Ali in August 2012 (detailed above).

Transit countries/regions

Turkey

11.49 Turkey is a key hub for the flow of funds to Syria for terrorist use. Intelligence suggests that cash has been withdrawn from ATMs on the border of Turkey and Syria by foreign fighters engaged in fighting in Syria. Turkey does not control the full length of its land border and there are plentiful routes for smuggling goods and people into Syria. The movement of oil from ISIL

controlled areas through a network of middle-men, and the risk of it moving through Turkey, is also of concern.

East Africa

11.50 Given the threat posed by Al-Shabaab, countries surrounding Somalia, for example Kenya and Ethiopia, are key countries in relation to funds entering Somalia and reaching Al-Shabaab. The ongoing conflicts in many border regions of Somalia enables funds to be moved into the country without detection.

Gulf

11.51 Private donations originating from the Gulf are a vital funding stream for AQ and AQ affiliated groups. There is evidence that recently some funding via donations has been diverted from Afghanistan and Pakistan to terrorist groups operating in Syria. Donors can use networks of facilitators and fundraisers in the Gulf to collect and move funds out to terrorist groups.

A Full list of AML/CFT supervisors

A.1 This is a full list of bodies currently designated as AML/CFT supervisors under the Money Laundering Regulations 2007 (as amended):

Association of Accounting Technicians (AAT)

Association of Chartered Certified Accountants (ACCA)

Association of International Accountants (AIA)

Association of Taxation Technicians (ATT)

Chartered Institute of Management Accountants (CIMA)

Chartered Institute of Legal Executives (CILEX)

Chartered Institute of Taxation (CIOT)

Council for Licensed Conveyancers (CLC)

Department of Enterprise, Trade, and Investment Northern Ireland (DETNI)

Faculty of Advocates (Scottish Bar Association) (FoA)

Faculty Office of the Archbishop of Canterbury (AoC)

Financial Conduct Authority (FCA)

Gambling Commission (GC)

General Council of the Bar (England and Wales) (GCBEW)

General Council of the Bar of Northern Ireland (GCBNI)

HM Revenue & Customs (HMRC)

Insolvency Practitioners Association (IPA)

Insolvency Service (SoS)

Institute of Certified Bookkeepers (ICB)

Institute of Chartered Accountants in England and Wales (ICAEW)

Institute of Chartered Accountants in Ireland (ICAI)

Institute of Chartered Accountants of Scotland (ICAS)

Institute of Financial Accountants (IFA)

International Association of Book-keepers (IAB)

Law Society of England and Wales (LSEW)

Law Society of Northern Ireland (LSNI)

Law Society of Scotland (LSS)

B Glossary

AML/CFT – anti-money laundering and counter financing of terrorism

CDD – customer due diligence

EDD – enhanced due diligence

SDD – simplified due diligence

FATF – Financial Action Task Force

JARD – Joint Asset Recovery Database

JMLSG – Joint Money Laundering Steering Group

MLAC – Money Laundering Advisory Committee

HMRC – HM Revenue and Customs

FCA – Financial Conduct Authority

Business risk appetite – The level of risk that an organisation is prepared to accept, balancing the potential threats, costs and benefits of taking on a business relationship.

Client account – the bank account that a professional services firm uses for holding client money.

Closed loop e-money card – A payment card which can only be used at certain locations, for example a store gift card, or a pre-loaded card for use on a public transport system (such as an Oyster card).

Complicit professional enablers – Complicit, negligent or unwitting professionals in financial, legal and accountancy professionals that facilitate money laundering.

Consent SAR – The Proceeds of Crime Act allows persons and businesses to avail themselves of a defence against money laundering charges by seeking the consent of the authorities to conduct a transaction or undertake other activity about which they have concerns through the submission of a consent SAR to the UKFIU.

Criminal spend – The spending of the proceeds of a criminal lifestyle (on goods including property, cars, jewellery etc.).

Customer due diligence – taking steps to identify your customers and checking they are who they say they are, such as obtaining a customer's name; photograph on an official document which confirms their identity; and residential address or date of birth.

Electronic-money (e-money) – a digital equivalent of cash, stored on an electronic device or remotely at a server.

(UK) Financial Investigations Unit (FIU) – The UK Financial Intelligence Unit (UKFIU) is part of the National Crime Agency (NCA) and receives, analyses and distributes financial intelligence gathered from suspicious activity reports (SARs).

Fit and proper test – A test to ensure that those registering for supervision meet the requirements under the Money Laundering Regulations 2007.

Gambling Commission – The Gambling Commission was set up under the Gambling Act 2005 to regulate commercial gambling in Great Britain in partnership with licensing authorities. They

are an independent non departmental public body (NDPB) sponsored by the Department for Culture, Media and Sport (DCMS).

High-end money laundering – laundering which is conducted as a service, either wittingly or unwittingly, by the financial sector or related professional services. High-end money laundering is specialist, usually involves transactions of substantial value, and involves abuse of the financial sector and professional enablers.

High risk customer – customers that present a higher money-laundering risk might include, but are not restricted to customers linked to higher-risk countries or business sectors; or who have unnecessarily complex or opaque beneficial ownership structures; and transactions which are unusual, lack an obvious economic or lawful purpose, are complex or large or might lend themselves to anonymity.

High value dealer (HVD) – Any business which accepts cash payments of €15,000 or more (or equivalent in any currency) in single transaction, or linked payments for a single transaction, in exchange for goods.

Home/host state – Refers to the division of supervisory responsibilities of cross-border entities in the EU, which means that branches may be able to operate in a host country under the supervision of the home supervisor.

Jurisdictions of risk – A term describing the inherent risk of operating in a foreign jurisdiction, or when an investor is exposed to risk because of unexpected changes in laws affecting the investment. While some risk is always present, it is generally considered to be higher in countries suffering from, or designated as high-risk areas for money-laundering, terrorism financing and corruption.

Identity fraud – Refers to crime in which criminal obtains and uses a victim's personal data through fraud or deception and usually for economic gain.

International controllers – Professional money launderers, usually based overseas, who operate laundering networks across multiple jurisdictions.

Money Laundering Regulations 2007 ('the regulations') – The regulations place requirements on relevant persons in the regulated sector for the purpose of preventing and detecting money laundering and terrorist financing. http://www.legislation.gov.uk/uksi/2007/2157/contents/made

Nominee director – Person who acts as a non-executive director on the board of directors of a firm, on behalf of another person or firm such as an bank, investor, or lender.

Open loop e-money card – A pre-loaded payment card which is accepted and processed at any retailer which accepts the relevant payment system (e.g. Visa or MasterCard).

Passporting – Passporting rights allow firms to conduct business into the EEA under a single market directive. A UK firm that is entitled to carry on an activity in another EEA State may either establish a physical presence or provide freedom of services into another EEA State, subject to the fulfilment of the conditions under the relevant directive.

Politically exposed persons (PEPs) – A term describing someone who has been entrusted with a prominent public function in a state other than the UK in the preceding year, or a relative or known associate of that person. A PEP generally presents a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold.

Predicate offence – The criminal offence that has occurred in order to generate the criminal property which is being laundered.

Proceeds of Crime Act 2002 (POCA) – contains the single set of money laundering offences applicable throughout the UK to the proceeds of all crimes. It provides the framework for asset recovery in the UK, as well as a number of investigative powers to enable law enforcement agencies to investigate money laundering and develop cases to recover the proceeds of crime. http://www.legislation.gov.uk/ukpga/2002/29

'Bank Quick Drop' – A service offered by some banks to businesses, which allows the business to drop off cash at either the bank directly or at a third party facility where the money is counted and then transferred to the bank to be deposited.

Regulated sector – individuals and firms subject to requirements under the Money Laundering Regulations 2007, including credit institutions, financial institutions, auditors, insolvency practitioners, external accountants and tax advisers, independent legal professionals, money service businesses, trust and company service providers, estate agents, high value dealers and casinos.

Reliance – Regulation 17 of the regulations allow that a regulated entity may rely on the customer due diligence measures carried out by another regulated entity, if the other entity consents to be relied on. Under such circumstances the regulated entity remains liable for any failure of the entity they are relying on to correctly apply CDD measures.

Remote Gambling – defined by the Gambling Act 2005 as gambling in which persons participate by the use of remote communication including: the internet, telephone, television, radio, and any other kind of electronic or other technology for facilitating communication.

Smurfing – When money launderers break up larger cash amounts which may attract attention/challenge if attempts are made to pass it through a supervised business. A simple example is for criminals to use multiple individuals to each pass smaller amounts, or for the same individual to pass smaller amounts at multiple businesses to avoid attention.

Suspicious activity report (SAR) – A report made to the NCA under the Proceeds of Crime Act 2002 or the Terrorism Act 2000 when a person knows or suspects that another person is engaged in money laundering or terrorist financing, or dealing in criminal property.

Trusts and companies service provider (TCSPs) – A trust or company service provider is any firm or sole practitioner that provides the following services by way of business:

- forming companies or other legal persons
- acting, or arranging for another person to act:

    (i) as a director or secretary of a company

    (ii) as a partner of a partnership

    (iii) in a similar position in relation to other legal persons
- providing a registered office, business address, correspondence or administrative address or other related services for a company, partnership or any other legal person or arrangement
- acting, or arranging for another person to act as either a trustee or an express trust or similar legal arrangement or a nominee shareholder for a person other than a company whose securities are listed on a regulated market

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

Email: public.enquiries@hmtreasury.gsi.gov.uk