HM Treasury

Home Office

National risk assessment of money laundering and terrorist financing 2020

December 2020

HM Treasury

Home Office

National risk assessment of money laundering and terrorist financing 2020

Presented to Parliament pursuant to Regulation 16 of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

December 2020

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

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

ISBN 978-1-5286-2321-6

CCS1220688488 12/20

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the APS Group on behalf of the Controller of Her Majesty's Stationery Office

Contents

Foreword

Our status as a global financial centre, our openness to trade and investment, and the ease of doing business here in the UK are all vital for our prosperity. However, these remarkable strengths also make us vulnerable to a wide range of economic crime and to those who wish to do us harm.

Serious and organised crime undermines the legitimacy and authority of the state and its institutions, threatens the safety of British citizens and communities, and is a fundamental threat to the country's future security, resilience and prosperity**.** It is estimated to cost the UK economy £37 billion per year. Motivated and fuelled by illicit funds, it continues to have a detrimental impact on our public services, businesses and individuals on a daily basis. The scale of the threat is becoming more complex, as criminals adapt to our response and exploit advances in technology to hide themselves in plain sight. This threat extends to terrorist financing as well, where we must continue to bear down on the possibility for terrorists to support dangerous organisations or to use funds in support of harmful attacks.

These threats have only become more salient, as COVID-19 presents new opportunities for criminals wanting to exploit the most vulnerable in our society. Stepping up our response will be critical to increasing resilience, protecting economic security and safeguarding our recovery following the pandemic.

The UK's third National Risk Assessment builds on the UK's strong understanding of these threats and provides the foundation for the government and private sector to meet this challenge, evaluating the actions certain sectors must take to protect individuals, businesses and society in order to stay resilient. It is a vital component of our commitment to combat economic crime and protect the security and prosperity of the UK. This assessment forms a critical evidence base for our response to money laundering and terrorist financing in the coming years.

The UK is at the forefront of tackling money laundering and terrorist financing globally; in 2018 the UK achieved the best rating of any country assessed so far in this round of the FATF evaluations But we know we must go further and faster in strengthening our response.

That's why in July 2019, the Home Office, HM Treasury and UK Finance, in collaboration with other public and private stakeholders published the Economic Crime Plan , setting out the UK's 7 strategic priority areas to further combat economic crime. This reinforces our increasingly strong partnership with the private sector, which has been cemented through the establishment of new public private governance. By taking an ambitious approach to tackling dirty money, grounded in prevention, education, effective enforcement and regulatory reforms, we will close-off systemic vulnerabilities to money laundering.

Since the 2017 National Risk Assessment, and in response to changing threats and the latest international standards, we have already brought additional sectors into

scope of the anti-money laundering and counter-terrorist financing regulations to ensure we are adapting to new criminal methodologies. We have strengthened the policing response to economic crime through the launch of the National Economic Crime Centre and will continue to build capacity to spot, investigate and seize the assets of criminals and money launderers. To achieve this, we are significantly increasing the number of dedicated financial investigators in law enforcement, consulting on the introduction of a sustainable resourcing model to tackle economic crime and considering how to remove barriers to information sharing, by ensuring we have the right legislation in place. We are committed to improving the quality of supervision of the regulated sectors, through the Office of Professional Body Anti-Money Laundering Supervisors. The Suspicious Activity Report Reform Programme began in July 2018, and we are taking further important steps to reform Companies House, Limited Partnerships and Trust registration to prevent criminals from laundering their ill-gotten gains through concealing their identity behind opaque corporate structures.

It is only through our collaborative efforts that we will ensure the UK remains a hostile location for illicit finance activity, protect our society and uphold the integrity of our financial system.

Rt Hon James Brokenshire MP
Minister for Security

John Glen MP
Economic Secretary to the Treasury

Executive summary

Since 2017, the UK's anti-money laundering (AML) and counter-terrorist financing (CTF) regime has undergone review by the Financial Action Task Force (FATF). The UK achieved the best ratings of over 100 countries assessed so far in this round of evaluations. The FATF found that the UK has a robust understanding of its money laundering and terrorist financing risks, and that our national AML and CTF policies, strategies and activities seek to address the risks identified in our public National Risk Assessments (NRAs).

Nevertheless, the UK cannot afford to be complacent, and continues to address ML and TF risks proactively. In July 2019, the Home Office, HM Treasury and UK Finance, in collaboration with other public and private stakeholders published the Economic Crime Plan, setting out the UK's 7 strategic priority areas to further combat economic crime. The plan builds on the commitments made in the UK's Anti-Money Laundering and Counter-Terrorist Financing Action Plan 2016, UK Anti-Corruption Strategy 2017 and Serious and Organised Crime Strategy 2018, by outlining 52 actions to enhance the UK's economic crime response, including recommendations following FATF's review of the UK.

Likewise, updates to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 in January 2020, following the EU's Fifth Anti-Money Laundering Directive (5MLD) have brought a greater number of sectors in scope. Cryptoasset exchange providers, custodian wallet providers, art market participants and letting agency businesses are all now subject to the regulations, and assessments have been made of the related risks within this NRA.

The creation of the National Economic Crime Centre (NECC), and the Office for Professional Body Anti-Money Laundering Supervision (OPBAS) in 2018 have both helped to further strengthen and coordinate our response to money laundering .Likewise, the public private partnership has continued to grow. This partnership was cemented with the inception of the biannual joint Home Secretary-Chancellor chaired Economic Crime Strategic Board in January 2019.

To further strengthen our regime and prevent money laundering and terrorist financing we must continue to update our understanding of where our ML and TF risks lie. This needs to be embedded into the work at the centre of government, through our supervision and law enforcement work, and to be well understood by the regulated sectors. This assessment sets out our latest understanding of these risks, including how they have changes since the 2017 NRA. It will inform all of our continuing work to prevent terrorists and criminals moving money through the UK.

Key findings

- The traditional high-risk areas of money laundering remain, including financial services, money service businesses, and cash. However, new methods continue to emerge within these, as criminals adapt to increased restrictions and exploit vulnerabilities in different sectors and emerging technology. The growth and

integration of financial technology firms for example presents criminals with new intermediaries and methods to abuse in this sector.

- Cash-based money laundering is still heavily characterised by the use of cash intensive businesses to disguise criminal sources of wealth, or by smuggling large amounts out of the UK. However, an increase in the abuse of cash-related services has been noted, such as cash deposit services in Post Offices, and the use of cash couriers and cash & valuables in transit companies. This is alongside continued abuse of legitimate UK services, such as money transmission and retail banking.

- Recent regulatory changes through the transposition of 5MLD recognised the risk cryptocurrencies pose. Overall, the cryptoasset ecosystem has developed and expanded considerably in the last 3 years, leading to an increased money laundering risk, with criminals increasingly using and incorporating them into their money laundering methodologies. Art market participants are also newly regulated entities. Although there is still a lack of complete understanding of the mitigations and vulnerabilities in the art market, the ability to conceal the beneficial owners and final destination of art make it attractive for money laundering. The same applies to the newly regulated letting agency businesses.

- Professional services remain attractive to criminals as a means to create and operate corporate structures, invest and transfer funds to disguise their origin, and lend layers of legitimacy to their operations. Recent thematic Private Public threat assessments have helped develop our understanding since 2017, particularly around the risks associated with trust and company service providers. Upcoming reforms of Companies House and Limited Partnership structures will help further mitigate against some of the identified risks and advance beneficial ownership transparency. While there have been improvements in the supervision of accountancy and legal service providers, in part due to the work of OPBAS, these services remain prevalent in law enforcement cases.

- The UK's terrorist financing threat continues to involve low levels of funds being raised by UK individuals for the purpose of lifestyle spending and low sophistication attacks. The majority of funds raised domestically are predominantly collected through legitimate means which includes salaries and state benefits. Terrorists are also using methods that are easily accessible to purchase items for attacks such as cash and debit/credit cards. We are seeing a small growth in other methods such as cryptoassets, though it is highly unlikely that usage for terrorist purposes in the UK is widespread. There is some evidence of funding being sent to relatives and associates engaging in terrorism abroad however, it is suspected that these funds are used for general living expenses, as opposed to international attack planning.

- Our knowledge of the money laundering and terrorist financing risks has improved greatly since 2017. This is beginning to improve the mitigations in multiple areas. However, due to improvements being very recent, we have not yet seen sufficient evidence to support a reduction of risk in any sector. As improvements continue to strengthen and economic-crime related reform programmes, such as Suspicious Activity Reports (SARs) reform and corporate transparency and register reform progress, we hope to see a reduction in risks. The detailed findings of this NRA should inform further mitigations.

Chapter 1
Aim and methodology

Aim

1.1 The National Risk Assessment (NRA) of Money Laundering and Terrorist Financing is the UK's stock-take of our collective knowledge of money laundering and terrorist financing risks in the UK. A shared understanding of money laundering and terrorist financing risks is crucial to effectively mitigate the issues, and we must continue to update our understanding as it evolves. This NRA builds on our understanding of the risks identified in our NRAs in 2015 and 2017.

1.2 The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 (MLRs) stipulate that HM Treasury and Home Office must prepare a joint report setting out the findings of a risk assessment, which identifies, assesses, understands and mitigates the risks of money laundering and terrorist financing affecting the United Kingdom. Likewise, the Financial Action Task Force (FATF) expects all countries to conduct NRAs. They expect countries to identify, assess and understand the money laundering and terrorist financing risks, to then develop and implement a risk-based national anti-money laundering (AML) and counter-terrorist financing (CTF) regime. HM Treasury and Home Office must use the NRA to inform the prioritisation and allocation of resources to counter money laundering and terrorist financing.

1.3 The MLRs also stipulate that supervisors and regulated firms have to conduct their own risk assessments, which must take into account this NRA.

1.4 Throughout, where we identify risks around services, sectors or entities, our message is not that all those involved in these areas are likely to be criminally complicit or negligent. Likewise, the overall risk ratings within the NRA is not a judgement on each individual business. Rather, our assessments reflect where sectors are at risk of abuse; individuals and firms should be vigilant towards the persistent efforts of criminals and terrorists to exploit the vulnerabilities in their services or sectors.

1.5 Taking note of the findings of this report and putting in place effective controls, policies and procedures to mitigate the risks are imperative to preventing abuse.

Methodology

1.6 The methodology used is the same as that used for the 2017 NRA. This follows the 3 key stages identified in FATF guidance of identification, assessment and evaluation of evidence within the context of the 'Management of Risk in Law Enforcement' (MoRiLE) model. The same methodology has been used for both the money laundering and terrorist financing elements of this assessment.

1.7 Several key terms are used throughout the NRA and are defined below:

- threat - this covers the intent and capability of people to cause harm, and the activities they conduct to do so: money laundering threats include predicate offences and criminals who commit them, while terrorist financing threats include those groups and individuals conducting terrorist activity.
- vulnerability - these are inherent things that can be exploited by threat actors: see below for the full list of vulnerabilities we refer to throughout the NRA.
- consequence - the impact or harm that money laundering or terrorist financing may cause, including the effect of the underlying criminal and terrorist activity on financial systems and institutions.
- likelihood - how much money laundering or terrorist financing we assess is actually happening in a sector.
- mitigations - these are the actions that are taken to reduce the risk. This includes the effectiveness, capability and capacity of firms within each sector, supervisors and law enforcement.

1.8 The first stage of the assessment focused on identifying evidence which had emerged since the last NRA was conducted in 2017. This included evidence submitted by law enforcement agencies, government departments, supervisors, firms and non-governmental organisations, as well as other published evidence. After collecting and reviewing this evidence, further evidence was gathered to fill gaps identified. Calls for evidence were issued to all supervisory bodies and to firms in all sectors, and roundtables or bilateral meetings were held to follow these up where possible. Altogether, this resulted in contributions submitted by over 100 organisations across the different sectors considered.

1.9 The next stage involved analysing the data provided by stakeholders to establish the risks present, assess the likelihood of them materialising, understand their impact, and assess the effectiveness of mitigations. We used the evidence for all sectors, activities or products to make an evaluation of the following risk factors under the categories of vulnerability, likelihood and mitigation. We used an adapted MoRiLE model to establish money laundering and terrorist financing risk rankings for each area. The MoRiLE model evaluates inherent risk, based on vulnerabilities and the likelihood of criminals or terrorists exploiting these, followed by evaluating mitigating factors to calculate the net risk in an area.

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

Table 1.A: MoRiLE model used to establish risk ratings

MoRiLE Category	Risk Factor
Vulnerabilities	Levels of transparency and anonymity in the sector
	The complexity of the product or service
	The level of exposure of the product or service to high-risk persons or jurisdictions
	Speed with which transactions relating to the product or service can be completed
	Typical volume and frequency of transactions relating to the product or service
	Accessibility of the product or service
Likelihood	An assessment of scale of money laundering or terrorist financing, including consideration of the intent and capability of actors
Mitigations	Capacity and capability of law enforcement agencies to mitigate the money laundering or terrorist financing risks around the product or service
	Capacity and capability of supervisors or regulators to mitigate the money laundering or terrorist financing risks around the product or service
	Capacity and capability of firms to mitigate the money laundering or terrorist financing risks around the product or service

1.11 Throughout the NRA, we will refer to these vulnerabilities and the likelihood and mitigations when discussing the risks.

1.12 Our assessments have been extensively reviewed by money laundering and terrorist financing experts across government, law enforcement, supervisors and the private sector. Therefore, the findings of this NRA reflect our collective understanding of the risks.

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

be exposed to some level of risk. It is also important that the narrative is read alongside the headline risk ratings, to fully understand the risks posed.

1.14 All chapters should be read. The multifaceted nature of money laundering and terrorist financing means that several sectors could be involved in one money laundering case. It is important to understand the interconnected nature of various sectors, and how controls at each and every stage in the process strengthens our defences against abuse. Throughout the NRA, we signpost connections to other sectors that you should refer to.

Next steps

1.15 Throughout the document, we have highlighted gaps in our collective understanding. All of these knowledge gaps will be fed into government's long-term Economic Crime Research Strategy. This research strategy, as committed to in the Economic Crime Plan, draws together the key evidence gaps in our understanding of the threat from economic crime. Government will work with partners from law enforcement, academia, industry and elsewhere to tackle research questions.

1.16 Government will use the NRA to inform work to fill identified response gaps. Many actions are progressing already to resolve weaknesses, which we hope will reduce the risks by the next NRA.

Chapter 2

Legal, regulatory and law enforcement framework

2.1 This chapter outlines the legal, regulatory, supervisory and law enforcement frameworks governing the anti-money laundering (AML) and counter-terrorist financing (CTF) regime in the UK, with a particular focus on where aspects of the regime have changed since the last NRA in 2017.

2.2 Since 2017, the UK's AML and CTF regime has undergone review by the Financial Action Task Force (FATF). The UK achieved the best ratings of any country assessed so far in this round of evaluations, outperforming other states who are at the forefront of tackling money laundering and terrorism financing.

2.3 The report identified key strengths for the UK as: understanding of money laundering and terrorist financing risks; cooperation domestically and internationally to address these risks; investigation and prosecution of money laundering and terrorist financing; confiscation of illicit proceeds; prevention of misuse of companies and trusts; protection of the non-profit sector from terrorist financing; and implementation of counter terrorism and counter-proliferation financial sanctions.

2.4 However, the report also identifies specific weaknesses in the UK regime which we are addressing through the ongoing HM Treasury and Home Office-led economic crime reform programme. The report identifies issues in relation to: the Financial Conduct Authority (FCA), HM Revenue & Customs (HMRC) and professional body supervisors' risk-based approach to AML/CTF supervision; inconsistent AML/CTF compliance across financial and other firms; the UK Financial Intelligence Unit (UKFIU) and Suspicious Activity Report (SARs) regime; and the accuracy of data held on the Companies House register. Where relevant, these are highlighted throughout the report.

2.5 The government has accepted FATF's recommendations and is delivering its response through the implementation of the Economic Crime Plan, along with other economic crime reform work.

Economic crime framework

2.6 In 2019, the Home Office, HM Treasury and UK Finance, in collaboration with other public and private stakeholders, published the Economic Crime Plan.[1] The plan agrees a joint vision to defend the UK against economic crime, prevent harm to society and individuals, protect the integrity of the

[1] See Economic Crime Plan 2019-2022

UK economy, and support legitimate growth and prosperity. To deliver this vision, the plan sets out 7 strategic priority areas and 52 actions to enhance the UK's economic crime response, including recommendations following FATF's review of the UK in 2018.

Table 2.A: Strategic priorities in the Economic Crime Plan

Economic Crime Plan: 7 Strategic priorities
Develop a better understanding of the threat posed by economic crime and our performance in combatting economic crime.
Pursue better sharing and usage of information to combat economic crime within and between the public and private sectors across all participants.
Ensure the powers, procedures and tools of law enforcement, the justice system and the private sector are as effective as possible.
Strengthen the capabilities of law enforcement, the justice system and private sector to detect, deter and disrupt economic crime.
Build greater resilience to economic crime by enhancing the management of economic crime risk in the private sector and the risk-based approach to supervision.
Improve our systems for transparency of ownership of legal entities and legal arrangements.
Deliver an ambitious international strategy to enhance security, prosperity and the UK's global influence.

2.7 The plan builds on the commitments made in the UK's Anti-Money Laundering and Counter-Terrorist Financing Action Plan 2016, UK Anti-Corruption Strategy 2017 and Serious and Organised Crime Strategy 2018.

2.8 The Scottish government is responsible for criminal justice policy in Scotland and is in the process of developing a plan to enhance the tackling of economic crime, in conjunction with Police Scotland and the Crown Office and Procurator Fiscal Service (COPFS). In Northern Ireland, criminal justice policy is overseen by the Department of Justice.

2.9 The UK is also undertaking the SARs Reform Programme, which will overhaul the current SARs system. The SARs regime requires transformation to manage the continued growth in the volume and complexity of financial transactions. Over the 2019 to 2020 period there were 573,085 SARs submitted to the UKFIU, a rise of over 20% since the previous reporting period, and a rise of 70% between 2011 to 2019.[2] The SARs Reform Programme began in July 2018. This is a collaborative project between public sector, private sector reporters and law enforcement to co-design a new, more efficient and effective regime to increase disruption, prevention and seizure activity.

2.10 Key elements of the programme include IT transformation, improved data analytics, and an uplift in the UKFIU resourcing to increase analytical capability, feedback and engagement with reporters. Review and

[2] 'Suspicious Activity Reports (SARs) Annual Report 2020', NCA, November 2020.

improvements to the Defence Against Money Laundering (DAML) regime and guidance aim to further improve the effectiveness of the consent regime and increase reporters' understanding of their obligations.

2.11 In July 2019, the Home Office published the Asset Recovery Action Plan for England and Wales. This sets out the commitment from the government to reform and improve the asset recovery regime in order to see a return to year-on-year increases in the value of assets denied to and recovered from criminals. It also sets out a clear ambition to work across government and the private sector to develop new, innovative approaches to recovering unenforced confiscation orders.

2.12 Drawing on the expertise of operational leaders in law enforcement and prosecution agencies to achieve these aims, the government's objectives for asset recovery is structured around 4 pillars: considering the efficacy of legal powers; strengthening the operational response; continuously reviewing and embedding best practice; and fostering innovation and collaborative working.

Legislation

Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs)

2.13 The 2017 NRA outlines the requirements imposed by the MLRs. The latest amendment to the MLRs came into force in 2020 implementing the EU's Fifth Anti-Money Laundering Directive (5MLD) and other technical changes to meet FATF recommendations and improve the supervision regime. The amendment notably brought new sectors in scope of the regulations including:

- art market participants when trading work of a value of 10,000 euros or more;
- letting agents for properties with a monthly rent of 10,000 euros or more;
- cryptoasset exchange providers and custodian wallet providers.

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. The 2017 NRA sets out more details on POCA.

Criminal Finances Act 2017

2.15 The Criminal Finances Act 2017 (CFA) amends POCA, the Terrorism Act 2000, and the Anti-Terrorism Crime & Security Act 2001, and provides additional powers to enable law enforcement and prosecution agencies to identify and recover corrupt and criminal funds from those seeking to hide, use or move them in the UK. The CFA:

- introduced unexplained wealth orders (UWOs), an investigative power which can be used to compel individuals to explain the sources of their wealth. This is a powerful tool for tackling illicit finances and corruption. Since their introduction in early 2018, the National Crime Agency (NCA) has obtained UWOs on 4 cases.[3] Recently, in the first UWO directed solely towards a Serious and Organised Crime subject, the respondent failed to show legitimate origin of his assets. This subsequently led to a settlement between the respondent and the NCA and the eventual recovery of 14 properties and 4 other assets, valued at £9.8m.
- makes provision for the freezing and forfeiture of bank and building society accounts (account freezing orders), with funds of a minimum value of £1,000, where there are reasonable grounds for suspecting an account contains the proceeds of unlawful conduct or funds intended for use in unlawful conduct.
- amends the pre-existing definition of cash to include gaming vouchers, fixed-value casino tokens and betting receipts.
- extends Part 5 (Civil Recovery) Enforcement Authority status to HMRC and the FCA, increasing their autonomy to pursue civil recovery investigations, including the use of UWOs.
- has introduced 2 new corporate criminal offences, where organisations which fail to prevent those acting for or on their behalf from facilitating tax evasion face becoming criminally liable themselves. While this is targeted at tax evasion offences, it can be used to tackle money laundering activity when the two coincide.
- has made legally certain the definition of 'unlawful conduct' to include acts of gross human rights abuse or violations – the so-called 'Magnitsky Amendment' – to facilitate the recovery of criminal assets in these cases.
- extends the potential maximum moratorium period that prevents dealing in property subject to a SAR by up to 7 months from 31 days.
- extends certain statutory POCA powers to officers of the Serious Fraud Office (SFO).

Terrorist financing legislation

2.16 The Terrorism Act (TACT) 2000 includes key provisions criminalising the financing of terrorism (sections 15-18). These include inviting, providing, or receiving money or property with the intention or reasonable suspicion that it will be used for the purposes of terrorism and using or intending to use money or other property for the purposes of terrorism. S.17A was amended by the Counter Terrorism and Security Act 2015, to explicitly criminalise the making of insurance payments in response to terrorist demands.

2.17 TACT requires institutions to submit SARs where they have knowledge, suspicion or reasonable grounds for suspicion of terrorist financing to the UKFIU. Any person can seek a defence against committing a terrorist finance

[3] With an estimated total value of £143.2 million as of 31 March 2020. 'Asset Recovery Statistical Bulletin: financial years ending 2015 – 2020.' Home Office, September 2020.

offence if they request the consent of the NCA to conduct a transaction or activity about which they have suspicions through submitting a 'Defence Against Terrorist Financing' SAR.

2.18 TACT also sets out the legislative framework for the forfeiture powers, which allows the court to make a forfeiture order where an individual is convicted of a terrorist property offence or for other terrorist offences and offences with a terrorist connection.

2.19 The Anti-Terrorism, Crime and Security Act 2001 as amended by the Criminal Finances Act 2017 (CFA), Terrorist Asset Freezing Act 2010, Crime and Courts Act 2013, Terrorism Act 2006 and Charities Act 2011 further supplements terrorist financing legislation. These specifically allow for the civil recovery of terrorist property, including powers to seize and forfeit terrorist cash, the freezing of terrorist funds in bank accounts, the permanent forfeiture of this terrorist property to the government, disclosure of information, asset-freezing and legislation under which charities operate.

Sanctions and Anti-Money Laundering Act 2018

2.20 The Sanctions and Anti-Money Laundering Act 2018 (SAMLA) provides the power for the UK to impose sanctions where appropriate for the purpose of compliance with United Nations obligations or other international obligations as well as for a number of other specific purposes, including furthering the prevention of terrorism in the UK or elsewhere and protection of UK national security interests. SAMLA enables sanctions to continue uninterrupted at the end of the EU exit transition period. Secondary legislation under SAMLA, in the form of Statutory Instruments will transfer existing EU sanctions into UK law.

2.21 SAMLA also enables the UK to bring into force autonomous sanctions regimes. On 6 July 2020, the Global Human Rights (GHR) sanctions regime was established via The Global Human Rights Sanctions Regulations 2020 under SAMLA. The GHR sanctions regime allows the UK government to impose sanctions in response to certain serious human rights violations or abuses around the world. The regime is intended to target individuals or organisations involved in serious human rights violations or abuses. The measures which can be imposed under the GHR sanctions regime are travel bans and asset freezes.

2.22 Overall, SAMLA provides the power for the UK to impose a range of sanctions, including trade sanctions such as arms embargoes, immigration sanctions such as travel bans and financial sanctions such as asset freezes.

2.23 The Office of Financial Sanctions Implementations (OFSI) in HM Treasury is responsible for helping ensure implementation and enforcement of financial sanctions in the UK, including implementation of HM Treasury powers (such as UK terrorist asset freezes). OFSI works with a wide range of individuals, businesses and non-profit organisations (NPO) affected by sanctions to raise awareness, provide financial sanctions guidance, while delivering a professional service to the public and industry. OFSI also works closely with other government departments to help ensure that sanctions breaches are rapidly detected and addressed effectively. OFSI's overarching aims are to:

support the UK's foreign policy and national security goals; and to help maintain the integrity of and confidence in the UK financial services sector.

2.24 Since receiving powers to impose monetary penalties, OFSI has issued 4 monetary penalties to companies found to be in breach of financial sanctions. The largest of these was a penalty of £20.4 million imposed on Standard Chartered bank in February 2020. OFSI took compliance action in every reported breach case, which in 2018 to 19 was 99 cases. To aide compliance, OFSI produces extensive guidance documents and engages internationally to help improve compliance, recognising well that cases with a UK nexus can be multi-jurisdictional.

Terrorist Asset-Freezing etc Act 2010

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

2.26 TAFA is currently the UK's main domestic counter-terror asset-freezing legislation, with HM Treasury responsible for final designations. Between 1 April 2019 and 31 March 2020, HM Treasury renewed the designations of 18 individuals and entities. HM Treasury delisted one entity (Hizballah Military Wing) under TAFA but also added one entity (Hizballah). This decision aligns with the UK decision made in 2019 to proscribe the entire Hizballah organisation under the Terrorism Act 2000.

2.27 The Counter Terrorism (Sanctions) (EU Exit) Regulations 2019 under SAMLA are designed to replace TAFA with substantially the same effect. Using the powers in SAMLA, this new regulation will enable the domestic counter-terrorist sanctions regime to operate more effectively and will ensure that elements of the counter-terrorism sanctions regimes are harmonised with other sanctions regimes. These regulations will come into force from the end of the EU Exit transition period.

Supervisors

2.28 There are 25 supervisors that oversee regulated firms' compliance with the MLRs. This includes credit institutions, financial institutions, cryptoasset businesses, auditors, insolvency practitioners, external accountants and tax advisers, independent legal professionals, money service businesses, trust and company service providers, estate and letting agents, high value dealers, casinos and art market participants. There are 3 statutory supervisors (FCA, HMRC and the Gambling Commission) and 22 approved professional body supervisors for supervising the legal and accountancy sectors, overseen by the Office for Professional Body Anti-Money Laundering Supervision (OPBAS).

2.29 HMRC supervises accountancy service providers (not supervised by professional body supervisors), art market participants, estate and letting agents, high value dealers, money services businesses (not supervised by the FCA), and trust and company service providers (not supervised by professional body supervisors or the FCA). In October 2019, HMRC

introduced a new sanctions framework for all supervised sectors and have a new basis for calculating penalties for non-compliance. The new framework ensures that the full range of sanctions are used as appropriate to reflect the scale of non-compliance and the money laundering and terrorist financing risks posed, and that financial penalties are dissuasive and proportionate to the severity of the breach.

2.30 HMRC's Fraud Investigation Service (FIS) is responsible for civil and criminal investigations into the most serious tax fraud and wrongdoing. HMRC's AML/CTF supervisory authority work is carried out by FIS, using powers derived from the MLRs. This includes powers to require the production of documents or information, to require individuals to attend and answer questions, and powers allowing HMRC supervisory staff to enter premises.

2.31 They also have powers to suspend or cancel a business's registration or issue a wide range of sanctions for non-compliance, including financial penalties as well as censuring statements. FIS can also progress criminal investigations for MLR breaches or POCA money laundering offences. Although terrorist financing is not a statutory responsibility for HMRC, it assists other law enforcement partners with terrorist financing investigations, including providing intelligence or alternative interventions, such as gift-aid fraud.

2.32 The FCA is the AML supervisor for credit and financial institutions[4] as well as cryptoasset businesses. In addition to its powers under the MLRs, the FCA gains the majority of its powers from the Financial Services and Markets Act 2000 (FSMA). It has extensive supervisory and enforcement powers to impose sanctions including suspensions and restrictions, prohibitions, public censures and disgorgement. It can compel firms to produce documents or information and require a firm to appoint a third-party skilled person to review their control environment. They also have powers in Part 4 FMSA to vary or cancel an authorised person's permission as well as impose a requirement on an authorised person.

2.33 The Gambling Commission is a non-departmental public body set up under the Gambling Act 2005. It regulates all commercial gaming in Great Britain, including all casinos, bingo, gaming machines and lotteries, including the National Lottery, betting and remote gambling. The Gambling Commission is the AML supervisory authority for currently 217 land-based and remote casinos, and the money service businesses offered in approximately 50 of those. The Gambling Commission also currently licences approximately 12,600 Personal Function Licence holders and around 505 Personal Management Licence holders who meet 'fit and proper' testing to undertake, among other responsibilities, AML and CTF oversight and management functions in casinos. The Gambling Commission has powers to supervise and enforce against breaches of the MLRs. Although terrorist financing is not a statutory responsibility for the Gambling Commission, it assists other law enforcement partners with terrorist financing investigations through its Intelligence Unit. Powers under the Gambling Act also afford the Gambling Commission the ability to revoke personal and business licences,

[4] The FCA supervises any MSB activity undertaken by a firm it already regulates for other activities such as banking.

implement unlimited fines for breaches and add additional licence conditions for businesses to operate.

2.34 **OPBAS** is hosted within the FCA and is the oversight body for the 22 legal and accountancy professional body supervisors (PBSs). It was established in 2018 to address weaknesses in AML/CTF supervision in the legal and accounting sectors identified in the 2015 and 2017 NRAs. It has 2 focused objectives: improving the standard and consistency of AML supervision by the PBSs and facilitating increased intelligence and information sharing between the PBSs, statutory AML supervisors and law enforcement. Similarly to the FCA, OPBAS has a range of additional powers under the OPBAS Regulations 2017[5] to ensure compliance including to require information and/or documents, require a PBS to attend and answer questions, issue directions or appoint a skilled person. They also have 2 further enforcement powers under the same regulations to issue a statement of public censure or to make a recommendation to HM Treasury to remove the PBS from Schedule 1 of the MLRs.

2.35 The **Charity Commission for England and Wales** is a non-ministerial government department that registers and regulates charities in England and Wales and maintains a public Register of Charities. It is a civil regulator but has and can intervene in cases where there has been, or there is a risk of, abuse of charities, working closely with law enforcement, and if required, can use its specific powers that include the ability to protect and redirect charitable funds, remove or disqualify trustees and direct dissolution of charities.

2.36 The **Office of the Scottish Charity Regulator** is a non-ministerial office and part of the Scottish Administration that is responsible for the registration and regulation of charities in Scotland and maintains the Scottish Charity Register. One of its functions is to identify and investigate apparent misconduct in the administration of charities and it works closely with other public bodies where required. It has a range of powers including those that can be used to freeze bank accounts of charities and prevent transactions being entered into. It can also apply to the Court of Session for more permanent sanctions to be applied including the disqualification of current and former charity trustees.

2.37 The **Charity Commission for Northern Ireland** is a non-departmental public body responsible for the registration and regulation of charities in Northern Ireland. Its functions include the identification and investigation of apparent misconduct or mismanagement in the administration of charities. It is empowered to take remedial or protective action in connection with such misconduct or mismanagement, including the freezing of property held on behalf of a charity, the restriction of transactions which may be entered into in the administration of a charity and the suspension or removal of trustees.

[5] The Oversight of Professional Body Anti-Money Laundering and Counter Terrorist Financing Supervision Regulations 2017.

Money Laundering related law enforcement agencies

2.38 The National Crime Agency is the lead law enforcement agency in England and Wales for serious and organised crime, dealing with the highest-level criminality. Their tools and powers include: intelligence and evidence-gathering; cash seizure and forfeiture; restraint and confiscation; and civil recovery and taxation.

2.39 The National Economic Crime Centre (NECC), hosted within the NCA, was established in 2018 and leads and coordinates the UK's response to economic crime both at home and abroad that has a national impact.[6] The multi-agency initiative comprises of representatives from a variety of law enforcement and government departments,[7] who work together to progress national and departmental priorities on economic crime. They do so by harnessing intelligence and capabilities from across the public and private sectors to tackle economic crime in the most effective way. It works with partners to jointly identify and prioritise the most appropriate type of investigations, whether criminal, civil or regulatory to ensure maximum impact. It seeks to maximise the use of innovative powers, for example Unexplained Wealth Orders and Account Freezing Orders, across all agencies to tackle the illicit finance that funds and enables all forms of serious and organised crime. The NECC also hosts the Proceeds of Crime Centre and the Expert Laundering Evidence cadre which provides impartial expert evidence to courts hearing money laundering cases throughout the UK, so that the courts can understand complex money laundering methodologies, and an interpretation of evidence. Police Scotland has worked closely with the NECC and has taken an active part in projects including the NECC's work on fraud.

2.40 The UKFIU, an operationally independent part of the NECC, receives financial intelligence gathered from SARs, and makes all SARs available to appropriately trained officers in law enforcement agencies and other approved bodies for their own analysis and investigations (with the exception of SARs in certain sensitive categories). The UKFIU works in close partnership with other key international organisations such as the Egmont Group to fight money laundering and terrorist financing. The UKFIU is a fully active member of the international Egmont Group of Financial Intelligence Units, set up to improve cooperation in the fight against money laundering and the financing of terrorism.

2.41 All police forces within the UK have the powers to conduct money laundering investigations. There are 43 police forces in England and Wales subject to oversight from Police and Crime Commissioners. Scotland has a single national police service, Police Scotland, which is funded by and accountable to the Scottish Police Authority. In Northern Ireland, the Police Service of Northern Ireland (PSNI) is funded by the Northern Ireland Department of Justice and is accountable to the Northern Ireland Policing Board. The City of London Police (as national lead force for economic crime

[6] The NECC's work covers England and Wales and it also works closely with Police Scotland and Police Service Northern Ireland.

[7] The NECC has officers or representatives from the NCA, SFO, FCA, City of London Police, HMRC, Crown Prosecution Service, Cabinet Office, Home Office and Foreign, Commonwealth and Development Office.

and fraud) and the **Metropolitan Police Service** regularly take on national investigations and provide support to the NCA.

2.42 Police forces in England and Wales have collaborated to form **Regional Organised Crime Units** (ROCUs) across 9 policing regions. These units deliver specialist investigative and intelligence capabilities within their regions and are the primary interface between the NCA and local forces and are accountable to their respective Police and Crime Commissioners. Within each ROCU is a **Regional Economic Crime Unit** (RECU), whose main role is to recover criminal assets through confiscation and civil powers on behalf of the regional and local forces, and other agencies such as HMRC, NCA and Trading Standards.

2.43 In addition to these capabilities, there is the **Asset Confiscation Enforcement** (ACE) network funded by the Asset Recovery Incentivisation Scheme. This capability has a presence across every region in England and Wales and has had a significant impact on tackling unenforced confiscation orders.

2.44 The policing response to serious and organised crime is a devolved matter. **Police Scotland** works closely with the NCA, HMRC, the FCA and other relevant agencies in investigating economic crime. The Scottish Crime Campus is a multiagency centre, established by the Scottish government in 2014, which accommodates the key agencies involved in tackling economic crime in Scotland.

2.45 The **Police Service of Northern Ireland** is the lead operational agency for serious and organised crime in Northern Ireland and the NCA and other UK law enforcement agencies work closely with them. PSNI has a dedicated Economic Crime Unit with specialist investigative capabilities. A central ACE team supported by regional ACE sub-teams lead on confiscation investigations and enforcement within PSNI, and are part of the ACE network.

2.46 The **SFO** is an independent government department that investigates and prosecutes serious or complex fraud, bribery and corruption and associated money laundering. It has jurisdiction in England, Wales and Northern Ireland but not in Scotland, where this responsibility rests with the Crown Office and Procurator Fiscal Service. The SFO has a dedicated Proceeds of Crime Division which comprises a team of lawyers and financial investigators who deal with confiscation investigations, restraint proceedings, money laundering investigations and civil recovery work across the SFO's cases, as well as mutual legal assistance requests.

2.47 **HMRC**, as the UK's tax authority, is a non-ministerial department reporting to Parliament through the Financial Secretary to the Treasury. As well as being an MLR supervisor, it is responsible for investigating serious tax fraud using its extensive range of civil, criminal and tax investigation powers. This include money laundering linked to tax offences. FIS works with the independent prosecuting authorities to secure convictions.

2.48 HMRC's Risk and Intelligence Service gathers information, develops intelligence and provides strategic and tactical understanding of tax-related money laundering risks. Subject to appropriate disclosure gateways, it shares

this insight with other domestic and international tax and customs administrations, and law enforcement partners.

2.49 Border Force are a law enforcement command of the Home Office responsible for keeping the border secure and promoting national prosperity by facilitating the legitimate movement of individuals and goods, while preventing those that would cause harm from entering the UK. Border Force perform a unique role within law enforcement anti-money laundering activity through a continued focus on the deterrence and prevention of illicit cash and listed asset smuggling across the UK border. Intelligence development and investigative work is carried out in close partnership with numerous UK and overseas law enforcement agencies.

2.50 The FCA investigates and prosecutes money laundering which is ancillary to offences that it is responsible for under its statutory objectives, including market manipulation, insider dealing and unauthorised business activity such as boiler room frauds.

Terrorist Financing related law enforcement agencies

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

2.52 UK intelligence agencies and the Joint Terrorism Analysis Centre are responsible for monitoring and assessing the terrorist financing threats to the UK and its interests overseas. These agencies are supported by the National Terrorist Financial Investigation Unit (NTFIU), part of the Metropolitan Police Service Counter Terrorism Command, which has the strategic police lead for countering terrorist financing in the UK. The NTFIU leads investigations where the primary focus is on addressing the finances of a terrorist, a financier of terrorism or of a terrorist organisation, and supports mainstream counter-terrorism investigations with both financial intelligence and financial disruption options. Nationally, there are ten additional Counter-Terrorism Units (CTUs) and intelligence units located in England, Scotland, Wales and Northern Ireland, responsible for investigating instances of terrorist financing occurring within their geographical regions and for supporting mainstream counter terrorism investigations with financial intelligence.

2.53 The UKFIU's Terrorist Finance Team identifies, assesses and exploits SARs submitted under both TACT and POCA. Due to the additional sensitivity around SARs submitted under TACT, and those SARs submitted under POCA identified as having a terrorist financing link, these SARs are made available only to a restricted group of end users.

2.54 In relation to terrorist asset-freezing, proposals for designation under TAFA are made to OFSI by the police and the Security Service, or by other government departments or international governments where there is evidence to support a designation. The investigation of breaches is

conducted by the relevant CTU, with engagement from others including OFSI and the Crown Prosecution Service.

Prosecution agencies

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

2.56 The Public Prosecution Service Northern Ireland is the independent prosecuting authority in Northern Ireland and is responsible for prosecuting criminal cases investigated by the police, HMRC and the NCA in Northern Ireland. It is headed by the Director of Public Prosecutions Northern Ireland who is appointed by the Attorney General for Northern Ireland.

2.57 The Crown Office and Procurator Fiscal Service (COPFS) is responsible for the prosecution of all crime in Scotland. COPFS' responsibilities include the investigation, prosecution and disruption of crime, including the maximisation of measures to ensure the recovery of proceeds of crime. COPFS has an investigative role and can provide instructions and directions to the police and all other specialist reporting agencies. In all matters of international cooperation, COPFS deals directly with the criminal authorities in other countries. COPFS is headed by the Crown Agent who is accountable to the Lord Advocate, the principal law officer of the Crown in Scotland.

2.58 The SFO and FCA are independent prosecutors. The FCA is the conduct regulator for financial services firms and financial markets in the UK as well as a prudential supervisor. The FCA has powers to investigate and prosecute breaches under the FSMA, the MLRs which constitute a criminal offence and in appropriate circumstances offences which constitute money laundering contrary to the POCA. Such circumstances include market abuse and unauthorised business activity such as boiler room frauds. The FCA has a dedicated Proceeds of Crime Team who deal with confiscation investigations, restraint proceedings and have the powers to undertake money laundering investigations and civil recovery work, both domestically and internationally, where authorised financial investigators and specialist POCA lawyers work in tandem on cases.

2.59 The SFO is a specialist prosecuting authority, established in 1988 following the Lord Roskill Report (Fraud Trials Committee Report) in order to investigate and prosecute cases at the top-most tier of serious or complex fraud. Under the Criminal Justice Act 1987 the Director of the SFO may investigate any suspected offence which appears to her on reasonable grounds to involve serious or complex fraud (a concept which includes both

cases of domestic or overseas bribery and corruption and money laundering). The SFO will investigate those cases which, in the Director's opinion, call for the multi-disciplinary approach and legislative powers available to the SFO. This involves lawyers, investigators, forensic accountants, intelligence analysts and other specialists working together in teams in order to tackle the increased complexity and sophistication of the business world, and is referred to as the 'Roskill' model.

2.60 The model of continuous ownership through investigation and prosecution stages is a fundamental characteristic of the SFO, together with its visible and demonstrable independence. It is a valuable exception to the normal practice in the UK, where crime is generally investigated by a police force and the evidence passed to the CPS to decide whether to prosecute.

Public private partnership

2.61 The public private partnership, which comprises of both government departments, law enforcement agencies[8], businesses and trade bodies from across the AML/CTF regulated sectors, underpins the delivery of the Economic Crime Plan by directly bringing together government and industry to ensure both sides have a voice and vested interest in the delivery of the Plan. The partnership first formally collaborated in 2002 with the formation of the Dedicated Card and Payment Crime Unit. It developed through 2015 and 2016 with the establishment of the Joint Money Laundering Intelligence Taskforce (JMLIT), and the Joint Fraud Taskforce respectively.

2.62 The partnership was cemented with establishment of new public private governance. This includes the inception of the biannual joint Minister chaired Economic Crime Strategic Board (ECSB) in January 2019, which published the Economic Crime Plan in July 2019, and the quarterly Public Private Steering Group (PPSG), tri-chaired by Home Office, HM Treasury and UK Finance. The PPSG oversees delivery of the Economic Crime Plan against joint priorities. Likewise, the Economic Crime Civil Society Organisations Steering Group (CSOSG) has been established. The CSOSG is an independent grouping of individual civil society organisations who track and inform the delivery of the Economic Crime Plan, highlight new and emerging areas of risk, and serve as an independent challenge function with the aim of ensuring that ECSB decision-making is transparent and in the public interest.

2.63 JMLIT groups have continued to grow in membership to further facilitate the exchange and analysis of information related to money laundering and terrorist financing. JMLIT has now been expanded to include members from the insurance and investment sectors.

2.64 JMLIT's Terrorist Financing Experts Working Group provides a centralised terrorist financing forum. The Terrorist Finance Experts Group was established to support the exchange and analysis of terrorist finance information. It is comprised of over 25 financial institutions, payment services, supervisors, government, law enforcement and civil society partners,

[8] Including HM Treasury, Home Office, BEIS, NCA, FCDO, Cabinet Office, and others.

with the ability to distribute information to a much wider audience. The group supports thematic pieces of work focused on improving understanding of threats, risks, typologies and methodologies that support the financing of terrorism to improve the detection and disruption of terrorist financing. This is carried out through analytical assessments and projects.

2.65 On the recommendation of a former Independent Reviewer of Terrorism Legislation, David Anderson QC, the UK has enhanced its partnerships with aid agencies by increasing dialogue with charities and the banking sector. This includes establishing the Tri-Sector Group. The Tri-Sector Group is a growing partnership between government and representatives of the charitable and financial sectors. It is a forum through which members can routinely discuss issues relating to the implementation of counter-terrorism legislation, including the impact this can have on charitable work overseas in high-risk areas. Through the Tri-Sector Group we are working collaboratively to help address key challenges and to support the work of aid agencies, while enabling members to play an active role in developing new policy. The partnership has also positively contributed towards awareness building which has enabled the charity sector to effectively equip and safeguard their activities from terrorist threats.

2.66 To expand the role the accountancy and legal professional body supervisors play in information sharing, OPBAS, alongside the NECC, established the Intelligence Sharing Expert Working Groups (ISEWGs). The ISEWGs bring together the PBSs, statutory AML supervisors and law enforcement to discuss and consider strategic and tactical intelligence related to money laundering or terrorist financing investigations featuring accountancy or legal professionals.

International framework

The Financial Action Task Force (FATF)

2.67 The FATF is an inter-governmental body established in 1989 by the ministers of its member jurisdictions. The objectives of the FATF are to set standards and promote effective implementation measures for combating money laundering, terrorist financing and proliferation financing. The FATF also periodically monitors the implementation of its recommendations among members through a peer review process (mutual evaluation).

2.68 As mentioned above, the FATF completed its assessment of the UK in 2018, as part of its regular peer review assessment cycle. The UK achieved the best ratings of any country assessed so far in this round of evaluations. This outcome helps to strengthen the UK's global reputation as a leader on tackling illicit finance and as a good place to do business. The UK continues to ensure it is updating its AML/CTF framework to align with the latest FATF standards. This includes the newest standards for cryptoassets. See chapter 8 for more details.

2.69 The European Union (EU) implements FATF recommendations through EU directives that member states are required to transpose into national law. Since the last NRA, the government has completed its transposition of 5MLD into domestic law. This transposition ensures the UK's AML/CTF regime remains comprehensive, responsive to emerging threats, and in line with evolving international standards set by the FATF. Although the UK has now left the EU, FATF recommendations that were implemented via EU legislation have been retained in UK law under the European Union (Withdrawal) Act 2018.

2.70 The UK will continue to meet and exceed FATF standards. The UK remains absolutely committed to ensuring the safety and security of UK citizens, including through combatting money laundering and terrorist financing.

Chapter 3
Money laundering threat

3.1 This chapter provides an update on the nature and scale of the UK money laundering threat, defined as those activities which lead to criminal intent to launder money.

3.2 Financial profit remains the primary motive for the vast majority of serious and organised criminals. In order for criminal profits to be incorporated into the legitimate economy they are often made to appear as from legitimate sources. However, this is not always necessary, depending on what criminals intend to use the funds for. Those responsible continue to make use of a wide range of methods, with varying purposes, levels of scale and complexity. This includes use of both the regulated and unregulated sectors. Methods can range from laundering small amounts of cash to sophisticated processes involving large sums of money. Methodologies can exploit UK and overseas financial and professional services industries, in particular those jurisdictions with weak or ineffective anti-money laundering (AML) controls.

3.3 While a significant amount of UK criminal activity generates its proceeds in cash, law enforcement agencies continue to see increasingly diverse methods, as criminals exploit vulnerabilities in different and emerging technology and sectors as well as adapt to increased restrictions in the regulated sector. The reason for the methods employed can vary, including to confuse the audit trail, to further invest in criminal activity or simply to enjoy the benefits of crime. Criminal decision making on the methods used to launder the proceeds of crime is also driven by the intended use of the funds. For example, groups may choose to reinvestment in supply in the source country or the concealment of assets offshore with the help of enabling services.

3.4 The traditional areas of money laundering activity remain, though new methods continue to emerge within these. Cash-based money laundering is still heavily characterised by the use of cash intensive businesses to disguise criminal sources of wealth, or huge amounts smuggled out of the UK. This is alongside continued abuse of legitimate UK services, such as money transmission (often managed through international controllers) and retail banking. Mule accounts continued to be used extensively to move funds; more than 42,482 cases of suspected money mule account activity were reported in 2019, the latest available figures, up 32% on 2017. While many willingly allow their accounts to be used for money laundering, organised crime groups (OCGs) continue to entice or groom young and vulnerable people, and more recently also the middle-aged, to become mules, increasingly targeting their victims through social media. With the increased

awareness of risk within the UK banking sector, it is almost certain that the de-banking of the money service business (MSB) sector by some retail banks has displaced criminal MSBs to the unregistered sector, using informal value transfer systems (IVTS) and complex and convoluted relationships with other MSBs to continue to operate.

3.5 Large amounts of criminal funds (often the proceeds of serious fraud or overseas corruption) continue to be laundered through the UK financial, professional services sectors and UK-registered corporate structures. The global nature of the financial system is exploited, often transferring funds through complex corporate vehicles and multiple offshore jurisdictions in order to hide the true beneficiary of the funds. This is regularly (wittingly or unwittingly) facilitated by professional services providers such as accountants, lawyers and trust and company service providers. Trade based money laundering involves exploiting both domestic trade practices and the international import and export system to disguise, convert and transfer criminal proceeds through movement of goods as well as funds. OCGs often use the services of professional money laundering networks who pool criminal proceeds from various areas of criminal activity and provide distance from the predicate offence. The section below provides an outline of the different sources of criminal proceeds assessed to be highest priority for the UK.

3.6 It remains difficult to quantify the scale of the money laundering threat to the UK, but it is likely there has been an increase in the amount of money being laundered since 2017. This is due to an increase in crime across a range of predicate offences.

3.7 The UN estimates that 2-5% of global GDP is laundered and given London's position as one of the world's largest financial centres, there is a realistic possibility that it remains in the hundreds of billions of pounds annually. It is likely that the majority of this is corrupt money from outside the UK, but it also includes the proceeds of crime generated from within the UK.

3.8 Between April 2018 and March 2020, law enforcement agencies in England, Wales and Northern Ireland have collected £306 million against confiscation orders, and forfeited an additional £130 million.[1]

Domestic threat

3.9 Serious and organised crime (SOC) continues to have more impact on UK citizens than any other national security threat, affecting a wide range of public services, infrastructure, and vulnerable individuals on a daily basis. SOC has a considerable impact on the UK economy, costing an estimated £37 billion per year.

3.10 The scale of the threat from SOC is growing across several areas, and the threat is becoming more complex, as criminals exploit available technology to communicate,commit and hide their crimes. The 2019 Crime Survey for England and Wales (CSEW) estimated 10.9 million incidents of crime, a

[1] 'Asset Recovery Statistical Bulletin: financial years ending 2015 – 2020.' Home Office, September 2020.

1.86% increase compared with the previous year's survey.[2] Victim reported losses from fraud increased by 38% to £2.2 billion in the year ending March 2019, levels of firearms offending continue to increase year on year, cocaine consumption has increased by at least 290% since 2011, while heroin purity levels are at a 10-year high. Detections of migrants attempting to enter the UK illegally have increased, and the criminals facilitating them continue to use high-risk smuggling methods, as shown by the deaths of 39 Vietnamese nationals concealed in a refrigerated lorry in October 2019.

3.11 The UK adopts an 'all-crimes approach' to money laundering, meaning that laundering the proceeds of any crime is an offence. Most serious and organised crime is conducted by criminals operating in loose networks based on reputation and experience. At the end of 2019, there were around 4,800 criminal groups in the UK, comprising approximately 37,000 associated nominals.

Fraud and tax evasion

3.12 Fraud and tax offences remain the largest known source of criminal proceeds from offending in the UK, as well as the most common crime type.

3.13 Fraud continues to cover a broad range of crime types, victims and perpetrators. The precise scale of fraud in the UK remains an intelligence gap, though the CSEW estimated there were 3.8 million incidents of fraud in the year ending September 2019, with the majority relating to bank and credit account fraud.[3]

3.14 The National Crime Agency (NCA) assesses it is likely that fraud in the UK is increasing and there has been a considerable rise in reported losses. The Office of National Statistics report that adults in England and Wales are more likely to be a victim of fraud than any other crime type.[4] Cheque, card and online banking remain the most reported type of fraud by volume, accounting for nearly half of reports to Action Fraud. UK Finance estimated fraud losses for payment card, cheques and remote banking at £853.1 million between July 2018 and June 2019, an 11% increase compared with the previous year.

3.15 Since 2017, there has also been a significant increase in reported courier fraud, with £6.5 million in reported losses. Likewise, investment fraud resulted in the highest total losses from victim reported fraud, with reported losses of £338 million in 2018 to 2019.

3.16 Cyber crime is a major enabler of fraud; data obtained via data breaches, phishing and malware is used directly to commit fraud, or is sold online to other fraudsters. It is estimated that the internet plays a role in at least 54% of all fraud.

---

[2] 'Crime Survey of England and Wales year ending September 2019', Office for National Statistics, January 2020 and 'Crime Survey of England and Wales year ending September 2018', Office for National Statistics, January 2019. This excludes the new experimental statistics on fraud and computer misuse.

[3] 'Crime Survey of England and Wales year ending September 2019', Office for National Statistics, January 2020.

[4] 'Crime Survey of England and Wales year ending September 2019', Office for National Statistics, January 2020.

3.17 Tax evasion is illegal activity, where individuals or businesses deliberately omit, conceal or misrepresent information in order to reduce or negate their tax liabilities. HM Revenue & Customs (HMRC)'s estimate of the tax gap is a useful tool for understanding fraud against the public sector. The estimated tax gap as a result of evasion in 2018 to 2019 was £4.6 billion.[5] Other tax regimes, such as excise duty also continue to be subject to criminal attacks including the coordinated and systematic smuggling of goods such as alcohol, tobacco or oils. HMRC estimate the tax gap resulting from criminal attacks to be a further £4.5 billion in 2018 to 2019.[6]

Drugs supply and drugs offences

3.18 The 2017 NRA highlighted the reduction in drug misuse in England and Wales. Following this decline, drugs misuse has been rising since 2016, and in 2018 to 2019, it was estimated that 9.4% of the UK population misused them. The CSEW shows 139,181 drug offences for the year ending June 2018, an increase of 4% on the previous year.

3.19 The size of the illicit drugs market in the UK in 2018 was estimated to be £5.3 billion. However, recent research into specific drugs suggests the actual figure is much higher. Cannabis, cocaine and heroin make up 72% of all drug criminality. However, other areas of the drug market have continued to diversify. New forms of synthetic drugs have come to market, with new customer bases and new techniques for buying and selling. For example, fentanyl is now being seized in a wider variety of forms, including as pills.

3.20 In terms of asset confiscation orders made in 2018 and 2019, drug trafficking orders account for 51% of volume and 16% of value. These figures are similar to those reported in the 2017 NRA.

Cyber crime

3.21 Cyber crime can be categorised as cyber-dependent, which can only be committed using computer technology (e.g. ransomware), or cyber-enabled, which can be conducted offline (such as fraud), but if done online, can take place at unprecedented scale and speed. Methods have remained fairly consistent, as existing tools continue to prove successful. Likewise, the bar for entry into cyber crime continues to lower, due to the ready availability of both cyber crime tools and the instructions in how to use them.

3.22 There were 21,471 computer misuse offences recorded by the National Fraud Intelligence Bureau in the year ending September 2019, a decrease of 11% on the previous year,[7] with ransomware being the most visible threat. High profile incidents include the 2019 ransomware attack on Eurofins Scientific, which affected victims globally, including UK businesses. The CSEW reported that in the year ending September 2019 there were just over a million computer misuse incidents against individuals, and that the internet played a role in an estimated 54% of the total 3.8 million incidents of fraud.

5 'Measuring tax gaps 2020 edition - tax gap estimates for 2018 to 2019', HMRC, July 2020.

6 'Measuring tax gaps 2020 edition - tax gap estimates for 2018 to 2019', HMRC, July 2020.

7 This decrease is reported to be affected by Action Fraud's internal case review process and their online reporting tool. Changes made in October 2018 resulted in some computer misuse offences now being more accurately classified as fraud offences.

However, under-reporting by both individuals and organisations (including financial institutions) remains a significant issue; the true scale and cost of cyber crime continues to be obscured.

3.23 Cyber attacks can have a large financial and psychological impact on victims. In one ransomware attack alone, a company lost €60million in revenue.

Acquisitive crime

3.24 Organised acquisitive crime (OAC) covers theft, robbery and burglary, and may be carried out by individuals or OCGs. Acquisitive crime is wide reaching, affecting members of the public, communities, industry and national infrastructure. Overall, there has been an increase in acquisitive crime in 2019. In the year to September 2019, there was a 4% increase in vehicle offences continuing a trend seen in the last 3 years. Similarly, robbery offences have also increased in the last 4 years, with an increase of 12% in the year to September 2019. Conversely, during the same time period, burglary offences decreased by 4%.

3.25 Since 2015, vehicle thefts have increased gradually; offenders use different methods, including technology to bypass modern security measures, often targeting prestigious and higher value cars. The online marketplace is a key disposal route for stolen property, including vehicle parts. In other areas of OAC, ATM attacks reduced in number in 2019 with a corresponding decrease in the amount stolen. Thefts from cash in transit vehicles also decreased in 2019.

Organised immigration crime

3.26 In 2015 and 2016, large scale migration across the Mediterranean, driven in part by instability in Africa and the Middle East, led to organised immigration crime (OIC) being assessed as the fastest growing criminal market in Europe. While numbers making illegal border crossings into Europe have reduced (about 140,000 in the year 2019 to 2020)[8], there remains a sophisticated criminal infrastructure run by OCGs who perceive OIC as a low risk-high reward activity. Home Office reporting from January 2019 estimated the social and economic costs to the UK as £73 million, though the true costs are almost certainly higher (these figures do not estimate the undetected impact or consider upstream/overseas OIC that impacts the UK). There remain intelligence gaps around the financial flows from organised immigration crime and the extent to which the UK is a destination for the related illicit funds.

Modern slavery

3.27 The term 'modern slavery' includes the offences of human trafficking, slavery, servitude and forced or compulsory labour. The FATF's 2018 study on human trafficking noted that it is an offence with diverse financial flows, and where proceeds are realised differently across the world, and across the various types of human trafficking. The report estimates the total proceeds

[8] See frontex.europea.eu/along-eu-borders/migratory-map.

of human trafficking to exceed $150.2 billion globally, making it one of the largest generators of criminal proceeds in the world.

3.28 Although only providing a partial picture, reporting from the National Referral Mechanism gives a total of 7,273 potential victims in 2019 up to October. This is a 45% increase from the same period in 2018, but it is not known if this is due to an increase in cases or improved reporting. In 2018, the Home Office estimated that the costs to the UK from modern slavery offences was between £3.3-4.3 billion in 2016 to 2017. Understanding of financial flows linked to modern slavery and human trafficking is improving, but knowledge gaps remain.

Illegal wildlife trade (IWT)

3.29 The IWT includes the trade in species that are protected and prohibited from all national or international commercial trade, and the trade in volumes of certain species of wild origin which is unsustainable and in violation of provisions set nationally or by the Convention on the International Trade of Endangered Species. Illegal trade in the UK can impact directly on the survival of endangered species in other parts of the world. The Government is committed to combatting the IWT at the global level and has established initiatives such as the Illegal Wildlife Trade Challenge Fund, which supports projects around the world that are tackling this activity.[9]

3.30 International organisations including the FATF have assessed the IWT to be a major transnational organised crime generating billions of criminal proceeds every year. A recent study by the FATF highlights that the criminal proceeds associated with the IWT are generated in and moved through jurisdictions around the world, including the UK, with criminals exploiting weaknesses in the financial and non-financial sectors[10].

3.31 To varying degrees, the UK is a source, transit and destination country for illegally traded wildlife. Among a wider range of species, this includes the illegal sale of ivory products via online marketplaces and social media with payments made through online payment platforms. The proceeds involved can in some cases reach significant amounts but typically involve lower levels of proceeds in the UK, with the potential to generate exponentially larger proceeds when shipped overseas and resold in the jurisdiction of the purchaser.[11] The IWT in the UK also includes the illegal transiting and export of protected European Eels beyond the EU. Criminals involved in this illicit trade are able to generate millions in proceeds and have used traditional money laundering methods to obfuscate the criminal origins of these proceeds including through the use of legitimate wildlife trade as front companies, as demonstrated by a recent case in the UK.[12]

9 Illegal Wildlife Trade (IWT) Challenge Fund .

10 'Money Laundering and the Illegal Wildlife Trade', FATF, June 2020.

11 'Two Men Sentenced For Illegally Exporting Carved Ivory Fans', National Wildlife Crime Unit, September 2019.

12 'Seafood salesman sentenced for smuggling eels' National Crime Agency, March 2020.

Chapter 4
International outlook

4.1 The UK has one of the world's largest and most open economies with London being particularly attractive for overseas investors. Research suggests the UK is the world's leading net exporter of financial services, alongside being a major centre for professional services that support financial services.[1] Likewise, the World Bank ranks the UK 8th in the world for its ease of doing business.[2] These factors make the UK attractive for legitimate business, but also expose the UK to money laundering risks from overseas. This section outlines particularly relevant cross-border money laundering risks faced by the UK.

International money laundering threat overview

Trade based money laundering (TBML)

4.2 TBML involves exploiting both domestic trade and the international import and export system to disguise, convert and transfer criminal proceeds through movement of funds, and goods (or the appearance of moving goods). Organised criminal gangs (OCGs) often use the services of professional money laundering networks who pool criminal proceeds from various areas. The complexity, anonymity and scale of global trade makes this a favoured money laundering technique, which has increased since 2017.

4.3 TBML schemes can enable the movement of any amount of criminal proceeds between entities and jurisdictions, including amounts larger than might otherwise be possible in cash-based money laundering. These entities are often shelf companies[3], or businesses where scrutiny and beneficial ownership transparency is avoided. Shelf companies may also be used for third party settlements, where legitimate monies can be used to pay criminal networks and criminal monies used to settle legitimate transactions. Some businesses may even be established for the sole purpose of acquiring a bank account to receive criminal cash deposits and arranging overseas transfers. This has increasingly been observed in TBML schemes. Company formation and related professional services are therefore a key enabler or gatekeeper of

1 'Key facts about the UK as an international financial centre 2019', The City UK, December 2019.

2 'Ease of Doing Business Index', World Bank, 2020.

3 Trust or Company Service Providers (TCSPs) often sell 'shelf' companies with established banking and credit histories to create the impression of a reputable company, or may offer nominee shareholder or directors, which can increase the anonymity of beneficial owners.

TBML activity. More detail on the risks associated with Trust and Company Service Providers can be found in chapters 9, 10 and 11.

4.4 Traditional TBML techniques such as 'ghost' or 'phantom' shipping and misrepresentation of the price, quantity and quality of goods, continue to be employed by criminals. Open account trading, while a legitimate means of facilitating international trade, has been abused by money launders, as it can enable the settlement of invoices via previously unknown third parties.[4] There is growing concern about the criminal infiltration of legitimate supply chains not reliant on any form of misrepresentation of price, quantity or quality of goods. This emerging risk creates even greater challenges in successfully detecting TBML.

4.5 Non-documentary trade transactions provide banks, in most cases, no information about the underlying goods and the unit price. This enables criminals to misrepresent the price, compared with the actual value of goods being moved, obfuscating the origin of illicit funds. Vulnerabilities in traditional letters of credit have also been identified.[5] These are often heavy on free-format text and unstructured data, creating automation and screening challenges for financial institutions, which result in misrepresented prices by criminals and are more likely to go unnoticed. This highlights the risk of TBML cutting across the financial services sector too, emphasising the importance of information sharing, within and across the different regulated sectors to detect TBML activity.

4.6 A range of commodities and services continue to be used as cover for TBML, including used cars and clothing, construction and gold. In the context of the COVID-19 crisis, pharmaceuticals, textiles and personal protective equipment are increasingly likely to be used.

Politically exposed persons (PEPs)

4.7 Corruption is assessed to cost the global economy billions, if not trillions of pounds every year. It also undermines trust in governments and institutions, while fuelling instability and allowing OCGs to profit from their criminality.

4.8 A considerable threat to the UK arises from overseas PEPs laundering their illicit gains through the UK. The UK's role in facilitating the laundering of these illicit gains is a threat to UK's prosperity, security and reputation both at home and abroad as it undermines the UK's efforts to build a cleaner global financial system.

4.9 Products and services from across the regulated sectors may be abused to facilitate the laundering of corruption proceeds. The continued use of effective enhanced due diligence measures on PEPs, their family members and their known close associates is therefore crucial.

4.10 The Financial Conduct Authority guidance on PEPs has remained unchanged since 2017, which sets out that PEPs who hold prominent public functions in the UK (and their family members and known close associates) should generally be treated as lower risk due to the Anti-Corruption regime in place

[4] A description of open-account trading can be found in 'Trade Finance Principles', Wolfsberg Group, 2019.

[5] 'Trade-Based Money Laundering White paper', Citi Group, 2016.

in the UK. However, firms are still required to apply more stringent approaches in cases of higher risks, including factors such as PEPs originating from countries without stringent Anti-Corruption measures in place. The government has been clear that financial institutions should continue to offer financial services to domestic PEPs and their families, and financial services should not be withdrawn solely because of this status.

4.11 In addition, we assess that wealth management, private banking, super prime property, as well as TCSP services are of the highest risk of being used to launder the proceeds of overseas corruption. Please see chapters 7, 11 and 12 for more detail.

Illicit financial flows

4.12 The UK's open and outward-facing economy, with its world-leading financial and professional services sectors and access to deep capital markets, means that UK businesses and banks create relationships and provide services across the globe. The strength of our economy makes it attractive for both legitimate businesses and criminals alike. It is vital that government acts decisively to prevent abuse of these sectors while ensuring that they continue to attract jobs and investment.

4.13 Government is committed to making our economy resilient to illicit finance. Illicit financial flows stifle economic growth, stable governance and the security of our global society. Here in the UK, illicit finance undermines our national security, weakens the integrity of our markets, and impairs investor and consumer confidence. In a global economy where money flows easily across borders, it is more important than ever that we work with our international partners to address weaknesses in combatting illicit finance both here and overseas and make us all safer.

4.14 In the Economic Crime Plan, government committed to further improving the understanding of the nature and impact of international illicit finance threats and delivering a shared understanding of the problems. The NRA supports this aim by articulating our understanding of where some overseas threats to the UK originate and how they manifest. A shared understanding of the threats allows more effective targeting and prioritisation of domestic and international action to mitigate the threats, both to the UK and globally.

4.15 This section thus outlines those jurisdictions assessed to be particularly relevant to the cross-border money laundering risks faced and posed by the UK. This section also notes some of the money laundering vulnerabilities these jurisdictions face domestically which, alongside the UK's vulnerabilities, may be exploited to enable illicit financial flows to and from the UK. While our assessment of the risks remains largely unchanged, key developments and changes since 2017 are highlighted in this section. Assessments by the FATF since 2017 have also contributed to an improved understanding of the risks the UK faces. [6].

[6] For more information on the work of FATF, and its assessment of the UK, see chapter 2.

China

4.16 A significant volume of proceeds of crime flow in and out of China annually, particularly through the use of informal value transfer systems (IVTS).[7] The legitimate use of IVTS is widespread throughout the UK, including within the Chinese diaspora in the UK. However, the prevalence of Chinese IVTS providers in the UK and other jurisdictions enables criminals to abuse these services to transfer illicit funds into and out of the UK and integrate them in the financial system, contravening China's strict currency controls. Many of these IVTS providers are operating illegally in the UK, as their services should be registered as an money service business (MSB), which means they are not abiding by the Money Laundering Regulations and makes them more vulnerable to criminal abuse.[8] Investigations have shown methodologies by criminals to launder funds through IVTS, by using criminally derived cash to settle separate and unconnected underground banking remittances to Chinese citizens in the UK. Payments by the Chinese IVTS provider into the recipient's UK account are frequently made in cash, broken down into a larger number of smaller amounts, and deposited via numerous branches which are geographically spaced out. Alternatively, payments are received from one or more bank accounts of other Chinese nationals, which are likely 'mule accounts'. Cash is often integrated and moved via 'mule accounts' held by Chinese students in the UK.[9]

4.17 The global desire for Chinese goods from all parts of the world also enables underground banking and other large-scale money laundering networks such as International Controller Networks[10] to broker and facilitate third party payments including to and from the UK, often under the guise of trade. Trade is also used to disguise UK-derived cash based money laundering, by paying cash derived from criminal activity into the accounts of persons carrying out a form of retail commerce known as Daigou, where goods in demand in China are purchased in the UK by Chinese citizens and exported to China for sale there, often in contravention of Chinese customs controls.[11]

4.18 Continued cooperation to prevent and pursue illicit funds transfers are therefore pivotal. The UK has been able to make progress with China in relation to certain proceeds-generating crimes and has established well-developed mechanisms for doing so. For example, HM Revenue & Customs (HMRC) has worked with Chinese authorities including China Customs to tackle the trade in high-risk commodities through joint exercises and the targeted exchange of data through initiatives like the UK-China Port

---

7 IVTS is a term often used to describe underground banking, by which we mean informal banking arrangements which run outside of the formal banking system. This type of banking involves the transfer of the value of currency without necessarily physically relocating it.

8 See case study 3 in the legal services chapter where HMRC intervention led to the conviction of a Chinese national for operating an unlicensed money-service business in the UK.

9 'Chinese Underground Banking', National Crime Agency, October 2019.

10 Criminals and OCGs that generate significant amounts of cash often use the services of cash controller networks that are capable of transferring vast sums of cash on their behalf. These international controller networks have the capacity to receive, hand over and transfer criminal proceeds, while charging a processing fee.

11 'Chinese Underground Banking', National Crime Agency, October 2019.

Twinning Arrangement. The UK has also established a UK-China Compliance and Transparency Forum which brings together representatives from the public and private sector to share experience and best practice on illicit finance related topics.

4.19 Prior to its evaluation by the FATF, China had already begun a number of reforms targeted at increasing its implementation of the FATF standards. This included conducting a National Risk Assessment of money laundering and terrorist financing risks and improving the ability to police its borders. These are welcome reforms which in the medium and long term will have a meaningful impact on addressing areas of weakness. The UK continues to work with Chinese authorities as they seek to address the deficiencies identified in the FATF Mutual Evaluation Report.

Hong Kong

4.20 Similarly to the UK, Hong Kong's established position as an international financial centre means it attracts not only legitimate investment from around the world, but also high-end money launderers who seek to conceal the criminal origin of proceeds of crimes occurring overseas, such as corruption and tax evasion, among the high volume of business transactions taking place daily, and integrate them into the financial system. Hong Kong continues to be used as a financial gateway into and out of mainland China for both legitimate and illicit funds. As a result of the significant business and financial links between the UK and Hong Kong, there are heightened risks of illicit funds also moving between our jurisdictions within these transactions. The FATF's assessment in 2019 confirmed that Hong Kong has a sound regime to fight money laundering and terrorist financing. However, there is more to do to enhance prosecution of money laundering involving crimes committed abroad including corruption and tax evasion, and to strengthen supervision of certain non-financial businesses.

Pakistan

4.21 The UK continues to have close economic links to Pakistan, including significant remittance flows between both jurisdictions, which according to estimates equated to approximately $1.7 billion in 2017.[12] These linkages also enable and disguise illicit funds to be transferred between the UK and Pakistan, including through illegal informal value transfers. Criminals continue to purchase high value assets, such as real estate, precious gems and jewellery to launder illicit funds which are transferred from Pakistan to the UK and vice versa. This includes proceeds from corruption and drug trafficking. The risk from cash-based money laundering from the UK to Pakistan via smuggled cash and MSBs also persists.

4.22 In 2018 Pakistan was nominated to the FATF's list of jurisdictions with strategic anti-money laundering and counter-terrorist financing (AML/CTF) deficiencies, known as the 'grey list', due to widespread CTF deficiencies. The FATF's regional body in Asia-Pacific also completed an assessment of Pakistan's AML and CTF system in 2019. Both processes highlighted the areas Pakistan is required to improve to create greater resilience and

12 'Bilateral Remittances Matrix 2017', World Bank, April 2018.

protection against the risks identified above. Pakistan failed to complete the FATF action plan resulting from their nomination to the 'grey list' by the required deadline of October 2019. While FATF acknowledged notable improvements in the months following, they also warned that should significant and sustainable progress not be made when next reviewed then the FATF could call on its members to advise their financial institutions to give special attention to business relations and transactions with Pakistan.[13] The UK, as a member of FATF, continues to closely monitor for sustained and timely efforts. The UK also continues to support Pakistan, including with capacity building assistance, to help Pakistani authorities meet their commitments. Joint operations between the National Crime Agency (NCA) and Pakistani authorities to tackle illicit finance threats have benefitted from good levels of cooperation. For example, in December 2019, the NCA negotiated a settlement with a Pakistani national to return funds and property valued at approximately £190 million to Pakistan. This success would not have been possible without the close cooperation between UK and Pakistan law enforcement agencies.

Russia

4.23 The UK continues to see a significant volume of Russian, or Russian-linked illicit finance channelled through the UK economy, through various regulated and unregulated sectors, including company formation and related professional services, as well as property. The UK's company formation mechanisms provide the necessary corporate vehicles for transferring funds through the international financial system and this is a vulnerability regularly exploited to move Russian-linked illicit finance into the UK. The Danske Bank Estonia money laundering scandal highlighted the ongoing popularity of UK legal entities for abuse by Russian money launderers, and emphasised how sectors may be exposed to these flows.[14] Banks for example, can be affected both via direct transactions their customers have with customers of affected banks and through funds they may clear as part of correspondent banking agreements with other banks. To manage this risk, the UK continues to encourage firms to take a risk-based approach in establishing and maintaining relationships with jurisdictions with higher levels of corruption.

4.24 The FATF's recent evaluation of Russia concluded that Russian authorities have an in-depth understanding of money laundering risks in Russia and strong utilisation of financial intelligence. However, it stressed the need for Russia to enhance its approach to supervision and the prioritisation of complex money laundering cases, especially in relation to cases involving the proceeds of corruption and other crimes that have been sent overseas to be laundered.[15]

4.25 In the UK this money is often invested in high end UK real estate, private school fees, luxury vehicles, and sometimes as donations to cultural

13 'Outcomes FATF Plenary, 19-21 February 2020', FATF, February 2020.

14 'The Case of Danske Bank and Money Laundering', Seven Pillars Institute, November 2019.

15 'Anti-money laundering and counter-terrorist financing measures – Russian Federation, Fourth Round Mutual Evaluation Report', FATF, December 2019.

institutions. These investments not only represent the end destination for this money but can also act as a mechanism for individuals to launder their reputation, improving their standing and influence in UK society. This poses a significant reputational risk for the UK as a global financial centre.

4.26 When countering the threat of illicit finance linked to Russia, UK activity focuses on key jurisdictions overseas that are used to facilitate the movement of Russian-linked illicit financial flows to the UK. Our approach is regional, rather than country specific and working with international partners to coordinate our response and improve our shared security is a core part of our approach. In addition, domestically, we continue to reinforce our ability to crack down on illicit finance, including that which is linked to Russia, in the UK through ground-breaking legislation and a strengthened law enforcement response. As part of its response to the Intelligence and Security Committee's Russia Report, the UK produced a more detailed response to Russia-related illicit finance.

United Arab Emirates (UAE)

4.27 The UAE – like the UK – is an established global financial centre and also a key regional trade and transport hub with strong links across the Middle East, South Asia and Europe. Given the ease of doing business, the open economy, and high quality of life on offer, it is an attractive location for those who also wish to launder the proceeds of crime from abroad – overwhelmingly foreign nationals using UAE systems, rather than Emirati nationals themselves.

4.28 The UAE recently underwent its Mutual Evaluation by FATF; the findings acknowledge the high-level commitment and significant progress made by the UAE since 2017 including improved AML legislation and regulation, the development of its first National Risk Assessment (NRA) of money laundering and terrorist financing risks, and improved domestic prosecutions for money laundering and terrorist financing. The FATF also identified vulnerabilities and has placed the UAE under observation. These deficiencies expose the UAE, and other countries, to abuse by international controller networks which continue to launder the proceeds of crime to and from countries including the UK. These criminal networks exploit features of the UAE's laws and systems, in order to move cash and gold easily into and out of the country, as well as engage in money laundering through the UAE property market, international trade, and newer areas such as cryptoassets.

4.29 The UAE continues to enact its programme of reforms to improve its AML/CTF regime in line with FATF's recommended actions. UK law enforcement agencies continue to support these reforms through close collaboration on capacity building, joint work on cryptoassets, and efforts to improve compliance in the MSB sector – affecting the UK and UAE equally. Additionally, the UAE authorities continue to cooperate with the UK to disrupt criminal activity originating in the UK and to pursue UK fugitives hiding in the UAE.

4.30 Recent cooperation includes the UK and UAE working in partnership to improve the effectiveness of a Money Service Businesses' AML controls and compliance framework, which have been used as an industry benchmark for

all UAE MSBs and reform within the sector. HMRC continues to work with UAE partners on this shared vision because some UAE MSBs also trade with the UK firms. As part of the collaborative partnership, Dubai Police acts as a critical friend assisting with enhancements to HMRC's programme of Anti-Money Laundering compliance.

4.31 The UAE Ministry of Interior (Federal Authorities) provided a number of pieces of pivotal intelligence, and participated at meetings in Europe and UK, which helped identify a global cash-smuggling network. This assisted UK criminal investigations and revealed hitherto unknown detail about the criminal methodologies involved, forming the basis for further international cooperation.

UK Crown Dependencies and Overseas Territories

4.32 The close economic ties between the UK's Home Nations, the Crown Dependencies (CDs) and its Overseas Territories (OTs) generate significant economic benefits for all in the form of jobs and business. However, criminals seek to exploit this close relationship and try to disguise illicit assets by taking advantage of existing channels and strong business connections. CDs and OTs continue to feature prominently in UK money laundering investigations and reporting.

4.33 To tackle this, since 2017 all CDs and OTs with financial centres participate in the Exchange of Notes arrangements for Information Sharing. The Exchange of Notes are bilateral arrangements under which they share beneficial ownership information on legal persons with UK law enforcement and other agencies within 24 hours (or 1 hour in urgent cases). Last year's statutory review found that these arrangements are working well and are providing UK law enforcement with rapid access to information used to support ongoing criminal investigations. During the first 18 months of operation, 296 requests were made under the arrangement, this equates on average to nearly 4 requests per week.[16]The UK is committed to further working with the CDs and OTs on increasing transparency about the ultimate beneficial ownership of companies registered in their jurisdictions. All 3 CDs, and all permanently inhabited OTs have committed to adopt publicly accessible registers of company beneficial ownership. The introduction of publicly accessible registers in these jurisdictions over the coming years will help mitigate any abuse, and further strengthen cooperation between the UK and the OTs and CDs.

4.34 Following recent FATF assessments, as well as improved information sharing under the Exchange of Notes arrangement since 2017, the UK now has a greater understanding of the risks of abuse faced by certain links between the OTs and the rest of the UK.

4.35 The British Virgin Islands (BVI) government was the latest to commit to introduce a publicly accessible register of beneficial ownership for companies by 2023, this is a welcomed step forward given the number of companies registered in that jurisdiction. Once implemented, ownership information

16 'Statutory review of the implementation of the exchange of notes on beneficial ownership between the United Kingdom, Crown Dependencies and Overseas Territories' Home Office, June 2019.

will provide transparency to businesses, the investment community and wider society, enabling them to better understand the companies with which they interact, helping to prevent their misuse. Offshore corporate structures are attractive to criminals due to the layer of legitimacy these structures may lend to criminal activity and associated illicit financial flows. Criminals use companies incorporated offshore to further mask beneficial owners of UK companies. Supporting the BVI in this commitment highlights the importance of continued close cooperation between the UK and BVI to pursue illicit funds, but also to prevent abuse and strengthen mitigations.

4.36 The BVI has substantive illicit finance and anti-money laundering legislation and its legislative framework is closely modelled on the UK standards. However, UK law enforcement has continued to observe the abuse of vulnerabilities in BVI's anti-money laundering regime by organised criminal networks with a UK nexus. In particular, this includes the involvement of UK[17] and BVI corporate structures set up to facilitate money laundering, indicating that greater actions are needed to prevent abuse in the future. The BVI government are currently working towards compliance with FATF standards ahead of their assessment and remain committed to the United Nations Convention against Corruption (UNCAC), having undergone a peer review on their compliance with UNCAC.

4.37 The BVI has already made significant progress in helping UK authorities to combat criminal activity and address these shared threats. They established the Business Ownership Secure Search System, under which beneficial owners must register with the BVI government. The Exchange of Notes arrangement has provided UK law enforcement with near real-time access to beneficial ownership information on legal persons registered in the BVI. Information provided by the BVI through this arrangement in 2018 supported the NCA's first Unexplained Wealth Order, which froze approximately £25 million. The risk should be further mitigated through increased investigations and prosecutions in line with BVI's risk profile, and supported by proactive risk-based supervision and increased engagement with the private sector to help prevent illicit finances entering the BVI.

4.38 The UK will continue to support all of the OTs and CDs to ensure they can adopt and implement the highest international standards, and reduce identified risks that would leave CDs, OTs and the UK exposed to greater levels of abuse if unaddressed.

The UK's response to international threats

4.39 The integrity of the UK as a global financial centre is essential for our international reputation and long-term prosperity. The FATF's assessment in 2018 found that the UK has a highly effective understanding of the threats it faces. However, there is more to be done to enhance the UK's domestic response to economic crime. To address the international dimension to money laundering the UK will continue to progress the necessary domestic reforms in order to improve our engagement operationally and at a strategic

[17] See chapter 11 for more information on the money laundering and terrorist risks of company formation and associated services.

level as a highly credible international partner in the fight against international illicit financial flows and economic crime.

4.40 Since publication of the 2017 NRA, the UK government has set out an ambitious international strategy in the Economic Crime Plan to enhance the global commitment and capacity to combat economic crime that will strengthen security, prosperity and the rules-based international system. This will be achieved through the delivery of 3 supporting objectives:

- maintaining and where necessary strengthening international standards, conventions and norms, and ensuring they are being effectively implemented;
- supporting sustainable development by strengthening resilience to economic crime and illicit finance; and
- protecting and promoting the UK's reputation.

4.41 Tackling international illicit financial flows is a top priority for the UK. It is critical in terms of reducing threats to the UK, protecting and promoting the UK's integrity as a global financial centre, and reducing the destabilising impacts of illicit finance on the wider world, particularly developing countries. Success on this agenda will underpin our support for the rules-based international system. Closer bilateral and regional cooperation on tackling economic crime can help improve collective defences, increase enforcement outcomes such as the recovery of proceeds of crime across international boundaries. Strong public private partnerships will help the private sector better understand and manage economic crime risks in high-risk jurisdictions and emerging markets, where there can be complex relationships and policy tensions to be managed. Many of the UK's international partners are following the UK lead by introducing public private partnerships in their own jurisdictions.

International Corruption Unit

4.42 In 2015, the UK established the International Corruption Unit (ICU) in the NCA, to recover stolen funds linked to the UK but stolen from developing countries and prosecute those responsible; and pursue UK companies and nationals who commit bribery and corruption overseas. The ICU is largely resourced through the UK's Official Development Assistance (ODA) budget. The ICU has returned assets totaling £199 million. In addition to £742 million worth of assets being restrained or detained globally and £7 million confiscated: a total of approximately £950m.[18]

International Anti-Corruption Coordination Centre

4.43 The International Anti-Corruption Coordination Centre, hosted by the NCA in London, brings together specialist law enforcement officers from multiple agencies into a single location to tackle to allegations of grand corruption. It is also resourced through the Official Development Assistance (ODA) budget.

[18] Figures provided by the NCA.

SOCnet

4.44 SOCnet is formed of 18 Home Office and Foreign, Commonwealth and Development (FCDO) policy officers based overseas. The policy officers are located in key regions across the globe, with dedicated illicit finance policy experts based in key financial centres. SOCnet regional coordinators operate in ten geographical regions supported by the Head of SOCnet who operates out of the Home Office. The network is largely funded by the ODA budget.

4.45 SOCnet's main objectives are to:

- improve shared understanding of the nature, drivers and challenges of tackling SOC upstream (including geo-political challenges).
- coordinate and enable a more strategic global response, including via the Joint Serious and Organised Crime platforms (JSOCs).
- influence policy with host governments and wider stakeholders to tackle SOC.
- build an effective global network to tackle SOC impacting on UK interests, and on poverty in developing countries.
- raise global standards and norms to tackle SOC both bilaterally and multilaterally.

4.46 The role of the Illicit Finance policy leads is to work with posts and partners across government to develop a single government response to illicit finance impacting on the UK within countries. They also work with interlocutors such as government, civil society, media, financial institutions and regulators using diplomatic engagement to lobby for greater transparency, legislative and policy changes, improved processes and greater political will to tackle illicit finance. They identify opportunities for bilateral or multilateral partnerships to drive change through developing global norms.

FCDO Illicit Finance Network

4.47 Beyond the SOCnet Illicit Finance network referenced above, FCDO is increasing its efforts to tackle international illicit finance with the aim to support a global financial system that works better for developing countries and minimises harm from international illicit finance. In order to achieve this FCDO is:

- establishing an overseas network of advisers embedded and supporting the wider HMG capabilities. The focus is on regional and emerging financial centres.
- establishing the International Centre of Excellence (ICE) - a global centre of expertise in understanding and tackling IF with capacity to offer draw down support to both the overseas network and wider HMG efforts.
- supporting HMG's domestic economic crime intelligence and analysis capability while leveraging this to support their development interests. This support is delivering the previous National Security Council commitment for FCDO to contribute £2 million ODA in 2019/20 to the NCA's economic crime uplift.

Overseas law enforcement liaison officers

4.48 There are in excess of 150 NCA officers located in 68 offices in 49 countries worldwide. Between them, the International Liaison Officer (ILO) Network has a coverage of over 130 countries.

4.49 ILOs are strategically located to help tackle the organised crime threat to the UK through collaboration with host nation law enforcement and intelligence organisations.

4.50 As the UK's lead agency to tackle money laundering, the NCA and the National Economic Crime Centre (NECC) are increasingly steering ILOs across the network to focus on money laundering and illicit finance, whether with associated predicate offences or as a standalone offence. ILOs drive a strategic approach to upstream law enforcement work, collaborating closely with HMG partners at post, and host governments to identify opportunities for the UK to contribute to strengthening of legislation, policy, and law enforcement operations in jurisdictions of risk around the world.

4.51 HMRC's Fiscal Crime Liaison Officers (FCLOs) are diplomatically accredited investigators based in UK Embassies and High Commissions around the world. The network currently consists of 41 officers in 32 posts, with strategic coverage of more than 100 countries. Their role is to disrupt and dismantle criminal attacks on the UK's tax system, through bi-lateral and multi-lateral engagement with host law enforcement partners, tax administrations and customs authorities. Although the FCLO's primary focus is on tax and customs risks, they are increasingly prioritising their efforts on associated money laundering risks and work collaboratively with other UK overseas liaison officers to share knowledge, expertise and legislative best practice on a range of common issues such as anti-money laundering, intelligence analysis and assessment, and asset recovery. By strengthening these legislative regimes in host countries, it increases collective resilience to transnational organised crime activity.

Chapter 5
Terrorist financing threat

UK threat level

5.1 The threat to the UK from terrorism was raised to 'severe' (an attack is highly likely) on 3 November 2020. Prior to this, the UK national threat level had been 'substantial' (an attack is likely) since 4 November 2019, this was the only period the threat level had not been 'severe' since August 2014, except for 2 increases to 'critical' (an attack is highly likely in the near future) in 2017, in response to the Manchester Arena and Parsons Green bombings, respectively.

5.2 In July 2019, the terrorism threat level system was updated to reflect the threat posed by all forms of terrorism, irrespective of ideology. This was in response to recommendations set out in the joint Police and MI5 Operational Improvement Review (OIR), conducted following the 2017 terrorist attacks. As a result, the UK national threat level now incorporates the threat from far-right terrorism and left-wing, anarchist and single-issue terrorism (LASIT)[1] in addition to Islamist terrorism and Northern Ireland-related terrorism (NIRT) in mainland Great Britain:

- Far-right terrorism encompasses ideologies adopted that can commonly be subdivided into cultural nationalism, white nationalism, and white supremacism. Although Islamist terrorism remains the greatest threat in the UK, far-right terrorism has evolved in recent years and is of growing concern both within the UK and across Europe. Since 2017, the police have disrupted 8 terrorist plots related to violent far-right extremist ideologies.[2]

- LASIT covers a broad spread of threat strands that sit outside of far-right terrorism: political left, anarchist, and single issue. For example, anti-state, animal rights abuses, environmental abuses, and anti-democracy.[3]

5.3 In line with the findings in the 2017 NRA, most terrorist attacks and plots in the UK continue to be planned by British residents. This includes the Fishmongers' Hall attack in November 2019, and Streatham attack in February 2020. We are continuing to see a trend towards lone actor, low-sophistication attacks, which are inherently harder to detect.

---

1 'Threat level system updated to include all forms of terrorism – news story', Home Office, July 2019.

2 'Fact sheet: Right-wing terrorism', Home Office, September 2019.

3 'CONTEST The United Kingdom's Strategy for Countering Terrorism', HM Government, June 2018.

Terrorist financing activity and scale

5.4 Terrorist finance activity in the UK remains varied and typically low-level in scale. There is no one method of financial activity associated with terrorism. The raising and movement of funds are not considered to be the primary aim for terrorists. Instead, terrorist finance activity continues to be for the purposes of sending small amounts to associates located abroad or for funding low-cost attacks. Recent attacks in the UK have not required external fundraising, using low-cost, low-sophistication methodologies

5.5 The methods used to raise terrorist funds domestically are predominantly through legitimate means (e.g. salaries and state benefits). Far less prevalent methods include fraud, abuse of mechanisms such as student loans, and abuse of the charitable sector. Compared with the overall size of the UK charity sector, the extent of known abuse for terrorist financing is low. Organised crime groups do not appear to have direct links to funding terrorism, apart from in relation to NIRT.

5.6 Methods used to move funds are opportunistic, and dependent on personal or shared knowledge and the end destination of funds. We continue to see terrorists using tried and tested methods to move funds, including physically carrying cash out of the country, bank transfers and the use of money service businesses (MSBs). We are also seeing a small growth in other methods such as cryptoassets, though it is highly unlikely that usage for terrorist purposes in the UK is widespread. These methods are discussed in more detail in subsequent chapters. Terrorists use methods that are easily accessible such as cash, debit/credit cards and gift cards to purchase items for attacks.

5.7 These methods are used to move the small amounts raised by UK-based individuals. These funds are primarily sent to relatives and associates located abroad with terrorist organisations, or to those formerly located with terrorist groups who may now be living within internally displaced persons (IDP) camps. It is suspected that these funds are used for general living expenses, as opposed to international attack planning.

International terrorism

5.8 Islamist terrorism emanating from Syria and Iraq, South East Asia and North, East and West Africa continues to be the most prominent threat to the UK and UK interests overseas. Terrorist groups based in these locations are often reliant on freedom of movement and local opportunities to generate and move funds. Sources of income are likely to be combinations of funds raised through extortion, robbery, donations and opportunistic business interests. This has become increasingly challenging for ISIL in Syria and Iraq since losing its physical hold of territories, having to adapt its sources and movement of income based on when and where opportunities arise.

5.9 We do not see funds entering the UK from hostile locations for attack planning.

Northern Ireland-related terrorism

5.10 The NIRT threat is driven by a small number of groups, who continue to pose an enduring threat. These groups aim to destabilise the framework for the

peaceful settlement of Northern Ireland's future, as set out in the 1998 Belfast Agreement. As a result, the terrorist financing threat in Northern Ireland is focused around the internal threat from violent Dissident Republicans (DRs).

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

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

5.13 Finance is assessed to be crucial to DR groups, but they do not require significant amounts of money to conduct small scale attacks. However, DR groups do require a regular income to sustain themselves, including to cover running costs (such as car, fuel, and other travel expenses), procure weapons and engineering components, and to sustain long-term attack campaigns. While some DR groups retain access to existing stockpiles of weapons and explosives, the majority needs to be purchased, or manufactured from component parts. A willing volunteer with access to a rifle or handgun and ammunition can also carry out an attack with little financial cost to his or her organisation however this is now rare. Longer-term, DR groups are having to look at more reliable funding streams in order to source firearms from organised criminal groups or to purchase commercially available precursors.

5.14 In October 2019 the Independent Reporting Commission's report on ending Paramilitary activity in Northern Ireland stated that "although there has been a downward trend in paramilitary violence over the last ten years, the number of deaths linked to paramilitary organisations and the number of paramilitary style attacks carried out between October 2018 and September 2019 increased. The situation, therefore, remains serious and concerning". The vague lines between organised crime, Paramilitary Groups, and terrorist funding in Northern Ireland continue to dictate how law enforcement responds to the risks. As predicate offences often fall under the category of

organised crime, the law enforcement response is more likely to address this activity through a proceeds of crime offence framework.

Far-right terrorism

5.15 Far-right extremists and terrorists likely utilise both traditional methods to fund their activities, such as the sale of merchandise, and innovative means, for example using emerging live streaming platforms to solicit donations via cryptoassets. Online donations of this kind are likely the principal source of external funding. However, most far-right extremist and terrorist activity is highly likely self-funded via legitimate means. Disruption by industry and law enforcement has highly likely motivated far-right extremists to utilise emerging and less regulated platforms, notably those associated with online gaming, to monetise their activism. While lack of funding probably limits extremists' ability to organise and promote their activities, it is unlikely a barrier to successful extremist activism owing to the low costs associated with online activism. The prevalence of online-focused activism and low associated costs will highly likely mean activity will remain self-funded and supplemented by donations from supporters.

UK government response

5.16 In 2018, the UK refreshed its Counter Terrorism Strategy, CONTEST. The aim of CONTEST is to provide a strategic framework to reduce the risk to the UK and its citizens and interests overseas from terrorism. The updated and strengthened CONTEST strategy reflects the findings of a fundamental review of all aspects of counter-terrorism and ensures we adopt the best response to the heightened threat in the coming years. There are 4 strands to CONTEST which provide the framework for all UK counter terrorism activity, these are more commonly referred to as the 'Four Ps':

- pursue: to stop terrorist attacks
- prevent: to stop people becoming terrorists or supporting terrorism
- protect: to strengthen our protections against a terrorist attack
- prepare: to mitigate the impact of a terrorist attack

5.17 As part of the CONTEST strategy we aim to detect, prevent, deter and disrupt the flow of terrorist finance alongside strengthening the UK's resilience and reputation as a leader in setting international financial regulatory standards. The UK's approach to responding to the threat focuses primarily through the operation of:

- intelligence Collection and Assessment: To enhance capability and detect emerging threats.
- investigation and Enforcement: To disrupt illicit activity and prosecute offenders.
- regulation and Supervision: To provide support and guidance to sectors at risk.

- Expanding and Enhancing Partnerships: To coordinate and identify opportunities to deliver shared objectives with the private sector and international partners collaboratively

5.18 International engagement and the provision of assistance to develop global counter terrorism financing strategies is an imperative part of our strategy. As a global leader, the UK plays a key role in sharing best practice in international fora, supporting the implementation of international disruption activity and driving the global agenda on countering the financing of terrorism. Independent evaluators have commended our response to the terrorist finance threat, reinforcing the UK's strategy as a form of best practice. This includes praise from the Financial Action Task Force (FATF), who in December 2018 awarded the UK the highest rating for how we tackle terrorist financing.

5.19 Chapter 2 further explains the legal, regulatory and law enforcement framework that applies to terrorist financing.

Chapter 6

Impact of COVID-19 on money laundering and terrorist financing

6.1 The outbreak of the COVID-19 pandemic has had a tremendous impact on countries and economies the world over. As government, society and businesses adapted, so has crime, including the way criminals may seek to launder profits from new and established types of criminality. Criminal groups have continued their operations despite restrictions, resulting in no significant drop in the illicit funds needing to be laundered. Businesses, supervisors and law enforcement however have remained alert, and cooperated closely to detect changes in methodologies and vulnerabilities that criminals may seek to exploit. The strong collaborative response has helped mitigate the overall risk of money laundering and terrorist financing to the UK, which has shifted but not increased as a result of COVID-19.[1]

6.2 The lockdown in the UK had a significant impact on the ability of money launderers to move cash across borders and led criminals to use other known methodologies such as cash via freight, use of cryptoassets or trade-based money laundering.

New threats and vulnerabilities

6.3 This section will provide a summary of how criminals have adapted their crime operations to take advantage of vulnerabilities that emerged in the wake of COVID-19, but also how their money laundering methods have shifted in attempts to continue to avoid detection where recent restrictions may have left their operations more exposed, or where methods have been restricted.

Predicate offences

6.4 Criminals committing predicate offences like fraud and cyber crime, have adapted their messaging to exploit fears of the pandemic[2] and to insert malware on personal computers or mobile devices.[3] There are a significant number of reports of COVID-19-related fraud, including online sales of fake

[1] As indicated by the steady number of Suspicious Activity Reports (SARs).

[2] 'Financial crime risk management and the COVID19 Pandemic: Issues for closer international cooperation and coordination', Institute of International Finance, April 2020.

[3] 'COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses', FATF, May 2020.

testing kits and personal protective equipment, appeals to support bogus charities and frauds targeting government financial support schemes.

6.5 The economic uncertainty and financial difficulties encountered by people and businesses likely increases the risk of crimes such as illegal money lending ('loan-sharking') and extortion.

Financial patterns

6.6 Established money laundering methods, including the use of money mule accounts, have persisted. Transaction and pattern monitoring continue to be an important line of defence. However, financial patterns did change due to restrictions to prevent the spread of COVID-19. Remote transactions have increased owing to branch closures of financial institutions or reduced operating hours. As the crisis evolved, cash withdrawals increased in some parts,[4] while falling confidence in the formal financial sector and stock markets triggered transfers of funds from securities. On the other hand, online commerce, payments, and transfers to different regions increased. These spikes in virtual money movements are an attractive way for criminals to obfuscate movements of cash-based criminal activity online.[5]

6.7 Increases in mobile banking, e-payments and cash stockpiling linked to suspicious activity by organised crime groups (OCGs) have been observed since the introduction of lockdown measures. Indeed, criminals may seek to use the pandemic as a potential justification for unusual account activity, including transfers to high-risk jurisdictions, or payments to and from multiple new beneficiaries, as well as cash deposits under the pretence of holiday, house or car purchase cancellations.

6.8 It is a realistic possibility that criminals' increased use of non-cash and mobile payment solutions may remain even after restrictions are lifted. Similarly, criminal use of cryptoassets was already on the increase prior to COVID-19, and as a result, OCG interest in cryptoassets as a means of laundering proceeds of crime is now likely to increase even further.

6.9 The decrease of international students residing in the UK, due to the pandemic, may have led to a reduction in activity through those types of mule accounts. Instead, informal value transfer operators and launderers may increasingly be setting up business mule accounts to use them for layering of funds. OCGs may also coerce vulnerable individuals into becoming money mules, with such instances having been observed in the US. The increase in home working is likely to aid recruitment of money mules, getting more people involved in money laundering schemes.

Businesses, trade and the economy

6.10 Criminals are likely to continue to invest and attempt to obfuscate their illicit gains in legitimate business. The changing business and trading environment

---

4 'Financial crime risk management and the COVID19 Pandemic: Issues for closer international cooperation and coordination', Institute of International Finance, April 2020.

5 Ibid.

may present attractive opportunities that OCGs may seek to exploit, and increases the risk for these sectors.

6.11 Many businesses have dealt with significant losses during the lockdown, while some businesses that are able to trade saw increased turnover. Lockdown restrictions have made it easier to spot suspicious account activity, where business that should see no, or reduced transactions are continuing to receive large (cash) deposits.

6.12 Criminals may also exploit the current distressed business environment by seeking to invest their illicit funds in struggling businesses, obtaining real estate sold out of desperation or bankruptcy.[6] OCGs may also look to invest liquidity in small and medium sized enterprises (SME) which cannot obtain funds elsewhere.[7] Professional services sectors are encouraged to be vigilant of such instances. There could be instances where criminals have sought to set-up companies simply to commit COVID-19 related fraud, and there are risks related to Companies House's lack of statutory powers to be able to stop suspect company registrations. While this practice pre-dates COVID-19, the pandemic has accentuated this risk. Planned Companies House reforms will help mitigate against these risks in the future. See Paragraph 11.30 for further information.

6.13 The increased demand for certain goods and services to combat the spread of COVID-19 presents additional trade-based money laundering (TBML) risks. Supply chains have also been disrupted, necessitating a pivot to new and potentially unfamiliar clients, increasing the risk of fraud and or money laundering for trade nationally and internationally.[8]

6.14 Criminals may also look to increase property purchases as a method to launder and increase their wealth, particularly while bank interest rates are low, and sellers may be more willing to accept much lower offers.[9] Likewise, there is a risk that criminals will exploit the increase in COVID-related charity donations and appeals to launder funds or commit fraud.

Cross border

6.15 The UK's lockdown and travel restrictions made it more difficult for launderers to move cash across borders and to integrate it into the legitimate financial sector. It is highly likely that fluctuations in travel restrictions linked to COVID-19 will lead to further surges (in the case of restrictions easing) or decreases (in the case of restrictions tightening) in criminal cash being moved out of the UK via passengers.

---

6 'COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses', FATF, May 2020.

7 'Financial crime risk management and the COVID19 Pandemic: Issues for closer international cooperation and coordination', Institute of International Finance, April 2020.

8 Ibid.

9 See related news stories https://www.propertyinvestortoday.co.uk/breaking-news/2020/4/revealed--why-are-hnwis-from-developing-markets-looking-to-invest-in-european-assets, https://www.propertyinvestortoday.co.uk/breaking-news/2020/4/revealed--chinese-interest-in-uk-residential-property-soars-despite-covid-19.

Terrorism financing

6.16 Terrorist groups may use the COVID-19 crisis to raise or move funds, including by increasing their illicit activities to raise funds.[10] They may also use the crisis to raise funds by moving into new COVID-19 linked criminal activity, while economic sanctions targets may seek to take advantage of disruptions and changes to supply chains to evade financial institutions' compliance systems.[11]

Impact on AML/CTF system

6.17 COVID-19 restrictions have undeniably affected all parts of the anti-money laundering/counter-terrorist financing (AML/CTF) system, requiring a concerted effort by reporters, supervisors and law enforcement to adapt.

6.18 The changes are assessed to have had some impact on the regulated sector's ability to carry out AML/CTF activity. The regulated sector must continue to implement their AML/CTF obligations and have been able to provide supervisors with requested information, however their operational workforce may have decreased due to remote working, self-isolation and shielding requirements. Restrictions on non-essential travel have also affected firms' abilities to use traditional methods to verify customer's identity and to carry out face-to-face customer due diligence (CDD). This will continue to be limited as restrictions are eased and is likely to further accelerate the shift towards greater online customer interactions that was already taking place across all sectors. In some sectors, such as land-based gambling, COVID-19 forced complete closure during initial lockdown and therefore mitigated any risks. Firms are reminded that the regulations are risk-based, enable risk sensitive judgements to be made and provide firms with a measure of flexibility in how they carry out their legal obligations. Several AML supervisors have supported this by providing guidance to aid understanding, such as the broad set of options available around client identity verification.[12] There is a risk that where supervisors have requested firms to undertake remedial work, some firms may need to delay related workstreams owing to other pressures in the system. This could perpetuate weaknesses in the system further, which criminals would seek to exploit.

6.19 Impact on supervisory activity has been limited. Supervisors are seeking to maintain business-as-usual and some have adapted their activity by substituting scheduled on-site visits with desk-based assessments. Supervisors are continuing their enforcement activity; investigations continue and have not been halted due to the pandemic. All other activity continues as normal, with limited impact due to staff working remotely. Some firms registering with supervisors may however experience delays in the completion of the registration process. There have been significant challenges for firms and supervisors but the Government is encouraged by

10 'COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses', FATF, May 2020.

11 'Financial crime risk management and the COVID19 Pandemic: Issues for closer international cooperation and coordination', Institute of International Finance, April 2020.

12 For example, see websites of the the FCA or the ICAEW for their guide.

the actions they have taken to ensure the UK's preventative regime remains operational.

6.20 All of the UK Financial Intelligence Unit's (UKFIU) domestic and international functions continue to be operational, with some refocussing of activity on abuse of the current situation by fraudsters and other criminals. Despite this, operational casework continues with the impact of COVID-19 measures assessed to be low.

6.21 The outbreak of the pandemic has had the most significant impact on courts and court time, where prosecutions had to be postponed or delayed due to the suspension of trials, hearings, and other in-person proceedings. This initially had some impact on investigators being able to obtain account information, and caused significant delays to Proceeds of Crime Act hearings, where it was not possible to do these via telephone listings or video-link. Likewise, this has impacted the ability to conduct interviews as part of civil recovery investigations. This impact is likely to be felt over an extended period of time due to a backlog of cases and the requirement for social distancing in court rooms, which will likely decrease the rate of prosecutions and convictions over the next 12 months.

Cross system response and mitigations

6.22 Government, law enforcement and the private sector have responded and cooperated in a timely manner to minimise risks and the impact resulting from the COVID-19 outbreak, through a risk based whole system response. Information on COVID-19 related financial crime and threats have been shared routinely and will continue to be as new risks emerge or as criminals change their approach. This collaborative response has limited the impact of emerging threats and vulnerabilities, meaning the overall money laundering and terrorist financing risk to the UK has not increased as result of COVID-19.

6.23 Regulators and supervisors have worked swiftly to issue guidance to the regulated sector, providing advice on issues where COVID-19 may cause disruption to usual processes, emphasising the use of a risk-based approach.[13]

6.24 In April 2020, the UKFIU introduced 3 new Suspicious Activity Report Glossary Codes in relation to criminal exploitation of the COVID-19 pandemic. This has helped both reporters and law enforcement agencies distil the information on suspicious transactions linked to COVID-19 criminality more quickly.

6.25 The response to the pandemic also saw the creation of the COVID-19 Fusion Cell, which is a joint public/private partnership, led by the National Economic Crime Centre (NECC) and financial institutions, which brings together banks, trade bodies, and the insurance sector, as well as UK law enforcement and the wider public sector. The Cell builds on the Joint Money Laundering Intelligence Taskforce model, regularly sharing information in order to

[13] For example, see Gambling Commission research on 'risks arising from Covid-19'.

identify changes in the economic crime threat and changes in criminal behaviour linked to COVID-19 and working across sectors to advance a response. Based on their assessment, additional types of suspicious activity to monitor are communicated to the regulated sector. The Cell is also used to identify areas for targeted intervention against criminal behaviour, while the NECC can task intelligence packages to the appropriate law enforcement agency for action.

6.26 In support of the NECC's sharing of COVID-19 related intelligence, the Cabinet Office Counter Fraud COVID-19 Response Unit set up an intelligence function that shares intelligence across government departments. This improved awareness of the threats during the crisis and allows departments to coordinate their response to known threats. There have been a number of successes where intelligence has informed the government's response and identified fraud. This shows the importance of proactively sharing intelligence across government and law enforcement to proactively prevent or identify vulnerabilities that may need thorough investigation.

6.27 The Cabinet Office's COVID-19 Response Team has also been working with departments to guide and support their counter fraud response to prevent COVID-19 schemes being abused by criminals. Connecting intelligence between government departments delivering COVID-19 schemes allows informed decision making based on threats. This involved risk assessing all ~120 government stimulus schemes, embedding qualified fraud risk resources to conduct detailed fraud risk assessments with departments and also setting up squads to focus support on specific government schemes to advise on fraud risk and counter measures that could be implemented to mitigate identified fraud risk. The team has also developed products that Departments can use to increase visibility of transactions such as the Experian Bank Account Verification Checker. This tool has already identified up to £53.5 million in potentially irregular payments identified for further investigation and made £1.15 million in confirmed savings (figures subject to audit). Never before has the counter-fraud function come together in this way to tackle fraud.

Chapter 7
Financial services

Financial services risk scores		
	2017 Risk Score	2020 Risk Score
Retail Banking		
Money Laundering	High	High
Terrorist Financing	High	High
Payment Services and electronic money		
Money Laundering	Medium	Medium
Terrorist Financing	Medium	Medium
Wholesale Banking		
Money Laundering	High	High
Terrorist Financing	Low	Low
Wealth management & private banking		
Money Laundering	High	High
Terrorist Financing	Low	Low

Summary and risks

- The scale and complexity of the UK's financial services sector continues to make it attractive for criminals and corrupt elites seeking to launder the proceeds of crime among huge volumes of legitimate business.
- The money laundering risk remains largely unchanged since 2017 across many of the sub-sectors of financial services previously examined. However, the growth and integration of financial technology firms presents criminals with new intermediaries and methods to abuse this sector. The risks arising from financial technology are considered throughout this chapter, alongside risks stemming from traditional financial services. Criminals will remain vigilant to exploiting any new financial service that provides a means to conceal criminal activity. Owing to greater understanding of the risk posed by cryptoassets, they are considered separately in chapter 8.
- Understanding of how financial services can be exploited has also developed further since 2017, including understanding how diversification in the retail banking sector can impact money laundering and terrorist financing risks, as

well as deeper insight into abuse of capital markets. However, intelligence gaps remain due to complex criminal methodologies and the great variety of business models across the sector.

- The terrorist financing risk is also largely unchanged since 2017, with the risk within the retail banking sector remaining **high**. In line with the money laundering assessment, financial innovation has brought new vulnerabilities that may be at risk of abuse for the purposes of terrorist financing. The nature of the domestic terrorist financing threat continues to pose particular challenges for detection and prevention by law enforcement and the financial services sector.

Retail banking

7.1 Retail banking services continue to be assessed as **high** risk of being abused for money laundering. Criminals continue to target retail bank accounts, which can be used to facilitate the rapid transfer and layering of criminal proceeds. Those that accept cash deposits face the highest risk.

Personal current accounts

7.2 The personal current account (PCA) market has continued to diversify since 2017. Although traditional high-street banks retain over 80% of the PCA market, several new challenger banks[1] have entered the market since 2017 and achieved widespread popularity. This has given criminals a greater number of products they can look to exploit for money laundering.

7.3 There is some limited evidence of the risks presented by challenger banks, including open source reporting of vulnerabilities in money laundering controls within several European challenger banks. However, overall, we assess there are only limited differences in the inherent risks represented by challenger banks, compared with traditional retail banks. All banks are required to carry out customer due diligence (CDD) checks, though criminals may be attracted to the fast onboarding process challenger banks advertise, particularly when setting up money mule networks. In addition, where banks promote the ability to open accounts very quickly to attract customers, there is a risk that information gathered at the account opening stage is insufficient to identify higher risk customers.

7.4 The last 2 years have seen an increase in the number of suspicious activity reports (SARs) filed relating to suspicions of money laundering through accounts held with challenger banks.[2] There has been significant growth in Defence Against Money Laundering (DAML) SARs from financial technology (fintech) start-ups offering a range of digital and mobile banking services. DAMLs from challenger banks suggest a more cautious approach to the risk of prosecution than the major banks. Further, threshold exemptions in the Proceeds of Crime Act (POCA) 2002, s.339A are only applicable to institutions who fall under the definition of deposit-taking bodies, which

[1] Although there is no universally agreed definition of challenger banks, these banks aim to reduce the market concentration of traditional high street banks through the use of technology and more up-to-date IT systems. Some may be more established, although others are smaller, recent entrants to the retail banking market, including some digital/online only banks.

[2] 'Suspicious Activity Reports (SARs) Annual Report 2020', NCA, November 2020.

may account in part for high volumes of low value DAML SARs from these institutions. Within the DAML process re-design we are undertaking in-depth analysis, which will include reviewing low value DAMLs, the use of threshold provisions and requirements for system change going forward.

7.5 The use of online banking continues to grow. As a consequence, banks are increasingly reliant on technology to detect criminal activity as face-to-face contact with trained staff declines. In 2018, 72% of UK adults used online banking[3] and 48% used mobile banking,[4] an increase of 7% compared to 2017. Most internet, mobile or telephone banking payments are now also processed using the Faster Payments Service (FPS). The number of remote banking payments processed via the FPS increased to £20 billion between 2017 and 2018.[5] These trends will make it increasingly easy and quick for criminals to obfuscate an audit trail of funds.

Money mule networks

7.6 Mule accounts remain a method used by criminals to launder the proceeds of crime, aided by the continued growth of social media and encrypted messaging. More than 40,000 cases of suspected money mule activity were reported in the UK to the fraud prevention organisation Cifas in 2019.[6] One mule network receiving the profits of a UK based drugs OCG, has been identified as paying more than £1.8 million in criminal cash into mule accounts in London high street banks. This was just over a 2- week period. There have been examples of children as young as 13 or 14 being approached in school playgrounds to act as mules. It is assessed that children are being targeted due to their naivety, attraction to earning quick cash and peer pressure.

7.7 Third-party deposits are often exploited to facilitate mule activity. This was the case in one large-scale investigation to tackle student accounts being used for third-party deposits. Through the Joint Money Laundering Intelligence Taskforce (JMLIT), a bank notified law enforcement of this methodology, which utilised the bank's Automated Services Devices (ASDs). The bank requires a depositor to be a bank customer, i.e. they hold an account with the bank, before cash can be credited to an account via an ASD. However, the facility then allows the depositor to credit any account of a customer of the bank. This facilitates the payment of cash into a large number of accounts held by the bank through one set of credentials without any of those funds being registered, assigned or recognised as being related to the customer making the deposit. The credentials being used are not capable of being subject to any kind of compliance checks to verify correct ownership/possession at the time the deposit is being made.

7.8 As part of the subsequent investigation, 95 Account Freezing Orders were obtained, freezing approximately £3.3 million, the majority of which has

---

3 'Payment Markets Report 2019', UKFinance, June 2019.

4 'Rise in mobile banking and contactless as consumers take pick 'n' mix approach to payments – Press release', UK Finance.

5 'Payment Markets Report 2019', UKFinance, June 2019.

6 Cifas, 2019.

since been successfully forfeited or returned. Some of the funds remain under investigation. The bank has also withdrawn third-party cash deposits.

Business accounts

7.9 Business bank accounts are also used for money laundering. The expected turnover of these accounts makes it easier to disguise high volumes of illicit funds. These accounts are used in trade-based money laundering schemes, which typically involve sums in excess of tens of millions of pounds disguised as business transactions, as well as in tax evasion schemes. The evolution of new payment service and e-money firms (as outlined in paragraphs 7.16-7.19 below) can have indirect consequences for the retail banking sector too. For example, where banks provide bank accounts to these businesses, they can then be used by the payment service firm or e-money firm to facilitate their own customers' transactions, much like a money service business (MSB). As a result, the bank providing the original account becomes one-step removed from the customer. The extra layer results in the retail bank being unsighted on all transaction details of those benefiting from their facilities. This underlines the importance of the obligation on banks to understand their exposure and be satisfied that such business clients have adequate controls in place.

Alternative banking platforms

7.10 Alternative banking platforms (ABPs) [7] are also at risk of money laundering. ABPs are a form of shadow banking that make use of bespoke online software to provide banking services, without regulated and audited know your customer (KYC) checks. They are an effective way to transfer the ownership of money at scale and provide banking services, without being reflected in traditional banking transactions. There appear to be no advantages for users of ABP websites other than to avoid regulatory compliance protocols and provide layers of complexity around transactions. It is assessed that most financial transactions are linked to criminal funds and users are linked to a range of criminal activity. ABPs can be structured in such a way as to be multi-jurisdictional, increasing the complexity of the transaction chains, while undermining law enforcement's ability to proactively identify transactions or dismantle the ABP network.

Terrorist financing

7.11 Due to its scale and widespread use in low-level financial activity, retail banking continues to be one of the primary means by which funds are moved and stored within the UK; this puts it at a **high** risk of terrorist financing. The universal nature of retail banking, ease of access, frequency and speed of transactions make the sector particularly vulnerable to abuse for terrorist financing purposes. Over the period 2017 to 2020, banks submitted by far the greatest proportion of terrorist finance SARs

7 Law enforcement understand there are 3 key requirements for an ABP to function: i) the software, ii) a front company which would justify large amounts of money being transferred to and from it, and iii) a linked bank account. The process as currently understood is; The ABP software program, accessible via a web portal, is linked to a bank account. The ABP software routes transactions through various accounts creating a layering process before the money reaches its intended destination. A fixed charge or commission, usually much higher than those charged by conventional financial institutions, is charged by the ABP to the account holder.

disseminated to the National Terrorist Financial Investigation Unit (NTFIU) and Counter-Terrorism Units, relative to other sectors.[8]

7.12 In line with the findings in the 2017 NRA, domestic terrorist financing activity predominantly involves low levels of funds, often raised through legitimate means (e.g. salaries or state benefits), used for costs related to attack planning, general living expenses, or sent to associates located overseas with terrorist groups. Since 2017, there has been a shift in the domestic threat picture, with an increase in low-sophistication terrorist attacks that are relatively inexpensive to mount, committed by lone actor individuals or known associates.

7.13 A National Crime Agency (NCA) review of SARs in relation to the 2017 attacks confirmed that in line with the general population, electronic bank transfers and cash were consistently the most reported ways those associated with terrorism move their money; however, these are not necessarily terrorist funds, and are usually just personal living expenses. The efficiency of electronic transfers combined with the size of the retail banking sector, enables low-value transactions to blend in and avoid unwanted attention, making this method particularly attractive for terrorist financing.

7.14 Similar to the findings of the 2017 NRA, terrorists have been observed to raise funds through the banking system, including by illicit means such as card fraud or loan fraud, or legitimate means such as use of credit facilities. However, this is rarely to raise funds for terrorist activity; rather, these individuals are likely to be conducting fraud for their own financial gain, and activity may predate suspected terrorist behaviour.

7.15 There are a number of emerging risks related to the retail banking sector that individuals could exploit: the growth of faster customer on-boarding, an increase in the outsourcing of CDD to non-UK companies unfamiliar with the UK risk landscape, greater reliance on technology, and less face-to-face interaction. Further, while the flow of individuals to conflict zones (such as Syria and Iraq) has reduced since 2017, there is a small emerging threat that Foreign Terrorist Fighters may seek to return to the UK. These individuals could re-open dormant personal bank accounts, open new accounts, or elicit payments from UK-based associates to fund their return.

Payment and electronic money services

7.16 In 2017, the financial technology section of the NRA featured the risks from emerging market entrants in the financial services sector such as cryptoassets (previously referred to as digital currencies), crowdfunding and payment services like, electronic-money (e-money). Since 2017, there have been considerable developments to improve understanding and respond to money laundering and terrorist financing risks associated with cryptoassets, outlined in more detail in chapter 8. We have seen no evidence of changes

[8] Banks submitted SARs accounting for 59.04%, 64.57% and 71.65% of total terrorist financing SARs over the last 3 reporting periods from 2017 to 2020 respectively , 'Suspicious Activity Reports (SARs) Annual Report 2018', NCA, November 2018, 'Suspicious Activity Reports (SARs) Annual Report 2019', NCA, November 2019 and 'Suspicious Activity Reports (SARs) Annual Report 2020', NCA, November 2020.

in the risks identified by 2017 NRA concerning crowdfunding. This sub-section will therefore explore regulated payment services and e-money alone.

7.17 Overall, payment services and e-money services are considered at **medium** risk of money laundering. This is owing to the continued diversification of products and platforms available, providing criminals with more options to control and move funds, often across borders. In 2018 alone, there were 708 million payments made using "other" payment methods,[9] outside traditional forms such as Bacs Direct Credit Payments. This includes firms in scope of the Payment Services Regulations 2017, such as Payment Initiation Service (PIS) providers.[10] The EU Revised Directive on Payment Services (PSD2) introduced new "Strong Customer Authentication" in regard to electronic payments, which will help to reduce the risk of fraudulently authorised payments. However, the business models of payment service providers continue to mature and evolve, making it difficult to detect and identify money laundering methodologies, compared with criminal activity using traditional retail banking services. Likewise, mitigations in the sector are variable (see paragraphs 7.38-7.39 for more details). Therefore, the money laundering and terrorist financing risks of such business operations will need to be monitored closely as this sub-sector develops further.

7.18 Despite loading limits, pre-paid cards continue to be used to launder funds, including in the most serious of offences, such as modern slavery. In this type of crime, offenders use pre-paid cards to launder profits by placing value onto cards either through cash purchases or by bank transfer. The cards are then used for business expenses and personal spending. The cards are physically moved abroad with little risk of detection or the funds are used for online purchases abroad which do not require movement. They are not currently classed as a listed asset or cash and therefore, cannot be seized under POCA.

7.19 Open source reporting also suggests that the appeal of UK e-money institutions is increasing to money launderers looking to move illicit funds in and out of Russia and Eastern Europe.[11] This is likely in response to a crack-down by Baltic banks after several laundromat scandals. The scale of such abuse is unclear and will need to be monitored closely.

Terrorist financing

7.20 Payment services continues to face a **medium** risk of terrorist financing, with evidence that terrorists have used pre-paid cards to store and move funds. Pre-paid cards are attractive for terrorists as they are a simple and discrete way to make low value payments.

---

9 'Payment Markets Report 2019', UKFinance, June 2019.

10 Payment Initiation Service (PIS) providers enable consumers to pay companies directly from a bank account rather than supplying debit or credit card through a third-party such as Visa or MasterCard. A PIS provider needs a customer's explicit consent before providing this service.

11 See www.opendemocracy.net/en/dark-money-investigations/will-e-money-boom-make-uk-hub-money-laundering/.

Wholesale banking

7.21 The money laundering risk from wholesale banking[12] is **high**. All wholesale banking services are vulnerable to abuse because criminals can exploit the complexity of the services' financial arrangements, which usually span multiple jurisdictions, to conceal their laundering activity. However, the complexity and lower accessibility of wholesale banking, compared to retail banking, may limit its abuse.

Capital markets

7.22 The UK's 2017 NRA identified money laundering through capital markets as an emerging risk. The capital markets continue to offer a route for criminals to move and disguise the audit trail of money through the use of complex financial transactions. Furthermore, these can be hidden by the large volume of legitimate business in this sector. On the London Stock Exchange alone, there were over 20 million trades reported in May 2020, at a value of £93 billion. Likewise, money market trades generally clear in less than a day and foreign exchange and equity trades clear in two. This demonstrates the ease with which experienced money launderers could hide large volumes of illicit transactions.

7.23 Our understanding of the inherent risks in the sector has improved since 2017, though the scale of money laundering through the capital markets remains unclear due to the difficulties in identifying it among the huge volume of transactions. As a result, understanding of the scale of abuse is mainly based on historic data and investigations.

7.24 The Financial Conduct Authority (FCA) and industry are continuing to build their understanding of risks in capital markets particularly through the JMLIT Money Laundering Through the Markets Group.[13] There has also been a 28.7% increase in the number of SARs filed under the "capital markets" glossary code between the 2017 to 2018 and 2019 to 2020 periods, potentially indicating an increased understanding and identification of the typology by firms.[14] The FCA continues to improve their knowledge of the risks through further data analysis too. However, the mirror trading scheme involving Deutsche Bank identified in the 2017 NRA, continues to be one of the few corroborated typologies demonstrating illicit funds being laundered through the UK's capital markets.

Correspondent banking

7.25 Correspondent banking relationships[15] continue to be assessed at a high risk of money laundering. The vulnerabilities in relation to correspondent

---

12 Wholesale banking refers to banking services sold to large clients. For the purposes of NRA 3, it includes capital market services and particularly secondary market activity, where shares, derivatives, bonds and other instruments are traded, as well as trade finance and correspondent banking.

13 'TR19/4: Understanding the money laundering risks in the capital markets', FCA, June 2019.

14 'Suspicious Activity Reports (SARs) Annual Report 2020', NCA, November 2020, and 'Suspicious Activity Reports (SARs) Annual Report 2018', NCA, October 2018.

15 Correspondent banking is the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank). Respondent banks may provide a range of services, including cash management (e.g. interest-bearing accounts

banking are well understood, such as the wide-spread exposure to high-risk jurisdictions, and the lack of oversight banks often have of every party involved in a chain. The FCA continues to see cases where UK banks have been exposed to money laundering through relationships with respondent banks, including overseas entities in non-EEA countries. While some countries may have similar anti-money laundering/counter-terrorist financing (AML/CTF) standards and supervisory regimes to the UK, the application of standards to address risks in relation to correspondent banks is not consistent across all countries. Criminal networks continue to seek out these locations to introduce illicit proceeds into the financial system.

7.26 Law enforcement has also seen evidence of abuse of the Faster Payment Service (FPS). Criminally complicit international banks have used their correspondent bank accounts in the UK to receive payments via the FPS for their overseas clients. These are then consolidated and transferred out of the UK.

7.27 UK banks' understanding of the money laundering risks associated with correspondent banking has meant UK banks have continued to reduce the number of correspondent relationships. The Committee on Payment and Market Infrastructures of the Basel Committee (CPMI) has reported that correspondent banking relationships have shrunk 20% between 2011 and 2018.[16] While this has decreased the risk since 2017, the de-risking trend continues to pose wider risks by shifting correspondent relationships into "nesting" relationships (accessing correspondent banking via another bank) and other forms of cross-border payment methods.

Terrorist financing

7.28 While wholesale banking overall is considered to be at a **low** risk of abuse for terrorist financing, correspondent banking continues to be vulnerable due to the complex and international nature of the banking relationships involved. While banks' risk appetites for correspondent relationships have continued to decline, data suggests that the need for correspondent services has not. This could lead to an increased use of less well-regulated and therefore higher risk methods to facilitate international transactions, including terrorist finance transactions (see correspondent banking section above and chapter 15 for more details).

Wealth management and private banking

7.29 Wealth management services continue to be at **high** risk for money laundering.[17] The sector's exposure to the proceeds of political corruption

in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services. As identified by FATF, banking relationships that are higher risk typically are cross border correspondent banking relationships involving the execution of third-party payments.

16 'On the global retreat of correspondent banks', BIS, March 2020.

17 This NRA defines wealth management using JMLSG's Chapter 5 Part II definition: "The provision of investment services including advice, discretionary fund management and brokerage to private investors, ranging from the mass affluent to high and ultra-high net worth individuals. Some wealth managers are parts of banks or private banks and may also provide banking services to the same clients.".

and tax evasion, particularly impacting wealth managers that have a global footprint, continues to make wealth management vulnerable to money laundering. 78% of wealth management firms count politically exposed persons (PEPs)[18] among their customer base.

7.30 Wealth managers may unknowingly enable criminals to invest proceeds of crime in legitimate products, with the legitimate investment return further cleaning and obfuscating the original illicit source. Furthermore, criminals continue to infiltrate and subvert the sector, including through family offices. These appeal to criminals as they offer high levels of privacy as well as offering a veneer of legitimacy through the obfuscation and legitimisation of sources of funds and wealth. Many family offices that operate in the UK are not required to be regulated. It is likely that many lack internal scrutiny as family offices and their employees will not necessarily be legally required to monitor and report wrongdoing.

7.31 Since 2017, there has been a rise in the accessibility and advertisement of retail investments through exchanges, platforms or advisors. In part, this is likely due to the increased customer base resulting from pension freedom rules introduced in 2016. Greater awareness and accessibility of these services could increase their risk of money laundering, though the current scale of abuse is unclear. It could also be difficult to detect money laundering as their traditional customer base diversifies.

7.32 Wealth management and private banking is considered to be at a low risk of abuse for terrorist financing.

Insurance

7.33 The insurance sector continues to be unattractive for money laundering. This is likely because the design of both general and life insurance products makes it difficult and unattractive for criminals to layer the proceeds of crime at speed. Criminals also have to provide significant personal information to inform an insurer's risk-based assessment during on-boarding, which may be a further deterrent. The international nature of the London insurance market increases the sector's exposure to providing cover in high-risk jurisdictions, trades or industries. However, the insurance sector remains at greater risk of abuse from other types of economic crime, particularly orchestrated fraud.

Supervision, compliance and law enforcement response

Economic crime governance

7.34 The Economic Crime Plan published in July 2019 provides a collective articulation of the actions the public and private sectors have committed to undertake. The interventions committed to in the Plan have already helped

[18] The UK's Money Laundering, Terrorist Financing and Transfer of Information on the Payer Regulations define a PEP as "an individual who is entrusted with prominent public functions, other than as a middle-ranking or more junior official."

mitigate money laundering and terrorist financing risks in the financial sector. For example, public-private threat updates (PPTU) have led to the sector developing an improved understanding about the money laundering risks it faces. The PPTUs are strategic assessments which draw upon both private sector data/intelligence, and that of law enforcement, civil society and government. This provides richer findings than relying upon law enforcement data sets and understanding alone. The SARs reform programme has also helped through the increased capacity of the UK Financial Intelligence Unit (UKFIU) to deliver feedback to reporters on SARs reporting, which will enhance the quality of information submitted to law enforcement in the future.

Firm compliance

7.35 Since 2017, most firms continue to make good progress to improve their mitigations against money laundering and terrorist financing. The 2017 NRA identified that the most common theme of enforcement action on firms was poor governance and general underinvestment in resourcing to spot financial crime. Generally, supervised financial services firms have a good understanding of the money laundering and terrorist financing risks they face owing to changes since 2017. Financial crime teams have generally grown, and many industry participants note the improvement in dialogue with the FCA. Greater firm employee awareness of the Senior Managers and Certification Regime[19] continues to improve firm culture, governance and attitude towards AML/CTF responsibilities. The growing use of technology also continues to help firms spot suspicious activity, particularly new challenger banks. However, access to wider industry intelligence can be difficult for these new firms. Many challenger banks are dependent on rapid customer growth for survival, which must not come to the detriment of CDD obligations. However, there has been no evidence of this yet.

7.36 Since 2017, the FCA has published a number of enforcement sanctions against firms for having inadequate AML/CTF controls, including Deutsche Bank, Canara Bank, Standard Chartered Bank and, most recently, Commerzbank London. The FCA continues to see deficiencies in control frameworks and their implementation across all types of retail and wholesale firms.

7.37 The FCA and firms' understanding of the money laundering and terrorist financing risks in the capital markets continues to develop. While the FCA has published its Capital Markets Thematic Review,[20] firms are in earlier stages of adopting appropriate controls than other financial services sectors. This was demonstrated in April 2019 with the FCA's letter to wholesale market firms, which identified "a culture and mindset which underestimates the risk of brokers committing or facilitating… financial crime through their role as market intermediaries, combined with poor monitoring and controls." [21]

19 'Senior Managers and Certification Regime: dual-regulated firms', FCA, December 2019.

20 'TR19/4: Understanding the money laundering risks in the capital markets', FCA, June 2019.

21 See at https://www.fca.org.uk/publication/correspondence/dear-ceo-letter-wholesale-market-broking-firms.pdf.

7.38 The payment services sector is developing rapidly due to regulatory changes allowing greater entry of non-bank firms into the financial services sector. This expands the relative risk the sector represents. The FCA's subsequent understanding of payment services' controls continues to develop, particularly in relation to Account Information Service Providers and Payment Initiation Service Providers. Unlike retail banks, many payment service providers (PSPs) operate under multiple brand names and often change their trading name multiple times. This may make it harder to understand potential money laundering through each firm.

7.39 The FCA's and law enforcement's understanding of the controls of many other PSPs has advanced since 2017. For example, law enforcement has observed that e-money firms generally have very well-developed live transaction monitoring and document verification. This is observed by the FCA's own assessment of the e-money sector.[22] It found they generally demonstrated a positive culture, and good awareness and understanding of their financial crime obligations in relation to e-money services. However, as in the banking sector, money laundering risks may increase if newer entrants to financial services do not channel adequate investment, resources and staff to the relevant areas as they grow.

7.40 Retail banks have a high level of awareness of the terrorist financing risks associated with their services. Other financial services sectors are improving their understanding of the terrorist financing risks, though gaps remain.

7.41 The ongoing public-private partnerships between the financial services sector and law enforcement continues to build understanding of the risks, as well as identify terrorist activity. For example, the government has recently published a statement to promote information sharing within corporate groups of banks.[23]

7.42 The JMLIT has delivered concrete results for terrorist financing and terrorism investigations. In the aftermath of the Westminster attack, multiple financial institutions proactively reached out to the head of the NTFIU to offer assistance in identifying the terrorist networks involved, allowing the NTFIU to more rapidly obtain a full financial picture. After the London Bridge attack, the NTFIU, with the UKFIU support, initiated a 24/7 response and the case was brought to the JMLIT within 12 hours of the attack. Within a few hours of the briefing, financial institutions were able to provide assistance to identify the payments for van hire and establish spending patterns, allowing further investigative strategies to be identified. This assistance was crucial in allowing investigators to conclude that the attack involved only 3 attackers with no broader network.[24]

Supervisor response

7.43 The FCA's approach to AML/CTF supervision, in line with its international AML/CTF counterparts, is risk based. The FCA looks for the most effective

22 'Money Laundering and Terrorist Financing Risks in the E-Money Sector', FCA, October 2018.

23 Government statement on cross-border information-sharing within corporate groups, May 2020

24 'Anti-money laundering and counter-terrorist financing measures United Kingdom Mutual Evaluation Report', FATF, December 2018.

and proportionate means to ensure good AML/CTF standards in regulated firms, and allocates its resources to focus most closely on those firms and activities that present the highest risks of money laundering and terrorist financing. AML/CTF is a responsibility for all supervisors, with sector supervisors responsible for assessing firms' overall AML/CTF compliance and supported by specialist financial crime supervisors.

7.44 The FCA continues to deploy powerful AML/CTF tools, including formal business restrictions (35 since August 2017) and skilled person reports into business practices (13 since August 2017). The wider supervision of financial services firms under the Financial Services and Markets Act 2000 (FSMA) continues to give the FCA scope to recruit industry specialists to provide the FCA with additional expertise. The FCA has also imposed its second largest fine of £102,163,200 for AML breaches in 2019 against Standard Chartered Bank.[25] The FCA continues to impose financial penalties on firms and individuals, with 3 significant enforcement outcomes since 2017, totalling over £140 million, and further investigations are on-going. In line with the findings from the FATF Mutual Evaluation Report (MER) of the UK, the FCA will continue to utilise its tools and resources to best effect and improve standards across industry.

7.45 The FCA is also improving its supervisory response. This includes re-examining the intensity of its supervision, as suggested by the UK's MER. The FCA has accepted this recommendation and is developing a new data-driven supervisory strategy in response to these concerns. The UK financial services sector remains deeply integrated with the international financial system and FCA effectiveness will remain reliant on continuing to review and improve its international partnerships with overseas supervisors.

7.46 The FCA remains committed to developing innovative methods to improve its specific understanding of money laundering through payment services and the capital markets. In its new business plan the FCA has committed to consult on extending its Financial Crime Data Return, previously launched in 2016 to provide a collective industry view of the risks. The inclusion of a greater number of firms the FCA supervises under the MLRs will help to strengthen its risk-based supervision.[26]

7.47 The FCA's AML TechSprints[27] have also ensured the UK is a global leader in supporting innovation in regulatory compliance for AML/CTF. In addition, HM Treasury and UK Finance have established the Innovation Working Group. The group is working to overcome barriers to firms adopting innovative new solutions that could increase the financial service sector's ability to mitigate the risk of money laundering and terrorist financing.

Law enforcement response

7.48 The UK's MER assessed that law enforcement's collective response to money laundering and terrorist financing was excellent, noting the UK "routinely and aggressively identifies, pursues and prioritises money laundering

25 See FCA Press release.

26 'FCA Business Plan 2020/21', FCA, April 2020.

27 For more information, see FCA website.

investigations and prosecutions". Law enforcement has continued to strengthen its response further. On 31 October 2018, the National Economic Crime Centre (NECC) was launched to further enhance cooperation between the public and private sector and deliver a step-change in the response to tackling serious and organised economic crime. The NECC is collaborating with law enforcement agencies to elicit and coordinate their input, alongside the private sector, in delivering public-private economic crime threat assessments. The NECC, Home Office and HM Treasury are ensuring the findings are reflected in responses to mitigate identified risks in the financial services sector. Where appropriate, UK Finance are also coordinating the response on behalf of its membership to support risk mitigation.

7.49 The NECC is also working with partners across law enforcement to examine the future demand for financial investigators and the potential results of further investment. This work will run alongside the implementation of the outcomes of the Proceeds of Crime Centre review and will include reconsideration of the future of financial investigator training.

7.50 Since 2017, law enforcement agencies have been given new enforcement powers. The Criminal Finances Act 2017 gives law enforcement greater power to seize and forfeit funds held in bank accounts through the use of account freezing orders (AFO). In the 2019 to 2020 period, law enforcement agencies in England, Wales and froze £208 million covering over 812 bank and building society accounts through the use of AFOs.[28] The increasing adoption will serve to complement traditional confiscation investigations.

7.51 The financial services sector continues to report huge numbers of SARs, with the retail banking sector reporting 462,895 in the 2019 to 2020 period. SARs are a critical intelligence development resource for law enforcement in tackling money laundering, terrorism, serious and organised crime, corruption and fraud, providing immediate opportunities to stop crime and arrest offenders, contributing to the UK's understanding of crime and informing strategies to reduce its impact.

7.52 Law enforcement have a high level of capacity and capability to investigate terrorist financing activity, as well as to use financial intelligence to investigate terrorist activity more generally. For example, between 1 April 2018 – 31 March 2020, law enforcement agencies in England and Wales have obtained 83 account freezing orders, and 25 forfeiture orders in relation to terrorist activity. However, the nature of domestic terrorist financing activity continues to present challenges for law enforcement to prevent and detect it. Low amounts of funds from legitimate sources are inherently difficult to detect and distinguish from non-concerning activity. This is confounded by the diversity of terrorist financing methods, making it difficult to compile a comprehensive set or combination of predictive indicators to identify it. For example, analysis of data following the 2017 terrorist attacks showed that the majority of SARs were submitted after the attacks, once the name of the attackers had become known through police enquiries and/or media reporting. While financial intelligence is very useful,

28 'Asset Recovery Statistical Bulletin: financial years ending 2015 – 2020.' Home Office, September 2020.

defensive SARs filed after an attack repeating information shared by the police with firms can unnecessarily over-burden the system.

Box 7.A: Case study 1

7.53 Project Princekin was the NECC-led multi-agency approach designed to tackle an identified threat to the UK financial system which was deemed as generating a high risk of money laundering by organised crime groups. These groups utilised accounts to receive high-value third party cash deposits. A bank recognised there was a significant threat of large scale money laundering activity where bank accounts are being exploited. The methodology adopted in this case utilises the bank's Automated Services Devices (ASDs). The bank requires a depositor to be a bank customer, i.e. they hold an account with the bank, before cash can be credited to an account via an ASD. However, the facility then allows the depositor to credit any account of a customer of the bank. This facilitates the payment of cash into a large number of accounts held by the bank through one set of credentials without any of those funds being registered, assigned or recognised as being related to the customer making the deposit. The credentials being used are not capable of being subject to any kind of compliance checks to verify correct ownership/possession at the time the deposit is being made.

7.54 Under Project Princekin 95 Account Freezing Orders were obtained, freezing approximately £3.3 million; the majority of which has since been successfully forfeited or returned. Some of the funds remain under investigation. The NCA, HM Revenue & Customs , City of London Police and NECC partners across law enforcement have also undertaken money laundering investigations following intelligence disseminations by the NECC. The NECC's Expert Laundering Evidence cadre also provided support to Project Princekin as impartial expert witnesses.

7.55 The NECC has also worked closely with partners, including the Chinese Embassy (a proportion of misused accounts belonged to Chinese students), UK universities, the Duke of Edinburgh's Award, UK Finance, Cifas and Crimestoppers. A strategy was developed to publicise the risks and penalties in becoming a money mule. Crimestoppers acted as an outlet for students to report, anonymously, any suspicions.[29]

7.56 The financial institution that had originally raised the alarm has since closed off the facility which enabled third party deposits.

29 'Chinese Underground Banking', National Crime Agency, October 2019.

Box 7.B: Case study 2

7.57 In April 2019, the FCA fined Standard Chartered Bank (SCB) £102 million for breaches in 2 higher risk areas of its business. SCB's failings occurred in its UK Correspondent Banking business during the period from November 2010 to July 2013 and in its UAE branches during the period from November 2009 to December 2014. This is the second largest financial penalty ever imposed by the FCA for AML failings.

7.58 The FCA found significant shortcomings in SCB's own internal assessments of the adequacy of its AML controls, its approach towards identifying and mitigating material money laundering risks and its escalation of money laundering risks. These failings exposed SCB to the risk of breaching sanctions and increased the risk of receiving and/or laundering the proceeds of crime. Examples include:

- opening an account with 3 million UAE Dirham in cash in a suitcase (just over £500,000) with little evidence that the origin of the funds had been investigated.
- not reviewing due diligence on a customer despite repeated red flags such as a blocked transaction from another bank indicating a link to a sanctioned entity.

7.59 The FCA worked alongside a number of authorities during this investigation including a number of UK and overseas agencies such as the US Department of Justice, New York County District Attorney, US Board of Governors of the Federal Reserve, New York State Department of Financial Services and US Office of Foreign Assets Control.[30]

Box 7.C: Case study 3

7.60 In June 2020, the FCA fined Commerzbank £37, 805, 400 for failing to have adequate AML systems and controls in place between October 2012 and September 2017.

7.61 Commerzbank London was aware of these weaknesses and failed to take reasonable and effective steps to fix them despite the FCA raising specific concerns about them in 2012, 2015 and 2017 through its supervisory activity. These weaknesses also persisted during a period when the FCA was publishing guidance on steps firms could take to reduce financial crime risk as well as taking enforcement action against a number of firms in relation to AML controls. Despite these clear warnings, the failures continued.

[30] For more information, see FCA website.

7.62 The FCA's investigation identified failings in a number of areas, including Commerzbank London's failure to:

- conduct timely periodic due diligence on its clients, which resulted in a significant number of existing clients not being subject to timely know-your-client checks. By 1 March 2017, 1,772 clients were overdue updated due diligence checks. A material number of these clients were able to continue to transact with the bank's London branch due to the implementation of an exceptions process, which was not adequately controlled or overseen, and which became 'out of control' by the end of 2016;
- address long-standing weaknesses in its automated tool for monitoring money laundering risk on transactions for clients. For example, in 2015 Commerzbank London identified that 40 high-risk countries were missing, and 1,110 high-risk clients had not been added, to the transaction monitoring tool; and
- have adequate policies and procedures in place when undertaking customer due diligence on clients.[31]

[31] For more information, see FCA website.

Chapter 8
Cryptoassets

Cryptoasset risk scores		
	2017 Risk Score	2020 Risk Score
Money laundering	Low	Medium
Terrorist financing	Low	Medium

Summary and risks

- The risk of money laundering through cryptoassets has increased since 2017, with criminals increasingly using and incorporating them into their money laundering methodologies. The risk of using cryptoassets for money laundering overall is now assessed as **medium**.
- The infrastructure supporting cryptoasset use remains vulnerable to abuse by criminals seeking to clean funds through the purchase and exchange of cryptoassets. The cryptoasset ecosystem has developed, matured and expanded considerably in the last 3 years, providing additional opportunities for abuse.
- Although cryptoassets use by terrorists is not widespread, there is information to suggest that terrorists may be using cryptoassets to finance some terrorist activities. This, combined with the improved accessibility of cryptoassets and the increased ability to mask the destination of funds, means that the risk of terrorist financing through cryptoassets has increased since 2017 to **medium**.
- The government's understanding of cryptoassets has also developed considerably since 2017, improving our understanding of the risks and respective mitigations. The inclusion of cryptoasset exchange providers and custodian wallet providers into the Money Laundering Regulations (MLRs) since January 2020 will help to mitigate vulnerabilities in time.

Overview of cryptoassets

8.1 Referred to in the 2017 NRA as "digital currencies", cryptoassets are cryptographically secured digital representations of value or contractual rights that use a form of distributed ledger technology and can be transferred, stored or traded electronically. Cryptoassets are now a legally defined term in the UK's MLRs. As with any form of value, cryptoassets continue to be abused by criminals, by being stolen, enabling criminal payments, including for drugs, or facilitating sanctions evasion. However, cryptoassets can be also exploited by illicit actors looking to disguise the origin of illegally obtained funds or used to fund terrorist activities. Cryptoassets are yet to achieve mainstream adoption by consumers or integration into the traditional financial services sector, although this may change in the future with the development of global stablecoins.

8.2 Cryptoassets are an alternative form of value to traditional fiat currency. While their value can appear volatile and their workings complex, several features make them attractive for money laundering. These features enable money launderers to transfer, integrate and layer illicit funds into cryptoassets, before being converted back to fiat currency, to obfuscate the original source and purpose of the funds and move value across the world. The scale of such abuse across the services that facilitate this activity is an intelligence gap.

8.3 Vulnerabilities include:

- their pseudo-anonymous nature – users are not able to be easily or immediately identified on the distributed ledger that underpins the running of a cryptoasset due to the use of pseudonyms rather than real-world identities. This means that users can employ a degree of obfuscation to hide their identity. Furthermore, identification and monitoring can be further obfuscated through the use of mixers and tumblers, or using privacy-enhanced cryptoassets known as "privacy coins"
- their accessibility online and global reach – cryptoassets enable criminals to quickly move funds across national borders at scale, without requirement for a face-to-face business relationship
- uneven regulatory requirements and regulatory arbitrage – some jurisdictions do not require firms facilitating the exchange of cryptoassets to perform adequate due diligence checks on customers and their transactions

8.4 Cryptoassets can also act as a method for payments between criminals, be used for the purchase of illicit tools and services online, and be exploited for other criminal activity such as fraud. Cryptoassets also remain a key tool in cybercrime. Cryptoassets are suited to being used in highly confrontational cybercrimes, such as ransomware and extortion attacks and are regularly used by cyber criminals to hold and transfer value.

Cryptoasset exchanges

8.5 Cryptoasset exchanges are at risk of abuse by money launderers, owing to their use as a gateway to buying and exchanging cryptoassets. Cryptoasset exchanges are the most common way for consumers to initially enter the cryptoasset market by purchasing, exchanging and investing in cryptoassets. The growth in exchanges continues to improve cryptoasset accessibility, with 5.35% of the UK population considered to have owned, or currently own cryptoassets today; an increase from 3% in 2019 alone.[2] This trend suggests it will be increasingly easy for criminal actors to enter the cryptoasset market by converting fiat currency. Prior to the inclusion of cryptoasset exchange providers into the MLRs in January 2020, cryptoasset exchanges were not legally required to perform customer due diligence (CDD) or establish the source of customer funds. While some of the more developed exchanges did have some controls in place prior to January, this potential gap offered criminals significant anonymity to disguise the source of their illicit funds through their exchange into and out of cryptoassets.

8.6 Law enforcement has seen examples of criminals planning to establish their own cryptoasset exchanges. If used for money laundering, such schemes could use third parties to purchase cryptoassets using the criminal's own funds as a mule investor. Research also suggests a minority of over the counter brokers,[3] who may be associated with an exchange but operate independently, specialise in providing money laundering services to criminals.[4]

8.7 Understanding of money laundering risk through exchange "mixers" has increased since 2017. Although it is almost certain that standard exchanges are the primary destination of illicit cryptoassets, it is likely mixers feature as a recipient in the laundering process too.[5] Mixers obfuscate the source of funds by pooling and then redepositing funds into different wallets. Any withdrawn funds are different from the original funds deposited. This conceals their origin and ownership, further complicating the trail for law enforcement to detect and mitigate illicit activity. Similar to mixing, other obfuscation techniques are available too, including CoinJoin and chain hopping.

Cryptoasset automated teller machines (CATMs)

8.8 CATMs are also at risk of being abused by money launderers, offering another gateway for criminals to enter the cryptoasset market to launder funds. Prior to their incorporation into the scope of the MLRs, CATMs offered criminals the anonymity to disguise the source of illicit cash through their exchange in and out of cryptoassets. CATMs are potentially more vulnerable to abuse than exchanges as they offer criminals the ability to

---

2 'Research Note - Unrestricted Cryptoasset consumer research', FCA, June 2020.

3 According to Chainalysis, OTC (Over The Counter) brokers facilitate trades between individual buyers and sellers who can't or don't want to transact on an open exchange. OTC brokers are typically associated with an exchange but operate independently. Traders often use OTC brokers if they want to liquidate a large amount of cryptocurrency for a set, negotiated price. OTC brokers are a crucial source of liquidity in the cryptocurrency market.

4 'The 2020 State of crypto crime', Chainalysis, January 2020.

5 Ibid.

convert the physical cash proceeds of crime directly, unlike an online exchange where typically cash may be transferred to the exchange through a bank or other payment system. Existing know your customer (KYC) checks prior to January 2020 were known to vary dramatically, further increasing their vulnerability.

8.9 Law enforcement has seen evidence of money mules increasingly making use of CATMs to launder illegally obtained cash. Furthermore, the opportunities for abuse has increased since 2017 with the growth of CATMs in the UK increasing to 271 in April 2020, compared with just 35 in May 2016. [6] Europol reports that in at least one instance, there have been "strong suspicions of complicity between the company managing the ATMs and money launderers".[7] The physical cash capacity limits of CATMs limit the scale of funds laundered, thereby restricting the risk of abuse to low-level criminals seeking to launder low amounts.

Peer to peer (P2P) exchange platforms

8.10 P2P platforms are also considered at risk of abuse by money launderers, and it is highly likely they are abused by organised criminal gangs (OCGs). The exchange of custody of cryptoassets is usually conducted online through a choice of methods and if a P2P exchange platform exchanges or arranges the exchange of cryptoassets by way of business, then they will have to abide by the MLRs, reducing the risk of abuse. However, P2P platforms can put users in direct contact over the internet or physical contact with one another, providing the opportunity to transfer ownership of cryptoassets. The sellers and buyers listed on a bulletin board may not necessarily fall in scope of the MLRs as the exact regulatory perimeter of P2P exchange providers that fall in scope of the MLRs is complex. P2P advertisements have appeared for London cash-based sales with purchases of up to £100,000 worth of Bitcoin, demonstrating the potential amounts that can be exchanged. Meetings can also be arranged using encrypted messaging, making it more difficult for law enforcement to track. In these instances, control of a cryptoasset cold storage wallet can be physically handed over to the new owner in exchange for payment without the transaction appearing on the blockchain. The wide range of P2P business models, compliance levels and rapid evolution means that risks can vary across the sub-sector.

8.11 Some of the larger P2P platforms have begun to remove the option for traders to advertise 'cash in person' trades, instead only allowing for payment to be made via bank transfer. Some platforms have also begun to introduce compliance technology for transaction monitoring. These efforts appear to have resulted in displacement of this activity onto other exchange platforms which still offer this service, as well as onto encrypted communications platforms.

8.12 The risk of P2P transactions is likely to increase further in the future with the development of stablecoins. They could make it more attractive to carry out P2P transactions because of the fixed value of the coin to a known value (such as the US Dollar), which removes the risk of holding assets in a more

[6] Coinatmradar search, April 2020.

[7] '2017 Virtual Currencies Money Laundering Typologies', Europol, December 2017.

volatile cryptocurrency, such as bitcoin. This may make such transactions more attractive in comparison to the use of formal cryptoasset exchanges to exchange value. The resulting risks of money laundering will need to be monitored carefully.

8.13 The development of decentralised P2P exchanges (DEXs) also creates new potential vulnerabilities in the P2P sector. DEXs create a P2P system of exchange directly on the digital blockchain, further enhancing the anonymity of exchange between criminals, and providing another route for exchange without formal physical contact. The regulation of DEXs is further complicated by their unclear jurisdictional origins and whether there is an identifiable centralised organising entity running it. However, the scale of illicit funds passing through a DEX is likely to be less than the more widely understood and developed centralised exchanges at this time.

Other exchange routes

8.14 Money laundering risks also arise from initial coin offerings (ICO) and cryptoasset payment cards. However, these are considered lower risk, based on the lack of evidence of abuse compared with formal exchanges, CATMs and P2P platforms. Cryptoasset "gift cards" are also available as a means for attributing value to a "card" which can then be transferred or exchanged with another party.

8.15 ICOs offer a route to exchange funds for cryptoassets and to raise funds for a blockchain project. The number of ICOs has declined since 2018. Law enforcement investigations into ICOs predominantly revolve around fraud. However, new cryptoassets can be easily set up, and criminals could then encourage mules to invest illicit funds into the cryptoasset, thereby creating a fake audit trail by claiming their wealth derives from legitimate investments.

8.16 The development of new payment cards since 2017 allows users to spend cryptoassets like fiat currency on an ordinary debit card. Criminals can exploit this by using laundered cash to purchase goods to realise their profits, or to resell for fiat currency. The number of market participants is considered small and some firms already fall under the the Financial Conduct Authority (FCA)'s supervision as an e-money institution, partially mitigating the risk. However, this market is growing, with the potential for an increasing variety of business models that use cryptoassets as a method of payment. The greater use of near field communication to facilitate contactless cryptoasset payments from a cryptoasset wallet linked to a mobile phone, should also be monitored carefully.

Terrorist financing

8.17 The 2017 NRA noted a lack of evidence of cryptoassets being used to facilitate and finance terrorist activity. It is still assessed that cryptoasset use by terrorists is not widespread but is slowly growing. Instead, terrorists continue to prioritise more traditional methods such as cash couriers, money service business, and bank transfers. These methods remain preferred due to their ease of use and the low sums usually involved.

8.18 The slow increase in use, alongside the improved accessibility of cryptoassets and the increased ability to mask the destination of funds means that the risk of terrorist financing through cryptoassets is now assessed to be **medium**. The use of cryptoassets is more prevalent with far-right terrorists. However, there has been a slow increase from both Islamist and far-right terrorists. This is likely due to the anonymous nature of cryptoasset transactions and their increasing accessibility. The movement of funds without in-person interactions is attractive for both raising and moving funds anonymously. Development of the cryptoasset technology means they are now more accessible than in 2017, and there are a greater number of services available to mask the end destination of funds.

8.19 In the UK, some isolated cases of the use of Bitcoin have been noted. However, there is no evidence that terrorists have used cryptoassets to purchase material for attacks. Ad-hoc donations to terrorist organisations using cryptoassets likely do occur, but the size and frequency of these transactions are assessed to be low. Terrorists' attempts to fundraise using cryptoassets are typically speculative and normally limited to linking Bitcoin wallet addresses on terrorist-linked social media accounts.

8.20 However, there are aspects of cryptoassets that likely limit their use for terrorist purposes, including a lack of understanding of how they work, and how they can be accessed and utilised (although this is less likely in the case of far-right terrorists). As legitimate usage of cryptoassets increases in the general population and their accessibility continues to grow, terrorist use of cryptoassets could increase. This risk may be mitigated by the introduction of anti-money laundering and counter-terrorist financing (AML/CTF) regulations on cryptoasset exchange providers, which requires identify verification of customers.

Supervision, compliance and law enforcement response

Supervision and compliance

8.21 The UK has recently updated its Money Laundering and Terrorist Financing Regulations (MLRs) to cover cryptoassets. As of 10th January 2020, the MLRs capture:

- UK cryptoasset exchange providers
- custodian wallet providers
- CATMs
- some peer-to-peer exchange providers
- the exchange of newly issued/minted cryptoassets as part of an initial coin offering (ICO) or initial exchange offering (IEO)
- cryptoasset payment cards

8.22 Incorporation into the MLRs creates new controls to mitigate the risk of money laundering and terrorist financing through cryptoassets. The businesses outlined above are now required to register with the UK's FCA, carry out appropriate checks on their customers and report suspicious activity. Any cryptoasset business existing prior to 10th January 2020 must comply with the MLRs and register with the FCA by 10th January 2021 or cease operations. If they continue to operate, they will face a potential criminal conviction. Any new business intending to begin cryptoasset activity after the 10th January 2020 must register with the FCA prior to commencing planned activity.

8.23 The scope of the UK's AML/CTF regime goes beyond the requirements of the EU's Fifth Anti-Money Laundering Directive (5MLD) to comply with all but one of the latest international Financial Action Taskforce (FATF) standards (recommendation 16).[8] This ensures a broad range of cryptoasset firms that facilitate cryptoasset exchange fall into scope of the regulations, helping to mitigate the risk of abuse. The regulations also apply to some of those participating in and providing financial services related to an issuer's offer and/or sale of a cryptoasset, as per the FATF's definition of a 'virtual asset service provider', where those individuals are 'arranging and making arrangements with a view to the exchange'. We consider that the risks related to firms providing cryptoasset services other than the direct exchange (such as cryptoasset advice) are lower than those carrying out the actual exchange.

8.24 The UK is in the process of incorporating recommendation 16 (the travel rule) of the FATF standards into the MLRs and is exploring options for implementation. This will require cryptoasset firms to obtain, hold and transmit identifying information of both parties in any cryptoasset transaction. The implementation of the travel rule will increase the information available to supervisors and law enforcement on the parties transferring cryptoassets, improving transparency of cryptoasset users and law enforcement's ability to 'follow the money'.

8.25 The introduction of regulatory standards on cryptoasset firms is an important step in the UK's regulatory treatment of cryptoassets and a significant development in reducing the risk of cryptoassets being used for money laundering and terrorist financing. However, it is too early to know exactly how well firms are implementing the regulations, and therefore, how far it will mitigate the risk.

8.26 Ahead of the regulations being extended to cryptoasset firms, some firms had already developed customer onboarding regimes, investigatory monitoring systems, and customer databases in order to help legitimise the industry and gain competitive advantage. Some firms also made use of crypto-forensic services in order to detect criminal abuse.

8.27 However, the quality of firms' control frameworks have so far proven varied. Some have little experience with regulatory compliance, impacting their effectiveness, and others may still decide not to comply with the requirement to register. Likewise, it will take time for firms to confidently implement the

[8] The 'travel rule': See HM Treasury response to consultation on the transposition of the Fifth Anti-Money Laundering Directive.

measures required of the MLRs, delaying the intended mitigation of risks. As a result, it is unlikely that the new controls will completely mitigate the risk of cryptoassets being abused for money laundering. The FCA will carefully examine registration applications and subsequent compliance with the MLRs to assess whether controls adequately meet the high standards required and take enforcement action as required.

8.28 The FCA can help mitigate some of these risks. For example, the MLRs include the ability for the FCA to order a skilled person to review a firm's systems and controls. It can also issue directions to remedy weaknesses in a firm's compliance and is using this tool to intervene in cases where firms fail to meet appropriate standards, including prior to the completion of registration. The FCA will continue to adapt its supervisory approach as the sector evolves, grows and compliance levels are better understood.

8.29 Due to inconsistent cryptoasset regulations globally, there is a risk of regulatory arbitrage. Criminals may choose to use foreign exchanges where AML/CTF checks are less onerous. Furthermore, complicit or criminal exchanges may choose to move to jurisdictions where AML/CTF regulatory requirements are lax. International cooperation, common understanding and a level of consistency in regulatory approach is critical to stopping the abuse of cryptoassets to launder money. The global adoption of AML/CTF obligations on cryptoasset firms, in line with the latest FATF standards, will in time diminish the risk of criminals accessing and abusing the global cryptoasset market.

8.30 In addition to AML/CTF specific regulations on cryptoassets, government and international partners are working to introduce prudential and consumer regulatory frameworks for cryptoassets. Increased consumer protection may further increase the attractiveness of cryptoassets to ordinary consumers in time, making it easier to hide money laundering activity within increasing volumes of legitimate transactions.

Law enforcement response

8.31 Law enforcement has taken significant steps to improve their ability to mitigate the cryptoasset risks since 2017. In 2018 to 2019, the National Police Chiefs' Council Cybercrime Programme committed funding for a law enforcement cryptoasset capability uplift, and law enforcement agencies continue to build their capability.

8.32 Although the number of investigations and prosecutions related to money laundering using cryptoassets remains low, they are increasing. This in turn is improving law enforcement and the FCA's understanding of money laundering methodologies. Continuing to improve the intelligence sharing relationship between law enforcement and the FCA is essential to share this understanding and support an effective AML/CTF regime.

8.33 In November 2019, the UK Financial Intelligence Unit (UKFIU) introduced new Suspicious Activity Reports (SARs) reporting codes, including "virtual assets." The use of glossary codes is considered good practice and are crucial for enabling the UKFIU and wider law enforcement to conduct analysis to identify money laundering trends, high-risk cases for development and take

immediate action where necessary. They also enable the production of feedback to reporters on trends and patterns identified in cryptoasset SARs.

Box 8.A: Case study 1

8.34 In February 2019, a suspected criminal was arrested on suspicion of money laundering having been found with cash to the value of £170,000. Analysis of phones in his possession showed that he was being directed by a Dubai-based network to make multiple cash collections in the UK. The cash was handed to a number of face to face cryptoasset exchangers who credited the value in Bitcoin to a wallet held by the suspects 'controller' in Dubai.

8.35 Evidence from 6 days of activity showed 8 cash exchanges occurring with a total value of about £1 million. The suspect subsequently pleaded guilty and was sentenced to 3 years 4 months in prison in August 2019.

Box 8.B: Case study 2

8.36 A UK based crypto exchange company submitted a SAR to the National Crime Agency regarding activity in relation to a cryptoasset wallet. While an investigation continues, the PSNI made a successful application to restrain Bitcoin funds held in a cryptoasset wallet. Due to concerns about the fluctuating value of Bitcoin, the Court granted an application to have it converted to sterling and held in a UK bank account.

Chapter 9
Accountancy services

Accountancy services risk scores		
	2017 Risk Score	2020 Risk Score
Money laundering	High	High
Terrorist financing	Low	Low

Summary and risks

- Accountancy Service Providers (ASPs) monitored under the Money Laundering Regulations (MLRs) offer a wide range of services and are either supervised by the Professional Body Supervisors (PBSs) or by HM Revenue & Customs (HMRC).[1]
- Overall, the risk of money laundering through ASPs remains **high**. The risk is highest when ASPs do not fully understand the money laundering risks and do not implement appropriate risk-based controls, particularly where ASPs fail to register with a supervisor.
- Accountancy services remain attractive to criminals due to the ability to use them to help their funds gain legitimacy and respectability, as implied by ASPs' professionally qualified status. Those providing accountancy services remain at risk of being exploited or abused by criminals, especially if ASPs become complacent in their regulatory obligations under the MLRs, or willingly facilitate money laundering. The accountancy services considered most at risk of exploitation continue to be company formation and termination, mainstream accounting and payroll. While there have been improvements in the supervision of ASPs, in part due to the work of the Office for Professional Body Anti-Money Laundering Supervision (OPBAS), these services remain prevalent in law enforcement cases.
- We continue to judge that accountancy services are not attractive for terrorist financing, and there remains no evidence of these services being abused by terrorists. Therefore, the risk of terrorist financing through the sector is assessed to be **low**.

[1] If a practitioner is undertaking regulated activity under the MLRs, they should be registered with PBSs or HMRC. However, as the term accountant is not protected and those practicing in the profession do not have to be registered with a supervisor for the majority of their accountancy activity, there is a risk that unsupervised practitioners carry out AML regulated business.

Trust and company service providers (TCSPs)

Company formation and associated TCSP services[2] continue to be the highest risk services provided by ASPs for money laundering. These can enable the laundering of millions of pounds, conceal the ownership of criminal assets and facilitate the movement of money to secrecy jurisdictions. Of the 23,400 TCSP providers in the UK, 72% are supervised by accountancy bodies; however most provide these services as an add on to their main accountancy services.

9.2 Company formation as a standalone service offers less exposure to potential abuse and it is therefore considered lower risk. However, when coupled with other high-risk services or high-risk factors, such as a third party outside of the UK, the level of risk increases. For example, a UK service provider was asked by a corporate service provider in another jurisdiction to set up a UK company. The risk was assessed based on the corporate service provider, rather than the underlying client. This resulted in the risk assessment on their part being lower than it should be and the TCSP not asking for business reasons as to why the client wanted to set up a company in the UK for revenues of £12,000.

9.3 ASPs that offer registered office or nominee directorship services are also at risk of exploitation for money laundering as those services can enable concealment of beneficial ownership or be used to facilitate the movement of money to offshore jurisdictions. Companies House acknowledge the issues surrounding beneficial ownership transparency in the UK and are taking steps to prevent the system being abused. See paragraphs 9.25 and 11.30 below for more information on the steps being taken by Companies House to mitigate this risk. See chapter 11 on trusts and corporate structures for more detail on the risks associated with company formation and other trust and company services ASPs may offer.

Mainstream accounting

9.4 False accounting continues to pose a high risk of money laundering, as it can enable criminals to mask the source of funds, often in large amounts. This can fall into 3 categories: false bookkeeping, production of false documents and audit. We consider audit to pose a lower risk of money laundering abuse due to the strict parameters placed on ASPs undertaking these services.

9.5 Bookkeepers can enable money laundering by transferring money or creating paperwork to legitimise the flow of funds, both unwittingly and knowingly. This can include trade-based money laundering, where invoices are created in the absence of a sale, or invoices inflate the value of goods sold. Records can also be created to hide the existence of taxable assets. This can legitimise large amounts of illicit funds. See paragraph 9.10 for more on placement of tax evasion proceeds. However, ASPs don't always have to be complicit in this activity to enable money laundering. Legitimate ASPs may fail to identify

[2] The MLRs define a TSCP as a firm or sole practitioner which by way of business, forms companies or other legal persons; acts as or arranges for someone else to act as a company director, partner or nominee shareholder; provides a registered office or business address or similar; and/or acts as or arranges for someone else to act as a trustee for a trust or similar arrangement. The provision of TCSP services involves various professional service sectors including ASPs, many of which provide these services as add on services to their core business activity.

receipts that their client has falsified or present an inaccurate picture. An ASP with poor MLR compliance can heighten their exposure to this risk, as it reduces the opportunities to identify red flags.

9.6 ASPs are often relied upon to produce or verify documents relating to financial positions, for use in applications such as mortgages, loans or visas. There is a risk that these services will be exploited by criminals to facilitate money laundering. ASPs could be used for their status as a trusted professional to produce falsified financial positions or legitimise criminal assets. Mitigations may include robust client due diligence procedures, but there are concerns that transactions are often overly complicated, and ASPs are not always scrutinising the authenticity of provided documentation and the underlying financial data.

9.7 Audit services can provide an additional layer of legitimacy to accounts and documents, and there is evidence that this has been used by criminals to launder millions of pounds.[3] However, it is highly unlikely to be used frequently for laundering due to the high barrier to entry to both access and provide audit services. Unlike other services offered by ASPs, authorisation from a supervisory body is required to perform audit services and strict monitoring conditions and protocols are imposed. Likewise, The Companies Act 2006 only requires the audit of certain companies with turnover and/or assets of several million pounds; companies of this size are more likely to have robust internal accounting procedures, making it harder to hide large scale laundering.

Payroll services

9.8 As with false accounting, payroll services can also provide criminals with a legitimate-looking record of money movement. We assess the risk of payroll services being used to launder funds is high due to poor mitigations in place. This may include poorly anti-money laundering (AML) trained staff providing these services, services provided by non-customer facing staff, and a lack of information provided to payroll providers by the customer to identify suspicious activity.

Other risks

9.9 The provision of tax advice and acting as an agent with HMRC on behalf of clients provides several means to launder money and poses a high risk. This is because large amounts of funds can be claimed or undeclared and there is a high likelihood of this service being used.

9.10 ASPs can advise clients on how to under-represent their turnover or income to reduce their tax liabilities. While this behaviour is primarily fraud (making a gain through false representation), it also counts as enabling money laundering. This is because the gain obtained (money retained that would otherwise be paid toward a tax liability) is then the proceeds of crime that is placed in the financial system. Likewise, ASPs can reclaim money from HMRC on a client's behalf when not entitled to do so. This places the proceeds of

[3] For example, see https://www.theguardian.com/world/2020/jan/23/pwc-growing-scrutiny-isabel-dos-santos-scandal-luanda-leaks-angola#maincontent.

crime in the financial system as the fraudulently gained funds will be transferred to the client's control as an apparently legitimate refund.

9.11 There continues to be a risk that criminals will exploit company liquidation and associated services (including insolvency practice, which may be conducted by certain accountancy professionals) to mask the audit trail of money laundered through a company. Regulatory guidance, increased supervision and strict legislative requirements on ASPs go some way to mitigate the risks of providing these services.

9.12 As highlighted in the 2017 NRA, it is likely that criminals continue to try and use the client accounts of ASPs to move large amounts of criminal funds quickly. However, supervisors have strict rules and guidance on how their members should handle client money, which reduces the likelihood of this abuse. We consider that the risk of an ASP's client accounts being used to launder money is lower for those supervised by a PBS or HMRC, than those that are operating unregulated.

9.13 Some supervisors have expressed concern that while still rare, ASPs are being increasingly asked to accept payment in cryptoassets. While use of cryptoassets alone is not necessarily suspicious, cryptoassets can be used to disguise the origin of funds more easily than other payment methods.

Terrorist financing

9.14 The risk of terrorist financing through accountancy services is **low.** We continue to assess that accountancy services are not attractive for terrorist financing and there remains no evidence of these services being abused for terrorist financing purposes.

Supervision, compliance and law enforcement response

Supervision and compliance

9.15 The 2018 UK Mutual Evaluation Report by the Financial Action Task Force (FATF) highlighted the inconsistencies in the AML supervision of the accountancy sector and the need for improvement, while noting the recent formation of OPBAS. Similarly, the 2019 Economic Crime Plan acknowledges the work of OPBAS and includes an assigned action (Action 36) for OPBAS to continue to strengthen the consistency of professional body AML supervision.

9.16 Changes to the MLRs in 2017 have boosted supervisors' capability to tackle non-compliance in their sector and the creation of OPBAS in 2018 has provided the PBSs with expectations on supervisory standards and a means of actively monitoring them. Although HMRC does not fall under OPBAS's remit for ASP supervision, they have committed to align their supervisory

approach[4] to the standards of the OPBAS Sourcebook[5] to further improve the consistency of ASP AML supervision.

9.17 Since the 2017 NRA, OPBAS has worked with the accountancy sector PBSs to increase the consistency of their AML supervision and facilitate increased intelligence and information sharing. OPBAS has assessed all 13 accountancy PBSs against its Sourcebook and is monitoring PBS action plans accordingly to address weaknesses identified. To further ensure consistency, OPBAS have held 4 workshops with the PBSs to cover areas of commonly identified weakness including: governance, risk-based approach, supervision and intelligence and information sharing.

9.18 In their 2020 supervisory report, OPBAS observed a notable increase in PBSs having appropriate governance arrangements for AML supervision; improvements in the application of a risk-based approach and an increase in PBSs undertaking proactive AML supervision. [6] The full impact of changes in AML supervision by the PBSs continues to be tested and assessed by OPBAS for effectiveness. This will be a focus of OPBAS supervision in 2020 to 2021.

9.19 Members of the Accountancy AML Supervisors Group (AASG) have continued to share good practice on the 'risk-based approach' required by the AML regime, ensuring a proportionate and consistent approach to different risk profiles while at the same time reflecting specific demographics of their membership, the services they provide, the nature of their clients and the geographic reach of member firms.

9.20 Intelligence and information sharing has also improved with OPBAS, alongside the National Economic Crime Centre (NECC), establishing the Intelligence Sharing Expert Working Groups (ISEWGs). The AASG members have also enhanced information and intelligence sharing, by actively engaging with OPBAS and the Accountancy ISEWG and in disseminating Joint Money Laundering Intelligence Taskforce (JMLIT) amber alerts.

9.21 This is alongside an increase in the number of self-reported AML related fines issued by ASP supervisors, with fines increasing to 226 in 2018 to 2019 up from 126 in 2017 to 2018.[7] However, the average fine amount has decreased and this increase in the number of fines was not consistent across all 13 accountancy PBSs; 3 did not issue any fines at all during the relevant period.

9.22 Likewise, wider public-private partnership work on private to private known suspicion information sharing will explore the feasibility of a mechanism to share information, both within and across sectors, on bad actors who have been exited or refused a service. This aims to improve the effectiveness of know your customer checks (KYC) and customer due diligence (CDD)

---

4 Action 35 in the UK's Economic Crime Plan.

5 'Sourcebook for professional body anti-money laundering supervisors', OPBAS, January 2018.

6 'Anti-Money Laundering Supervision by the Legal and Accountancy Professional Body Supervisors: Progress and themes from 2019', OPBAS, March 2020.

7 'Anti-money laundering and counter-terrorist financing: Supervision report 2018-19', HM Treasury, August 2020.

processes at the point of taking on a client to reduce the number of customers firms are required to exit.

9.23 There have also been a number of roundtable sessions held with the Economic Secretary to the Treasury, John Glen, where PBS senior leaders have been recognised for their progress so far but where they were also reminded of the importance of OPBAS's work and that the government expects more to be done to tackle illicit finance in the professional services sector.

9.24 There are still variable levels of understanding of the AML risks in the sector by ASP firms and individuals, which may limit the effectiveness of mitigations. For example, criminals can evade the checks that could identify their suspicious activity if firms do not conduct appropriate risk-based controls. The key non-compliance trends ASP supervisors have identified are a lack of comprehensive risk assessments or appropriate risk-based controls and poor documentation or record keeping demonstrating appropriate client due diligence. The drivers behind this are:

- a failure by ASPs to understand their obligations under the MLRs, therefore making them more vulnerable to abuse if they are lacking robust AML compliance procedures.
- non-prioritisation of AML compliance responsibilities by ASPs looking to save time and costs, or compliance being approached in a tick box manner.
- the lack of accountancy specific AML training available to ASPs, along with the lack of time or funding for training.

9.25 Transparency of beneficial ownership has also long been viewed as an issue in the UK, due to the nature of the company formation process. In September 2020, the Department for Business, Energy & Industrial Strategy published a response to its consultation on options to enhance the role of Companies House, committing to take forward plans to increase transparency and introduce ID verification for individuals setting up, controlling and owning companies.[8] The consultation has helped the government consider how we can improve the accuracy and searchability of the information held at Companies House, and give it greater powers to query and check the information submitted to it.

Law enforcement response

9.26 Steps have been taken to improve information sharing between law enforcement, supervisors and firms, which is increasing the collective understanding of the AML/CTF risks in the sector.

9.27 OPBAS, alongside the NECC and the JMLIT, established the ISEWGs in 2018 to 2019. The ISEWGs reflect the initial steps in sharing intelligence between PBSs, statutory AML supervisors and law enforcement. They were created to offer a platform for strategic and tactical intelligence to be shared and

[8] 'Corporate Transparency and Register Reform - Consultation on options to enhance the role of Companies House and increase the transparency of UK corporate entities', BEIS, September 2020.

enable communication between supervisors and law enforcement, and enable a greater understanding of the threat which supervisors can take account of in their supervisory activities. For the accountancy sector, all ASP supervisors are members of the ISEWG, including HMRC, as well as the NECC and the Financial Conduct Authority (FCA). There have been 6 strategic accountancy ISEWGs to date with a further 5 bilateral tactical intelligence sharing sessions taking place between individual accountancy PBSs and law enforcement.

9.28 Since the ISEWG's creation, OPBAS has seen a significant rise in intelligence centred communication between law enforcement, third parties and the PBSs. For example, up until March 2020, 32 detailed section 7[9] requests have been shared between the National Crime Agency and the accountancy PBSs relating to live investigations[10].

9.29 Outside the ISEWGs, the number of Suspicious Activity Reports (SARs) reported by accountants has seen a slight increase of 3.5% in 2019 to 2020, compared with the 2017 to 2018 period. The SARs guidance working group, including reporting sectors, the UK Financial Intelligence Unit (UKFIU), OPBAS and supervisors, is engaged with the sector on developing updated guidance. There is recognition that further work is required to improve effectiveness of the SARs reporting by the sector; improving the quality and effectiveness of information provided, as well as the percentage of ASPs who report SARs will help towards addressing this issue.

9.30 Targeting professional enablers is a priority for the NECC in its response to money laundering. The NECC has established a dedicated practitioners group to formulate a pipeline of cases for enforcement action. The Enablers Practitioners Group (EPG) also serves to inform best practice and share operational learning on professional enablers across the law enforcement community. Complex financial crime investigations can be hindered by the need to deploy specialist investigation skills, including forensic accountants, and the NECC has utilised the EPG to identify these resources across law enforcement and make them available to operational case teams.

Box 9.A: Case study 1

9.31 A PBS conducted an AML compliance review of a sole practitioner. The review started as a desk-based review. Upon receipt of the initial set of documents requested, the type and nature of clients of the firm raised some concerns with the reviewer. Open source research was conducted on the clients which raised further concerns as they identified a number of high-risk indicators of involvement of the client in human trafficking. Despite this, the sole practitioner had categorised

[9] Section 7 of the Crime and Courts Act 2013 is an information sharing gateway between the NCA and others to share information to assist the NCAs function.

[10] 'Anti-Money Laundering Supervision by the Legal and Accountancy Professional Body Supervisors: Progress and themes from 2019', OPBAS, March 2020.

all the clients as low risk for money laundering. At this point it was not clear if the sole practitioner was knowingly involved or had not identified these issues because of a lack of awareness and controls. An onsite visit was made to the sole practitioner to establish more about their procedures and risk assessment. The PBS also gathered more details on the clients (including the names, nationality, date of birth, National Insurance Numbers of the individuals working in the massage parlours as the firm provide payroll services so had these on file) which they included in a report to the UKFIU. Following the review, the PBS determined that the sole practitioner did not have an awareness of risk or the threats posed by his clients, and do not believe he was knowingly involved. No further action was taken.

Box 9.B: Case study 2

9.32 Through its risk-based approach to supervision, an accountancy sector PBS identified significant weaknesses in the AML compliance of a member.

9.33 The PBS's intelligence section identified concerning information linked to the staff/client ratio of the practice, which was being run as a one-man, sole trader operation. The firm was also acting as a TCSP, with research showing that there were tens of thousands of Companies House matches, of both companies and officers, registered at the premises. This was considered a substantial amount for a sole trader to manage.

9.34 An on-site AML compliance inspection was subsequently carried out which confirmed the earlier intelligence. 70% - 80% of the firm's client base was made up of small freight operators, many of which operated in Continental Europe and hold overseas bank accounts. This prompted concerns regarding the potential use of haulage contractors in people and drugs trafficking, the facilitation of illegal immigration and the smuggling of other contraband.

9.35 The compliance inspection identified significant failures in the member's AML systems and controls, including a lack of understanding of AML risk and outdated policies and procedures. It also found that although client due diligence was outsourced to a third-party company, which was run by a relative of the practice licence holder, there was a total lack of acceptable CDD carried out by this practice. Open source research also discovered that a family member of the practice licence holder, who was also a haulage contractor client of the practice, had recently been convicted of serious criminal offences and sentenced to a lengthy period in custody.

9.36 Although they could not establish any links between the practice and the criminality uncovered, the PBS did find this information relevant in

assessing the member's risk profile. Formal disciplinary action was then taken against the member.

Chapter 10
Legal services

Legal services risk scores		
	2017 Risk Score	2020 Risk Score
Money laundering	High	High
Terrorist financing	Low	Low

Summary and risks

- The risk of abuse of legal services for money laundering purposes remains high overall. Legal service providers (LSPs) offer a wide range of services and the services most at risk of exploitation by criminals and corrupt elites for money laundering purposes continue to be conveyancing, trust and company services and client accounts.
- The risk of these services being exploited by criminals increases when legal professionals fail to carry out their obligations under the money laundering regulations (MLRs) or take a tick box approach to compliance. Although there are strict regulations on who can become a legal professional, there also remains a risk that some legal professionals are complicit and willingly enable money laundering.
- There have been improvements in the supervision of LSPs, in part due to the work of the Office for Professional Body Anti-Money Laundering Supervision (OPBAS). However, the risk of these services being abused for money laundering continues to be high.
- Consistent with the findings of previous NRAs, we continue to assess that legal services are not attractive for terrorism financing and assess the risk to be low.

Conveyancing

10.1 There is no evidence that the risks in the sector have changed from the previous NRA. LSPs remain essential to the purchase of property in the UK and we continue to consider conveyancing services related to both residential and commercial properties at high risk of abuse for money laundering due to the high value and large volume of transactions. The risk is significantly higher when LSPs fail to comply with their obligations under

the MLRs or do not fully understand and mitigate the risks associated with the service.

10.2 Buying property in the UK remains attractive to both foreign and domestic criminals seeking to conceal large amounts of illicit funds, disguise their ownership, realise the proceeds of their criminal activities, or even see an investment return on them. Based on HM Revenue & Customs (HMRC) estimates, around 100,000 properties are sold every month in the UK and statistics from the anti-money laundering (AML) supervisors' annual returns to HM Treasury in 2019 show that thousands of UK LSPs offer conveyancing services.[1] Although it is likely that the majority of properties in the UK are bought with legitimate funds, it is also likely that thousands of properties in London have been bought with illicit funds over the years and that hundreds of millions are laundered through conveyancing across the UK.[2]

10.3 Although further evidence is needed to ascertain geographical conveyancing risks, it is likely that criminals favour locations with high value residential properties such as London or university towns due to high demand and potential investment return opportunities. However, commercial properties are also attractive for money laundering purposes, as they often carry an equally high price.

10.4 Not all conveyancing poses the same level of risk of criminal exploitation. Red flags indicating a higher risk of money laundering may include (but are not limited to):

- clients seeking anonymity buying property through complex corporate structures, such as companies based in secrecy jurisdictions which can mask the ultimate beneficial owner.
- clients buying the property without a mortgage from a financial institution with no verifiable source of income justifying their wealth.
- conveyancing transactions that involve multiple LSPs.
- customers that are PEPs from high corruption- risk jurisdictions and those charged with or alleged to have committed corruption offences.

10.5 For more details on the risks associated with the property sector see chapter 12.

Trust and company service providers (TCSPs)

10.6 Consistent with the findings of previous NRAs, we continue to assess there is a risk that negligent or complicit LSPs unwittingly or willingly facilitating money laundering through their provision of trust and company services (TCSPs).[3] Of the almost 25,000 UK registered businesses providing TCSP

[1] 'UK property transactions statistics September 2020 provisional data update', HMRC, October 2020.

[2] 'At Your Service', Transparency International, October 2019, identified 421 properties worth £5 billion bought with suspicious wealth over the years.

[3] The MLRs define a TSCP as a firm or sole practitioner which by way of business, forms companies or other legal persons; acts as or arranges for someone else to act as a company director, partner or nominee shareholder; provides a registered office or business address or similar; and/or acts as or arranges for someone else to act as a trustee for a trust or similar arrangement. The provision

services in the UK, approximately 23% of these are LSPs providing this service on top of their core MLR supervised activity. While the majority of trusts, partnerships and companies are formed for legitimate reasons, and TCSPs are not requisite to the abuse of legal entities and arrangements for illicit purposes, TCSPs can assist in their exploitation for money laundering.

10.7 An LSP can offer multiple TCSP services, including company formation, nominee directorship, registered office and trusts, all of which attract a different level of risk. If TCSP services are coupled with other risk factors such as complex structures intended to conceal beneficial ownership or parties outside the UK, the risk may increase. See chapter 11 for more detail on the risks associated with company formation and other trust and company services LSPs may offer.

10.8 The risk of money laundering through TCSP services provided by LSPs can be heightened by poor compliance with the MLRs. In 2018, the Solicitors Regulation Authority reviewed 59 law firms in England and Wales carrying out TCSP work. They found that a significant amount of firms were not doing enough to meet their MLR obligations. More than a third of the firms lacked appropriate risk assessments and some had none at all. A quarter of firms did not adequately manage risks around Politically Exposed Persons and some did not conduct ongoing customer due diligence. Only 10 firms had submitted a Suspicious Activity Report (SAR) in the last 2 years.[4]

10.9 Similarly, in 2020, the Law Society of Scotland published a thematic review on 30 Scottish law firms providing TCSP services. They found firms failed to acknowledge or consider the risk of their TCSP services in their risk assessments, policies, controls and procedures. They also found that some firms had poor AML file management and inadequate ongoing monitoring of client relationships.[5] Four of the selected firms progressed to further reviews where significant deficiencies were found.[6] For full details of the risks associated with trusts and companies please read chapter 11.

Misuse and exploitation of client accounts

10.10 The NRA 2017 found that client accounts are at risk of being exploited by criminals to move illicit funds to third parties. We consider this continues to be a risk as the use of client accounts is attractive because it breaks the audit trail, facilitating the laundering of funds. LSP supervisors have strict rules on how their members should handle client money. However, recent cases suggest that client accounts remain at risk of exploitation by criminals and that criminals are employing methodologies such as sham litigations and fraudulent investment schemes through client accounts.

10.11 LSPs often use client accounts to hold and move money on behalf of their clients for related legal services. Money may move through these accounts rapidly and in large sums to third parties. It is also possible that criminals are

---

of TCSP services involves various professional service sectors including ASPs, many of which provide these services as add on services to their core business activity.

4 'A thematic review of trust and company service providers', Solicitors Regulatory Authority, May 2019.

5 'Trust or company service provision by the Scottish legal profession', Law Society of Scotland, February 2020.

6 'Trust or company service provision by the Scottish legal profession', Law Society of Scotland, February 2020.

using new forms of payments such as cryptoassets or crowdfunding to obscure the origins of funds.

Other risks

10.12 Recent civil society research suggests the UK court system is vulnerable to being exploited for money laundering. Money could be laundered when criminals, often those from overseas jurisdictions, agree to sue each other in the English court with the payment of damages being used to launder their funds. They can also arrange to bring cases against themselves using sham companies.[7]

10.13 Similarly, research suggests that notary services could be exploited for money laundering by willingly or unwittingly verifying forged documents to help customers obtain overseas bank accounts.

10.14 There is an acknowledged intelligence gap on the risks associated with the services provided by barristers and notaries but no evidence to suggest that the level of risk has changed since the last NRA. This intelligence gap is being address through the Intelligence Sharing Expert Working Groups (ISEWGs) and building closer intelligence and information sharing relationships between the relevant PBSs and law enforcement.

10.15 Legal sector PBSs also noted that several firms had asked about receiving payments in cryptocurrencies or money raised through crowdfunding. We are unsighted on how frequent such requests are however, it is likely that they will increase as cryptoassets grow in popularity. While use of cryptoassets alone is not necessarily suspicious, cryptoassets can be used to disguise the origin of funds more easily than other payment methods.

Terrorist financing

10.16 The risk of terrorist financing through legal services is **low.** We continue to assess that legal services are not attractive for terrorist financing and there remains no evidence of these services being abused for terrorist financing purposes.

Supervision, compliance and law enforcement response

Supervision and compliance

10.17 The large number of legal sector supervisors and the lack of a nation-wide data collection mechanism on cases involving professional enablers prevents a better understanding of the risk in the sector. Likewise, the poor compliance of a significant minority of LSPs has enabled criminals to exploit legal sector services for money laundering purposes. However, the recent changes in the regulatory landscape of the legal sector as well as the creation of (OPBAS) and the National Economic Crime Centre (NECC) are

[7] For example, https://www.thetimes.co.uk/article/oligarchs-launder-dirty-cash-in-our-courts-z93kzprzq.

positive steps towards a coordinated response to addressing risks in the sector.

10.18 In Scotland, the legal sector is regulated by the Law Society of Scotland. Police Scotland has an collaborative working relationship with the Society, with intelligence sharing between both agencies in relation to legal practitioners or legal firms believed to be involved in criminality.

10.19 Most LSPs comply with their AML obligations and legal PBSs have found an improvement in their technical compliance with the MLRs among their populations. However, there is more work to be done as PBSs are still finding that a significant minority of LSPs do not focus on AML compliance and some still lack an understanding of the risks they face. This increases the risk of legal services being exploited by criminals as there are insufficient or no controls in place.

10.20 Key non-compliance trends in LSPs observed by PSBs include:

- many LSPs treating AML compliance as a low priority or a tick box exercise which comes second to their day job.
- insufficient or weak risk-based controls in place.
- a lack of legal sector specific AML training available for LSPs

10.21 There has been a significant improvement in the capacity and capability of legal sector PBSs since 2017. Changes to the MLRs in 2017 has boosted supervisors' capability to tackle non-compliance in their sector. Likewise, OPBAS has begun to address inconsistencies in the AML supervision of the legal sector, identified in the Financial Action Task Force's (FATF) 2018 UK Mutual Evaluation Report, as part of their assigned action under the Economic Crime Plan. This includes providing legal sector PBSs with expectations on consistency, raising the standards of supervision, and increasing coordination and intelligence sharing across supervisors.

10.22 OPBAS have assessed the 12 legal PBSs against their sourcebook and are monitoring PBSs' action plans to address identified weaknesses. [8] To further ensure consistency, the legal sector PBSs have participated in 4 workshops held by OPBAS to cover areas of commonly identified weakness: governance, risk-based approach, supervision and intelligence and information sharing. Legal PBSs have also attended a number of roundtable sessions held by the Economic Secretary to the Treasury, John Glen, where legal PBS senior leaders were recognised for their progress so far in addressing weaknesses. However, messages were reinforced of the importance of OPBAS's work and that the government expects more to be done to tackle illicit finance in the professional services sectors.

10.23 In their 2020 report, OPBAS observed a notable increase in PBSs having appropriate governance arrangements for AML supervision; improvements in the application of a risk-based approach and an increase in PBSs undertaking

[8] There are 9 Legal PBSs are listed on Schedule 1 of the MLRs but OPBAS has oversight of an additional 3 legal PBSs in England and Wales who have been delegated regulatory functions from their representative counterparts following the Clementi Review.

proactive AML supervision.[9] However, low levels of enforcement and an inconsistent approach taken to non-compliance in the sector may fail to create sufficient deterrents for LSPs to comply with their AML obligations. The full impact of changes in AML supervision by the legal PBSs continues to be tested and assessed by OPBAS for effectiveness; this will be a focus of OPBAS supervision in 2020 to 2021.

10.24 Intelligence and information sharing have also improved with OPBAS and the NECC establishing the Intelligence Sharing Expert Working Groups (ISEWGs). Likewise, wider public-private partnership work on private to private known suspicion information sharing will explore the feasibility of a mechanism to share information, both within and across sectors, on bad actors who have been exited or refused a service. This aims to improve the effectiveness of know your customer (KYC) and customer due diligence (CDD) processes at the point of taking on a client to reduce the number of customers firms are required to exit.

Law enforcement response

10.25 OPBAS, in conjunction with the NECC and the Joint Money Laundering Intelligence Taskforce (JMLIT), established the ISEWGs in 2018 to 2019 to increase the sharing of intelligence between PBSs, statutory AML supervisors and law enforcement. The ISEWGs were created to offer a platform for strategic and tactical intelligence to be shared and enable communication between supervisors and law enforcement, and enable a greater understanding of the threat which supervisors can take account of in their supervisory activities. For the legal sector, there have been 4 strategic sessions to date and all 12 legal PBS supervisors are members of the ISEWG, as well as the NECC, the FCA and HMRC.

10.26 The recent creation of the NECC and the ISEWGs facilitated by OPBAS are good steps towards better intelligence sharing on lawyers. Through the ISEWGs, OPBAS has seen a rise in intelligence centred communications shared between law enforcement and the PSBs, including regular use of the section 7 gateway.

10.27 As mentioned in chapter 9, targeting professional enablers is a priority for the NECC in its response to money laundering. The NECC has established a dedicated practitioners group to formulate a pipeline of cases for enforcement action. The Enablers Practitioners Group (EPG) also serves to inform best practice and share operational learning on professional enablers across the law enforcement community. Complex financial crime investigations can be hindered by the need to deploy specialist investigation skills, including forensic accountants, and the NECC has utilised the EPG to identify these resources across law enforcement and make them available to operational case teams.

10.28 There still continues to be a low proportion of SARs submitted by LSPs relevant to their risk profile. However, according to the UK Financial Intelligence Unit (UKFIU) 2020 annual report, the number of SARs reported

[9] 'Anti-Money Laundering Supervision by the Legal and Accountancy Professional Body Supervisors: Progress and themes from 2019', OPBAS, March 2020.

by the legal sector has seen an increase of 13% in 2019 to 2020 compared to the same period in 2017 to 2018.[10] This number has continued to increase over the past year. The SARs guidance working group, including reporting sectors, the UKFIU, OPBAS and supervisors, is engaged with the sector on developing updated guidance. There is recognition that further work is required to improve effectiveness of the SARs reporting by the sector; improving the quality and effectiveness of information provided, as well as the percentage of LSPs who report SARs will help towards addressing this issue.

Box 10.A: Case study 1

10.29 Mr. Smith was sentenced to 3 years imprisonment for mortgage fraud and money laundering. He used complex arrangements involving some off-shore limited companies in overseas jurisdictions such as Belize and Delaware in the US. He also used friends and acquaintances in the UK to hold or deal with the assets on his behalf. Smith owned a number of properties through offshore companies to conceal the fact he was the ultimate beneficial owner. He contracted a solicitor to carry out the sale of the properties posing as an 'employee' of the companies with a Power of Attorney.

10.30 The buyer's solicitor was anxious about buying property from an offshore company so Smith transferred the property for no monetary value to another front company based in the UK that an acquaintance operated for him. Smith's conveyancing solicitor continued to accept instructions from Smith despite the change of customer and transferred the proceeds of the sale to the account of Smith's partner in Spain and the business account of one of the front companies operated by his acquaintance thereby enabling money laundering.

Box 10.B: Case study 2

10.31 In 2018, Neil Richard Bolton was banned from practicing after he was sentenced to 9 months in prison following his conviction on 7 counts of failing to comply with the money laundering regulations. Bolton dealt with conveyances in a way that facilitates mortgage frauds through the dishonest acquisition of properties by clients as he failed to comply with the money laundering regulations. Files were found with no identity documents or inadequate proof of identity. His failure to carry out appropriate customer due diligence enabled several criminals all of whom were subsequently convicted of serious criminal

[10] 'Suspicious Activity Reports (SARs) Annual Report 2018', NCA, November 2018, and 'Suspicious Activity Reports (SARs) Annual Report 2020', NCA, November 2020.

offences including drug dealing, mortgage fraud tax evasion and money laundering to acquire properties.

Box 10.C: Case study 3

10.32 Mr. Jiang had used the proceeds from operating an unregistered money service business to purchase a £710,000 property in the UK as a cash buyer. Solicitors acting as conveyancers did not conduct due diligence to enable them to identify the ultimate source of these funds. Jiang pleaded guilty in June 2019 to failing to comply with a requirement, contrary to regulations 45 and 26 of the Money Laundering Regulations 2007.

Box 10.D: Case study 4

10.33 There have been reports that London law firms are repeatedly approached by potential new clients based in overseas jurisdictions asking firms to represent their company in a dispute with a business based in the UK. In some instances, firms have conducted initial checks and then sent their terms. The potential client accepts these and then proposes transferring the law firm a significant sum of money as upfront payment on account. Days later, the client informs the law firm that they have unexpectedly resolved their dispute and request the refund of their upfront payment, minus a fee for initial time. Doing so makes this money now appear clean.

Box 10.E: Case study 5

10.34 Mr. Jones was convicted in April 2019 of fraud and money laundering and sentenced to 8 years in prison. Mr. Jones and his associate Mr. Brown who had been previously convicted of fraud visited a solicitor to buy a property for £350,000. The name on the solicitors' file was then changed to Mr Brown's partner. Between the 18th December and the 12th February 2019 Jones and Brown's solicitor received a series of unsolicited electronic payments into its client account totalling £250,025. The funds had originated in their entirety from the bank account of a limited company (Company A) for which Brown's partner was, at the time of the transactions, again a director and the sole authorised signatory.

10.35 In accordance with Money Laundering Regulations the solicitor contacted Brown's partner seeking proof of the provenance of the funds on several occasions but no evidence was provided. Mr. Brown changed the name of the property to be bought several times and

eventually notified the solicitor he needed the money back. The solicitor submitted a consent SAR asking for permission to pay the money back to the client, the permission was refused and the money was ultimately forfeited via POCA. Had the solicitor refunded the upfront payment received on their client accounts they would have enabled money laundering.

Chapter 11
Companies, partnerships and trusts

Company, partnership and trust risk scores		
	2017 Risk Score	2020 Risk Score
Company and partnership risk scores		
Money laundering	High	High
Terrorist financing	Low	Low
Trusts Risk Scores		
Money laundering	Low	Low
Terrorist financing	Low	Low
TCSP Risk Scores		
Money laundering	Medium	High
Terrorist financing	Low	Low

Summary and risks

- The 2017 NRA highlighted that companies and trusts are known globally to be misused for money laundering, and as a global financial centre the UK is particularly exposed to criminal exploitation of these activities. There remains insufficient evidence to quantify the exact extent of money laundering through UK companies, partnerships and trusts, but the vast majority are assessed to be used for legitimate purposes.
- The possibilities to create complex structures and enhance anonymity makes a corporate structure an attractive tool for criminals, and their use is regularly identified within money laundering investigations. This may be supplemented with other services provided by Trust and company service providers (TCSPs), for example 'shelf' companies which provide banking and credit history, together with nominee shareholders or directors.
- We continue to assess that there is a high risk that UK companies and partnerships will be abused for money laundering. This is unchanged from the 2017 NRA. Changes since 2017 have targeted some of the vulnerabilities identified, for example by extending Persons of Significant Control (PSC) registration to Scottish limited partnerships (SLPs). Since then, the number of registrations of new SLPs has greatly reduced though it is unclear if this has

reduced the use of SLPs overall, for either legitimate or illegitimate purposes. However, other vulnerabilities within the framework to establish and verify companies and partnerships persist, maintaining their attractiveness for money laundering. Planned reform will further improve the transparency and oversight of the UK framework.

- There is little evidence that trusts established within the UK are used for illicit purposes, but government is seeking to expand its knowledge base on trusts. It is too early to determine if the greater registration of trusts through the Trust Registration Service will generate greater intelligence. Overall, the risk of UK trusts being abused for money laundering is assessed to be **low**. This rating is unchanged from the 2017 NRA.
- TCSPs are not necessary for the abuse of legal entities and arrangements for illicit purposes, but they can assist in their exploitation, for example by creating the complex structures which impede investigations or obscure beneficial ownership. Since the last NRA, our understanding of the scale of TCSP use linked to money laundering and risk from them has increased greatly. Based on this, we now assess the money laundering risk from TCSPs as **high**.
- We have seen little evidence of exploitation of trusts, companies or partnerships for terrorist financing purposes. Therefore, the terrorist financing risk is assessed as **low**.

UK companies and partnerships

11.1 UK companies and partnerships continue to be at a **high** risk of being used for money laundering purposes. UK legal entities,[1] such as limited companies, limited liability partnerships (LLPs) and SLPs are exploited to facilitate a range of illicit activity, including large scale money laundering and tax evasion. When PSC requirements were brought in for SLPs, there was a drastic reduction in the registration of them, with incorporations of SLPs falling from 4,932 in 2016 to 2017, to 2,689 in 2017 to 2018, and falling further to 657 in 2019 to 2020. Although England and Wales limited partnerships (EWLPs) and Northern Ireland limited partnerships (NILPs) do not offer a separate legal entity, unlike SLPs, there was a significant rise in registrations of these structures in 2017 to 2018, when PSC requirements were introduced for SLPs. Although, the total of new registrations was a fraction of the reduction in new SLPs.[2] The number of incorporations of EWLPs and NILPs has since returned to pre-2017 to 2018 figures. While we have no firm evidence of abuse of EWLPs and NILPs, it is likely that some of this demand was driven by criminals seeking to exploit EWLPs and NILPs for illicit purposes. As of June 2020, there are now estimated to be over 4 million companies registered. The vast majority of these are used for legitimate purposes.

[1] Legal entities include: public and private limited and unlimited companies, Scottish general partnerships, Scottish limited partnerships and (all) limited liability partnerships.

[2] For England and Wales Limited Partnerships, 1,415 were registered in 2017-18 compared with 645 in 2016-17, with comparable figures for NILPs being 349 registration in 2017-18 compared with 73 in 2016-17.

11.2 Corporate structures are used globally for money laundering schemes, particularly where they offer opacity that can be exploited to conceal beneficial ownership. UK companies and partnerships are likely to be particularly attractive for money laundering due to the UK's international reputation for trade and finance and rule of law. While UK legal entities may be involved in money laundering schemes, and the legal entity can disguise the origin of the funds or make them appear legitimate, these funds do not necessarily flow through the UK. This means that due diligence typically sits in the jurisdiction where the transaction takes places, and UK authorities may not become aware of these transactions or accounts unless brought to their attention. Criminals benefit from the implied trustworthiness of the UK legal entity but are not necessarily subject to the same anti-money laundering and counter-terrorist financing (AML/CTF) checks as a company with an account held by a UK bank.

11.3 There are several factors that continue to make UK companies and partnerships vulnerable to being used for money laundering purposes. While the UK has reporting requirements in place for legal entities and arrangements, as well as a requirement for UK companies, LLPs and SLPs to provide information of their people with significant control to Companies House, there remains gaps that can be exploited to disguise beneficial ownership and control of entities and their assets. Creating complex, multi-layered structures can help keep beneficial owners anonymous, particularly if entities within the chain are based overseas in secrecy jurisdictions.

11.4 UK legal entities can be set up within a matter of hours, very cheaply, and with few barriers. If they are set-up directly with Companies House rather than through a TCSP, there is no requirement to go through AML/CTF checks. Furthermore, overseas TCSPs can form companies directly through Companies House and are included in the list of formation agents on the Companies House website. Entities have been found to breach national reporting requirements by falsely declaring themselves dormant or providing inaccurate identity information to Companies House, who are not in a position to know otherwise.

11.5 The Department for Business, Energy & Industrial Strategy (BEIS) and Companies House are taking steps to increase the transparency of companies and other legal entities through Limited Partnership Reform and Corporate Transparency and Register Reform programmes. See paragraphs 11.30 to 11.32 below for more details.

11.6 It is difficult to ascertain the extent to which different legal entities and arrangements are used to facilitate money laundering. There is strong evidence of UK limited companies, LLPs and SLPs being abused to facilitate the laundering of millions of pounds. For example, in BEIS' 2018 consultation on Limited Partnership Reform, it was noted that the National Crime Agency (NCA) has identified a disproportionately high volume of suspected criminal activity involving Scottish limited partnerships, and there have been prominent examples of them featuring in international money laundering schemes that have made international headlines.[3] While there is

[3] 'Limited Partnerships: Reform of limited partnership law.', BEIS, April 2018.

less evidence of the abuse of EWLPs and NILPs and they do not offer the separate legal entity granted by SLPs, there is a possibility that they could still be used within opaque corporate structures, or used in overseas jurisdictions where their legal status may not be properly understood. It is likely that these structures are attractive for money laundering purposes due to the lower reporting requirements on those that ultimately control the partnerships, compared with legal entities. For example, registrations for NILPs increased by 582% in 2017 after the requirement for PSC information on SLPs was introduced, though the number of registrations has since fallen back to pre-2017 levels. The Government has announced plans to modernise limited partnership law, which would improve the transparency of these kinds of structures and make them easier to understand (see paragraph 11.31 below).

11.7 The lack of evidence of UK companies and partnerships being used for terrorist financing means the risk is still assessed to be low.

Trusts

11.8 The misuse of trusts for money laundering remains a global problem, particularly in the role they play in the layering of funds. They can be used (often alongside corporate entities) to create complex structures which increase the difficulty of identifying if they are being used for illicit purposes or investigating illicit funds held within, and can provide anonymity to individuals, slowing down investigations and protecting the proceeds of crime. However, trust arrangements are often more complicated to establish than companies or partnerships, with a different legal status and utility, and are more likely to require professional support to establish. The transfer of control of assets may also make them unattractive to some criminals. Due to these factors, and the limited evidence of UK trusts being used for illicit purposes, the money laundering and terrorist financing risk for UK trusts is assessed as low.

11.9 Within the UK, law enforcement agencies rarely encounter abuse of UK trusts in high-end money laundering investigations. Overseas trusts are likely to be more attractive for illicit purposes as they can offer better levels of secrecy and tax advantages compared to UK-based trusts, while removing funds beyond the UK's AML/CTF regime and the investigatory powers of UK law enforcement.

11.10 Trusts are established for a range of legitimate purposes. These include but are not limited to: managing assets on behalf of vulnerable persons, including children; jointly holding property; ensuring inheritance is distributed in accordance with a person's last will and testament; performing commercial activity; and conducting charitable work. Each type of trust has different levels of utility, restrictions and requirements, meaning that they all carry different levels of risk.

11.11 The 2017 Money Laundering Regulations (MLRs) legislated for a UK central registry of trusts with tax consequences, maintained by HM Revenue & Customs (HMRC). This Trust Registration Service had 107,500 registrations as

of 5 March 2019. This excludes a significant volume of trusts, including bare trusts which do not generate tax consequences to trustees. The transposition of the EU's Fifth Money Laundering Directive (5MLD) broadened the scope of the trusts register, but given the low evidence base for the use of UK trusts in money laundering, the effect on money laundering risk is uncertain.

11.12 Where trusts are abused by UK-linked criminals, they are almost invariably administered offshore, including in several Unexplained Wealth Order cases managed by the NCA.

11.13 The introduction of beneficial ownership registers for corporate entities in several overseas jurisdictions may make them less attractive for money laundering purposes overall, but these registers do not apply to trusts, so they will likely remain attractive for criminal purposes. It is also possible that other jurisdictions which have not introduced registers for beneficial ownership will become increasingly popular destinations for criminals and corrupt elites to deposit their illicit proceeds.

Trust and company service providers (TCSPs)

11.14 TCSPs can be exploited, either wittingly or unwittingly to enable the laundering of significant illicit flows through companies, partnerships and trusts. They often offer services which can enhance the attractiveness of companies and partnerships to criminals, for example increasing anonymity or creating complex structures. While it is assessed that the majority of UK TCSPs adequately risk assess their clients and seek to understand the nature of their customer's business activity, it is almost certain that a relatively small number do not fully understand the risks involved. Evidence has demonstrated the laundering of millions of pounds through UK legal entities established by TCSPs. The risk of TCSPs being used to facilitate money laundering is therefore rated **high**.

11.15 Although UK companies and partnerships can be set-up directly with Companies House with comparative ease and low cost, approximately half of corporate entities are still established through TCSPs. TCSPs offer a convenient method to establish a company for legal purposes, but many of their services can be exploited by criminals, including the use of nominee directorships, UK mail forwarding services and providing a registration address for hundreds of companies at single addresses. This is particularly attractive for those establishing a UK company from overseas, since the company must have a UK registered office to serve as its official address but is not required to operate in the UK or have a UK bank account.

11.16 Other services can enhance the vulnerabilities of companies, partnerships and trusts discussed above. For example, TCSPs often sell 'shelf' companies; these are reputable companies with established banking and credit histories or nominee shareholders and directors. These are attractive to criminals because once purchased, the criminal can more easily hide their money laundering behind the reputable history and further conceal true ownership information.

11.17 The provision of nominee shareholders and directors by some TCSPs can also be high-risk. This is particularly the case where TCSPs offer directors where the directors have no understanding of the business and no oversight of its operations, or where they offer directors who are already the director for 20 or more companies.

11.18 It is likely that a high proportion of high-risk TCSPs are in the minority of stand-alone TCSPs supervised by HMRC. These include specialist company formation agents and virtual office providers, which are often skilled in the layering of corporate structures and use of anonymity provisions to clients. There are about 23,400 UK registered businesses that provide TCSP-related services and 24 different UK TCSP supervisors. For most, TCSP activity is not the firm's core business activity; this is usually another supervised activity such as accountancy (approximately 16,800) or legal services (approximately 5,400) but can include non-supervised activity, such as management consultancy. In such cases, the TCSP activity is usually carried out on top of other work regulated by its Professional Body Supervisor (PBS). Such companies can combine TCSP services with other professional services such as legal or accountancy provision. The interlinking of TCSP services with other professional services is at high risk of being used to create complex legal structures. See chapter 9 on accountancy service providers and chapter 10 on legal service providers for more detail on the risks in these sectors.

11.19 There appears to have been significant consolidation in the TCSP sector, with the number of HMRC-supervised TCSPs declining from 2,640 in 2014-15 to 1,366 in 2018 to 2019. Over half of all company incorporations in 2018 to 2019 were undertaken electronically by just 106 companies, many of whom are TCSPs. The high level of competition in the TCSP sector likely creates additional risks, for example companies often attract customers by offering the rapid incorporation of companies. Systems are available to conduct rapid customer due diligence (CDD), but it is likely that such services are at increased risk of attempted criminal exploitation. The sale of shelf companies is often also advertised as a time-saving benefit, but they can also serve illicit purposes by creating a false impression of longevity.

11.20 UK TCSPs can provide services directly to overseas TCSPs. Overseas TCSPs are not subject to the UK MLRs, and beyond the European Economic Area, they are subject to varying levels of regulation. This increases the risk to UK-based TCSPs due to low CDD carried out by overseas TCSPs. TCSPs are also sometimes unsure of the authenticity of identity documents presented during the CDD process, with several examples identified by HMRC where individuals were unwilling to provide identity documents.

Terrorist financing

11.21 The risk of terrorist financing through trusts, companies or partnerships is low. We continue to assess that these are not attractive for terrorist financing and there remains no evidence of them being abused for terrorist financing purposes.

Supervision, compliance and law enforcement response

Compliance and supervision

11.22 As has been discussed earlier in this chapter, high levels of competition in the TCSP sector likely creates vulnerabilities through the need to provide rapid registration services to customers, and the potential for poor CDD this implies. The lack of resources available for CDD, training and AML decision-making in smaller TCSPs exacerbates this problem. Non-compliant TCSPs will often use generic policies, controls and procedures not tailored to their business or specific customer patterns.

11.23 It is possible for a TCSP to have complied with the MLRs but still have been utilised for illicit purposes for example, because it was provided with false CDD information which it failed to detect. It is also possible for a complicit business to present a façade of apparent compliance.

11.24 Due to the range of possible professional service providers which may undertake TCSP activity, the supervision regime remains diverse. This includes the Financial Conduct Authority (where it supervises entities for other purposes), the 22 PBSs for legal and accountancy service providers, who are supervised by Office for Professional Body Anti-Money Laundering Supervision (OPBAS), and HMRC. HMRC hosts a TCSP register populated by the PBSs and can supply information from the register to law enforcement agencies on request. PBSs are required to notify HMRC if members report undertaking TCSP activity, so the register can also help identify non-supervised TCSPs. The public portal allowing users to verify HMRC businesses includes all HMRC supervised TCSPs.

11.25 OPBAS seeks to strengthen the supervisory regime and ensure that the 22 PBSs provide consistently high standards of supervision. OPBAS also have an assigned action under the Economic Crime Plan to increase the consistency of PBS AML supervision. Since being established in 2018, OPBAS has taken steps to increase the consistency of PBS AML supervision including issuing each PBS with a findings letter outlining their weaknesses, monitoring PBSs implementation of improvements and holding additional workshops to outline expectations and share good practice. OPBAS will continue to assess the effectiveness of PBS AML supervision, including TCSPs, in 2020 to 2021.

11.26 The 2020 OPBAS report outlined improvements in the approach of PBSs to AML supervision. PBSs are also renewing their focus of TCSP supervision utilising tools such as thematic reviews to assess their populations and target their supervisory approach at high-risk areas.

11.27 Most PBSs report having adequate powers to deal with MLR breaches among their supervised populations. Action by PBSs against breaches of the MLRs has however been rare, with most preferring to use disciplinary powers in relation to professional standards breaches, and only one example could be found of where a PBS had revoked membership due a breach of the MLRs.

11.28 More robust supervisory action against UK TCSPs must be alongside the reforms to Companies House outlined below, to ensure that greater supervisory action does not just displace the risk, either to overseas TCSPs or to criminal groups directly setting up their own UK companies and partnerships.

Policy changes

11.29 The Persons of Significant Control register was expanded in June 2017, requiring SLPs to file their beneficial ownership information. We are unable to determine what impact this has had on the abuse of legal entities and arrangements for money laundering purposes. Gaps remain that enable UK legal entities and arrangements to be abused for money laundering, including the establishment of PSCs outside of the UK beyond the reach of UK law enforcement, limited data quality and validation checks, and poor CDD checks by some TCSPs.

11.30 BEIS' Corporate Transparency and Register Reform programme and their Limited Partnership reform programme will address many of these vulnerabilities. Newly announced proposals for Corporate Transparency and Register Reform will improve the accuracy and usability of the data on the companies register, helping us know who is setting up, managing and controlling corporate entities. Greater legal powers to query and seek corroboration on information submitted, closer work with law enforcement and other partners to support investigations and an improved analytical capability will help to detect suspicious activity earlier and hold those responsible to account.[4]

11.31 BEIS published their response to their Limited Partnership reform consultation in December 2018 and are now working to implement their proposed measures. This will include further work to explore whether to require beneficial ownership information from corporate partners that do not already hold a PSC register. This will take into account the value to law enforcement of this information; their relevance to the UK's compliance with international standards; the existing reporting requirements of these entities; and the potential burden of introducing these reporting requirements.[5] Further potential reform includes making it mandatory for presenters of new applications for registration of limited partnerships to demonstrate that they are registered with an AML supervisory body, and to provide evidence of this on the application form, more stringent requirements on demonstrable links to the UK, greater reporting requirements and greater powers for the Registrar to strike off limited partnerships that are now dissolved or which the Registrar concludes are not carrying on business or in operation. These will all serve to reduce the opportunities to misuse limited partnerships and improve the quality of information of the register.

11.32 The introduction of discrepancy reporting in January 2020 as part of 5MLD, is also improving the quality of beneficial ownership data held on the PSC

[4] 'Corporate Transparency and Register Reform Government response to the consultation on options to enhance the role of Companies House and increase the transparency of UK corporate entities', BEIS, September 2020.

[5] 'Limited Partnerships: Reform of Limited Partnership Law. The Government response to the consultation.', BEIS, December 2018.

register. Obliged entities are required to notify Companies House when it identifies a discrepancy between the information it holds and that held by Companies House. As of August 2020, there had been over 3,000 reports submitted so far.

11.33 The UK has also expanded the trusts register as per 5MLD to require registration of UK express trusts and 2 further sorts of trusts.[6] It is too early to ascertain how the information provided by greater registration will assist law enforcement agencies and other authorities in tackling the misuse of trusts.

11.34 There is ongoing work to improve the capability of law enforcement agencies in tackling the threat posed by overseas trusts. The 2017 NRA noted that every Crown Dependency and Overseas Territory with a financial centre had signed up to the Common Reporting Standards (CRS), the new global standard for tax transparency, under which CDOTs will share details of financial accounts (including trusts) which are held in their countries and belong to UK tax payers with HMRC.

11.35 Most CDOTs with financial centres have also developed private central registers of corporate beneficial ownership. Information in these registers are accessible to UK law enforcement agencies through bilateral arrangements. These arrangements were assessed in a UK Statutory Review, which was published in June 2019, and found to be providing highly effective support to UK law enforcement investigations. Access to this information has enabled the seizure of illicit funds, including a case with an approximate value of £25 million. See paragraphs 4.32 – 4.38 for more details on the risks associated with CDOTs.

Law enforcement response

11.36 The 2017 NRA drew attention to the low levels of Suspicious Activity Reports (SARs) submitted by TCSPs since the 2015 to2016 reporting period. This downward trend continued with the sector seeing a 41.5% decrease in reporting for the period 2019 to 2020 compared to the 2017 to 2018 period. However, the trend partially reversed this year, with the UK Financial Intelligence Unit (UKFIU) reporting a 34.78% increase for 2019 to 2020, compared to the 2018 to 2019 period.[7] It is accepted that TCSPs may also be reporting SARs as either legal or accountancy service providers. The decline in SARs is also likely due in part to the drop in number of TCSPs who identify as a TCSP rather than being part of the accountancy or legal sectors. However, the level of reporting may also be due to a lack of awareness

[6] UK express trusts with taxable consequences are already required to collect information on beneficial ownership and register with HMRC's Trust Registration Service (TRS). New regulation 45ZA now widens the scope of trusts required to register to include all UK express trusts, including those with no tax consequences, with explicit exemptions for some categories of trusts. Non-UK trusts are also required to register where the trust has at least one UK resident trustee and enters into a UK business relationship, or where the trust acquires an interest in land in the UK.

[7] The significant percentage fluctuations between reporting periods should be viewed in the context of the low number of SARs reported in this sector each year. Suspicious Activity Reports (SARs) Annual Report 2018', NCA, November 2018, and 'Suspicious Activity Reports (SARs) Annual Report 2020', NCA, November 2020; Suspicious Activity Report (SARs) Annual Report 2019, NCA, November 2019

among reporters, a lack of resources needed to submit reports, or the lack of penalties for not doing so. .

11.37 The National Economic Crime Centre (NECC), working with law enforcement partners including HMRC, has developed a plan to address the illicit finance risks associated with the TCSP sector. The NECC is identifying those TCSPs which represent the highest risk to the UK, and is tasking supervisory and/or law enforcement bodies to take appropriate action against them. The NECC is also improving the law enforcement intelligence picture in relation to TCSPs. This enriched intelligence picture has also been used to inform the government's corporate transparency reforms. For example, it has allowed the NECC to identify core vulnerabilities within the current corporate transparency framework relating to the TCSP sector, and the NECC has engaged with BEIS on behalf of its partner agencies to share their views in the Corporate Transparency and Register Reform consultation.

Box 11.A: Abuse of overseas trusts

11.38 A business owner who avoided tax by under declaring profits from his business laundered the funds by using a trust based in Gibraltar. The trust was set up and money transferred to the trust from bank accounts in the UK, with the assistance of a complicit accountant. The beneficiary was recorded as his daughter, and funds were transferred to bank accounts in Cyprus believed to have belonged to his daughter, but the money was later used to purchase property for the business owner.

Box 11.B: UK-based TCSPs providing services to overseas TCSPs

11.39 A UK based TCSP provided LLP, SLP and other legal entities to 2 non-UK based TCSPs (one based in Latvia, one in Cyprus). The UK-based TCSP considered the overseas TCSPs the customers, had met them and assessed them as low risk. The UK TCSP did not raise suspicions when products used to favour anonymity were requested and failed to monitor suspicious patterns of behaviour (for example, after legislative changes introduced a requirement for one director of a company be a natural person, the intermediaries requested SLP/LLP arrangements instead).

Chapter 12

Property, estate agency businesses and letting agency businesses

Property, estate agency and letting agency risk scores		
	2017 Risk Score	2020 Risk Score
Property risk scores		
Money laundering	Medium	High
Terrorist financing	Low	Low
Estate agency risk scores		
Money laundering	Low	Medium
Terrorist financing	Low	Low
Letting agency risk scores		
Money laundering	N/A	Medium
Terrorist financing	N/A	Low

Summary and risks

- The property sector faces a **high** risk from money laundering, due to the large amounts that can be moved through or invested in the sector, and the low levels of transparency. Since 2017, law enforcement agencies have observed increased overseas buyers and overseas cash flows into the UK property market. Money laundering cases involving the ownership of property by overseas individuals and companies are inherently complex and their greater occurrence has increased investigative resource constraints. This coupled with a greater understanding of abuse in the sector has led to an increased risk score.

- Estate agency businesses' (EABs') facilitation of property purchases puts them at a **medium** risk from money laundering. The increase in score since 2017 is again a result of a greater understanding of the risks in the sector and the increase law enforcement has observed in money laundering cases involving overseas buyers and use of complex structures.

- As of 10th Jan 2020, letting agency businesses (LABs) are now subject to the Money Laundering Regulations (MLRs) when letting a residential or commercial property for more than €10,000 per month. This NRA therefore assesses LABs separately to estate agents as their risk profile differs. Although there is still a lack of complete understanding of the mitigations and vulnerabilities in the LAB sector, the ability to conceal the beneficial

owners and final destination of funds, and the regular flow of funds make it attractive for money laundering. This NRA assesses the risk of money laundering through LABs to be **medium**. This risk score assesses the risk of the sector as a whole, not just within LABs captured under the new MLRs.

- The sector as a whole is facilitated by a range of service providers, including legal services, estate & letting agency services and financial services, and often features the use of corporate structures. Therefore, the NRA chapters relating to all these services should also be read alongside this one to fully understand the interconnectedness of sectors when money is laundered through property.
- We have seen very little evidence to suggest that UK property transactions are used for terrorist financing and assess the risk of terrorist financing in the property sector, estate agency businesses and letting agency businesses to be **low**.

Property purchases

12.1 UK property purchases remain an attractive method to launder illicit funds due to the large amounts that can be moved and the low levels of transparency of ownership or source of funds. Purchases made by corporate structures or trusts based in secrecy jurisdictions pose the greatest level of risk, due to the difficulties in determining the ultimate beneficial owners. The inherent complexity of these structures alongside their increased use since 2017 and the increased investigative resource requirements this brings, are assessed to result in the property sector being at a **high** risk of money laundering.

12.2 Properties can be purchased via several facilitators. Estate agents, auction houses and 'off-market' agents are required by law to be registered for supervision. However, there are others responsible for the sale of properties that are not subject to the MLRs or the Estate Agents Act such as house builders, who can sell properties directly to the client. While some construction companies may be subject to regulations, not all are captured by the MLRs. This provides opportunities for property purchases without any checks on the buyer or their source of funds.

12.3 Criminals often purchase properties as long-term investments and to release their criminal funds. The high amounts of money that can be moved in one transaction and the appreciation in value, along with the enhanced lifestyle, makes them very attractive to criminals.

12.4 However, properties are also purchased and sold as a method to layer criminal funds. Criminals may abort transactions, manipulate values and turn-around purchase and resale in short timeframes. While the speed of money movement involved in property purchases is slow compared with other methods, the large volumes that can be moved, and the accessibility of the sector are likely to still make property an attractive laundering method.

12.5 Property is particularly attractive for high-end money launderers looking to conceal large sums of money in few transactions. In particular, super-prime

property[1] is considered to be high-risk due to its location in highly desirable areas as well as its significant economic value. Super-prime property commonly features in investigations into grand corruption and money laundering.

12.6 Corrupt foreign elites continue to be attracted to the UK property market, especially in London, to disguise their corruption proceeds. Property can be bought through complex systems of shell companies registered overseas in secrecy jurisdictions to obscure ownership, rendering the true purpose and origin of money transactions unclear. For example, research by Transparency International has found that 75% of properties linked to corruption are owned by companies registered in secrecy jurisdictions.[2]

12.7 Further evidence is needed to ascertain geographical risks, but it is likely that criminals favour locations with high value properties such as London, Edinburgh or university towns, with London in particular considered highly desirable for overseas entities to operate a residential or commercial base in. Importantly, commercial properties located outside of these regions can facilitate money laundering due to their high value and the ability to conceal large sums of money as legitimate commercial transactions.

12.8 As in 2017, residential property is deemed to be a higher risk than commercial property. This is due to the high client turn over as well as the speed and ease of selling on properties. However, commercial property, particularly office and retail space, remains attractive and the complex, opaque company structures used by overseas entities are less likely to raise suspicion in the commercial sector compared with the residential market. Furthermore, commercial property may be purchased by criminals as premises for cash intensive businesses involved in money laundering.

12.9 The full scale of laundering through the UK property sector is unknown. Money laundering likely only makes up a small part of overall property transactions, but the amounts moved are still significant. For example, Transparency International have identified 513 properties in the UK that have been bought with suspicious wealth,[3] with a combined value of more than £5 billion. This is likely only a small proportion of the total proceeds of crime invested in UK property.

Estate agency businesses

12.10 Estate agency businesses (EABs) facilitate the purchase and sale of properties and therefore estate agency services are at **medium** risk of money laundering. Many EABs do not handle client money however, their relationships with both the buyers and sellers of properties can provide crucial information to identify suspicious transactions. Conducting customer due diligence checks on both the buyers and sellers of properties, as required

[1] In the context of this document, super prime property refers to property which is considered in the top 5% of the most valuable property in a geographical area/postcode. The prices of super prime property can vary, but the common requirements are that the property is of high value and highly desirable for the location.

[2] 'Corruption on Your Doorstep, How Corrupt Capital is Used to Buy Property in the UK', Transparency International, March 2015.

[3] Property purchased by PEPs from high corruption risk jurisdictions, individuals with corruption allegations against them, or those charged or convicted with corruption offences.

by the MLRs, collects important information on the beneficial owner of properties and their source of funds. Failure to conduct these checks can mean an EAB unwittingly facilitates the laundering of funds.

Letting agency businesses

12.11 Certain letting agency businesses became subject to the MLRs as of the 10th Jan 2020. Only those who let land or property for a month or more, at a rent of €10,000 or above, are covered by the Regulations. Rental land and properties above this threshold are considered attractive for laundering illicit funds due to their high value. However, money laundering can be facilitated at lower rent properties and our understanding of the risks in this sector are still limited. Based on the understanding we do have and the lack of mitigations for much of the sector, we assess the risk of money laundering through the LAB sector as a whole to be **medium**.

12.12 All LABs are required by law to perform right to rent checks on tenants, however customer due diligence (CDD) is only required on the small number of tenancies over €10,000 per month. As a result, it is possible for there to be high levels of anonymity within the lettings sector, including the landlord, tenant and other interested parties and clients.[4] Landlords may have purchased the property with illicit funds, tenants may be paying rent with illicit funds (as a realisation of their proceeds), or the landlord and tenant may be part of the same criminal group, laundering their funds under the guise of rent payments. This anonymity is exacerbated by the potential exposure to high-risk jurisdictions when letting agents pay rent into offshore accounts without knowing the ultimate beneficial owner.

12.13 The volume of funds that can be laundered through rental properties varies greatly across property location and type. However, significant volumes can be moved on a regular (usually monthly) basis. The median monthly rent for residential properties in the UK is £690 per month, rising to £1,473 per month in London. A large market enables multiple lets, increasing the flow of funds.

12.14 Unlike EABs, LABs handle client money, including fees, deposits and rent, which brings increased risks. Funds are often moved quickly, especially when properties are rented for under the €10,000 threshold for MLR checks, as deposits can be taken without performing CDD. Increasing demand for rental property (7 tenants chasing every new property) makes it normal for deposits to be transferred on the day of viewing. Although in instances where properties are over the €10,000 threshold, all checks and CDD must be completed before accepting any deposits, mitigating the increased risk associated with higher amounts and the fast transfer of funds.[5]

Terrorist Financing

12.15 The risk of terrorist financing through the property sector is **low.** We continue to assess that the purchase or sale of property is not attractive for

[4] 'Client' refers to current or prospective customers of the relevant business such as the vendor, buyer, landlord, tenant, authorised occupier, guarantor and other relevant parties to the transaction, such as a trustee holding a tenancy on behalf of a minor.

[5] For further information, see HMRC guidance for EAB and LABs.

terrorist financing and there remains no evidence of properties being abused for terrorist financing purposes.

Supervision, compliance and law enforcement response

Supervision and compliance

12.16 Overall, estate agency businesses continue to have a lot of weaknesses in their anti-money laundering and counter-terrorist financing (AML/CTF) controls, limiting the mitigations against the risk of money laundering in the sector. Common failings are the lack of bespoke policies, controls and procedures aligned with an appropriate risk assessment of each firm's clients. This includes a lack of consideration of property location on the risk (e.g. failing to recognise that higher priced London property is at higher risk of money laundering). This is particularly true of EABs that operate solely online, with no face-to-face relationship with clients. Likewise, many EABs do not conduct sufficient ID checks, particularly on customers based overseas. Some EABs, have an overreliance on ID checking software which they do not fully understand. HM Revenue & Customs (HMRC) has found many firms who assume that the software they use automatically checks for PEPs and sanctioned individuals without realising that this functionality is only available via the premium version of the package, which the EABs have not purchased. HMRC has identified that larger EABs with multiple branches usually have the right policies and risk assessments in place but fail to adequately audit their branches for compliance.

12.17 As in 2017, is it assessed that a large number of EABs continue to operate without being registered with HMRC. In 2019, HMRC identified that 50% of EABs advertising properties for sale at £5 million had failed to register with them for AML supervision or had failed to pay their annual fees. Action against those businesses is ongoing. Of those registered, HMRC has found that firms do not always have sufficient training in place for staff.

12.18 The cost of compliance may be one factor influencing the levels of compliance with the MLRs. There is a high level of competition within the housing market therefore, EABs may be deterred from fully conducting CDD in case they lose out to less compliant competitors. Likewise, the fractured nature of transactions, involving various regulated professionals, may influence EABs to rely on others such as lawyers to conduct CDD, believing the risk or responsibility lies with others in the process.

12.19 A lack of information sharing between EABs, lawyers and lenders further hinders the identification of money laundering. This also applies to information sharing between the relevant supervisors. The multiple supervisors across all these professional services can limit identification and collaboration on common issues without effective coordination between them. This is being addressed in part by the Intelligence Sharing Expert Working Groups (ISEWGs) founded by the Office for Professional Body Anti-Money Laundering Supervision (OPBAS) and the National Economic Crime Centre (NECC). HMRC is a member of both the legal and accountancy sector

ISEWGs and have intelligence sharing capabilities with professional body supervisors in both sectors.

12.20 HMRC has continued to build its supervision of EABs, including educating their supervised businesses through the launch of an online guide, as well as broader outreach programmes. HMRC publishes a list of businesses which they have sanctioned for failing to comply with regulations. In Sept 2019, HMRC added to this list a £215,000 fine for Countrywide estate agency group. The fine reflected the group's failure to ensure that its money laundering procedures and record keeping were in line with the regulations.[6] This was publicised at the same time as visits to 50 businesses who were trading while unregistered.

12.21 It is too early to determine the compliance levels of letting agents now in scope of the MLRs. As only a small proportion of letting agents and lets are subject to the MLRs, large gaps remain in mitigation of the money laundering risk in the sector. HMRC analysis suggests there are only around 100 LABs that will be in scope of the regulations, many of whom are already registered as EABs.

Law enforcement response

12.22 Law enforcement agencies have noted an increase in the number of overseas based buyers they are investigating, which adds to the complexity of these investigations and increases the strain on law enforcement resources. Even when buyers are based in the UK, it is not unusual for them to be sourcing their funds from overseas which is a well-established hurdle when investigating these cases of money laundering.

12.23 Properties have featured significantly in cases where Unexplained Wealth Orders (UWO) were sought. UWOs offer many potential benefits in investigations where available information is limited. Seeking a UWO is very resource intensive and costly due to the likely lengthy litigations they attract. The National Crime Agency (NCA) is the only law enforcement agency to have used UWOs thus far. The draft Registration of Overseas Entities Bill is intended to proactively address this problem.[7] This will achieve a greater transparency around overseas entities that own or buy property in the UK by recording the beneficial ownership information relating to these entities. The register is likely to be one of the first of its type in the world.

12.24 There are various civil and criminal proceedings which can be used by law enforcement agencies to deny criminals the use of their assets, including UK property. LEAs will, as part of their investigations, seek to remove property derived from or connected to criminality and will utilise the most appropriate legislative tools to do so.

12.25 In 2019 to 2020 estate agents submitted 861 Suspicious Activity Reports (SARs), a 21% increase from the 2017 to 2018 reporting period, which suggests improvements in identifying money laundering activity have been made. However, compared with the overall number of transactions taking

6 See https://www.gov.uk/government/news/estate-agents-targeted-in-money-laundering-crackdown.

7 'Draft Registration of Overseas Entities Bill', BEIS, July 2018.

place within the property sector (1,171,550 residential property transactions over £40,000 in 2019 to 2020),[8] a higher proportion would be expected in line with the size of the sector and its risk profile.

Box 12.A: Case study 1

12.26 Fifty-nine properties worth an estimated £17 million were recovered following NCA investigations carried out over almost a decade into a prolific OCG. In addition to a successful criminal investigation, which saw members of the crime group imprisoned for drug trafficking offences, the NCA conducted 4 linked civil recovery investigations over an 8 1/2 period into dozens of individuals who were suspected of financial or familial links to drug dealers in East Birmingham. NCA officers established that the properties were acquired using the proceeds of crime including heroin importation and distribution, fraud and money laundering. The majority of the 59 properties recovered were private residential properties, which were rented out in the Birmingham area. Three properties were located in the seaside town of Bangor in Northern Ireland. The NCA adopted the first civil investigation into the OCG following a referral from the Police Service of Northern Ireland in December 2011.

8 'UK property transactions statistics July 2020 provisional data update', HMRC, August 2020.

Chapter 13
Cash

Cash risk scores		
	2017 Risk Score	2020 Risk Score
Money laundering	High	High
Terrorist financing	High	High

Summary and risks

- Cash continues to be at high risk of money laundering, with little change in the vulnerabilities that make it attractive to criminals.
- However, since 2017, we have noted a wider number of cash-related services that are abused in money laundering, such as cash deposit services in Post Offices, and the use of cash couriers and cash & valuables in transit companies. Some criminals and professional money launderers are also using alternatives to cash, such as gold and other precious metals or stones, primarily for smuggling out of the UK to countries with large markets specialising in precious metals or stones. The prevalence of the use of these cash proxies is under currently under review by law enforcement agencies.
- The cash methods most at risk can be grouped into 3 categories:
    - movement across the border
    - integration into financial system
    - cash-intensive businesses
- Cash usage in the UK continues to decline, with cash only being used for 28% of payments in 2018, compared with 45% in 2015. While cash use is decreasing, it remains in widespread use for a variety of illegitimate purposes. Additionally, demand for Bank of England banknotes has grown in recent years with the value of total Notes in Circulation (NIC) approximately doubling between 2005 and 2017, largely driven by £20 and £50. This suggests cash remains attractive to criminals.
- Cash remains at high risk of use for terrorist financing, with cases continuing to demonstrate this. Terrorists are known to raise and store funds in cash, and to physically move cash via hand or through cross-border cash couriers. Cash is also deposited into the financial system and moved through formal banking mechanisms or via money service businesses (MSBs).

Movement across the border

13.1 Cash continues to be moved across the UK borders via passengers, freight and cash and valuables in transit (CVIT) companies. While cash in itself is not complicated, criminals continue to employ complex methods to obfuscate its movement and avoid law enforcement detection.

13.2 Sterling continues to be the most frequent currency seized at the UK border, followed by Euros and US dollars.

13.3 It is possible that MSBs are increasingly using the services of CVIT companies to move cash, as an alternative to bank transfers due to de-risking by banks. The risk to MSBs themselves is high (as will be discussed in the next chapter), and the risk is heightened where MSBs use CVITs. There are few barriers to becoming a CVIT company, only a requirement for a Security Industry Association licence. They are not subject to suspicious activity reporting requirements therefore, there are few mitigations to limit the risks.

13.4 Some criminals and professional money launderers are also using alternatives to cash, such as gold and other precious metals or stones. Gold is one of the most commonly seized cash proxies at the UK border and is attractive to money launderers due to its relative portability and stability. Since April 2018, the Proceeds of Crime Act (POCA) 2002 includes powers to seize, detain and forfeit certain items of property including gold and precious stones. This change in legislation has generated an increase in detections and seizures of gold at the UK border. In addition to their viability as an alternative to cash, items such as gold or art and antiquities, can also be associated with trade-based money laundering. The extent to which these cash proxies are a viable and sustainable alternative to cash is currently under review by law enforcement agencies.

Integration into financial system

13.5 Since 2017, we have seen an increase in suspicious cash deposits into bank accounts either through banks' quick-drop cash facilities or via the Post Office.

13.6 The UK Financial Intelligence Unit (UKFIU) has noted a large increase in the number of Suspicious Activity Reports (SARs) reported on suspicious cash deposits at Post Office branches since 2017, with the total for the first 5 months of 2019 (710) almost double that of the same period in 2018 (373). Deposits via a Post Office branch offer greater anonymity and less scrutiny at the point of deposit, as Post Office staff are unable to access the account details of where the funds are being deposited. Likewise, this service offers an opportunity to spread cash deposits more widely, thus limiting suspicion.

13.7 It is likely that suspicious cash deposits via Post Offices have grown due to the increase in banking services they offer as a result of the Banking Framework Agreement in 2017. This seeks to minimise the impact of bank closures by putting satisfactory alternative banking services in place before closing branches; one of these options is the use of Post Office branches.

13.8 UK banks are also increasingly aware of the risks of cash being paid into accounts via third parties. As a result, most high street banks have recently

introduced policies preventing payment of cash into personal bank accounts by anyone other than the account holder.[1]

Cash-intensive businesses

13.9 Cash-intensive businesses continue to be used to clean money. Cash made from criminal activity is documented as legitimate business proceeds and can be placed into company business accounts. Alternatively, it is often reinvested within the UK to fund further criminality or legitimate business ventures. Cash intensive businesses include beauty parlours, newsagents, restaurants, takeaways and car washes. Sometimes, these businesses are linked to modern slavery and human trafficking. See chapter 14 and chapter 17 for more details.

Terrorist financing

13.10 Cash continues to be at a high risk of use for terrorist financing due to it being easily accessible, untraceable, readily exchangeable and anonymous. This means it is very easy to hide the ownerships, origin and purpose or destination of funds, with no audit trail of transactions. No specialist expertise or planning is required to facilitate the use of cash. These vulnerabilities remain unchanged since 2017.

13.11 Terrorists are known to use cash to pay for purchases, including those related to general living expenses as well as those related to attack planning.

13.12 Cash couriering is assessed to be a popular method of moving terrorist funds overseas from the UK, although the full extent of this is unknown. Cash couriering is easily accessible and there is no requirement for specific planning or expertise. The use of high value notes can also make cash transportation easier.[2]

13.13 Destinations for cash have evolved in recent years, with a reduction in funds being moved to Syria. However, it is usually very difficult to determine the end destination of funds leaving the UK. A small subsection of charities operating in high-risk jurisdictions may use cash couriers, which face a higher risk of abuse for terrorist financing purposes than movement via formal banking channels (see chapter 15 for more details).

Supervision, compliance and law enforcement response

13.14 The sector is largely unregulated, with no anti-money laundering and counter-terrorist financing (AML/CTF) regulations for cash intensive businesses (unless they are high-value dealers), providers of merchant-fill ATMs or cash and valuables in transit companies. The Financial Conduct

[1] For more information, see https://www.which.co.uk/news/2018/05/has-your-bank-banned-other-people-from-paying-cash-into-your-account/.

[2] 'Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities', European Commission, July 2019.

Authority supervises banks for their cash deposit services, including the Post Office 'Everyday Banking' services.

Law enforcement response

13.15 Cash continues to be seen in almost every money laundering investigation, and its inherent anonymity continues to provide obstacles for law enforcement in disrupting or investigating its use for both money laundering and terrorist financing. Ongoing work by the Joint Money Laundering Intelligence Taskforce aims to identify instances of money laundering through the facilitation of information sharing between the financial sector and law enforcement agencies. Work to tackle illicit cash movements across the UK border has been identified as a top priority for Border Force, particularly as cash can be used to fund other threats and organised crime.

13.16 Since 2017, cash seizure powers have continued to be used regularly and have significant disruptive effect. There has been an increased focus on cash seizures with a greater number of specialist cash seizure teams at UK ports. As well as seizing and ultimately forfeiting cash at the border, cash seizure teams also actively share information with other government agencies to allow them to act on intelligence relating to individuals who may be suspected of transporting cash out of the UK, including for suspected terrorist purposes.

13.17 Border Force has noted their increased allocation of resourcing for cash seizures has resulted in an increased in cash seizures since 2017. Likewise, a National Crime Agency (NCA) project aimed at tackling money laundering has seized £115 million in cash since its inception, including £21 million in 2019. Each of the UK's 11 regional counter-terrorism police units has a memorandum of understanding with local ports to manage cash seizures. This has led to an increase in cash seizures suspected to be linked to terrorist financing too.

13.18 Amendments to the Proceeds of Crime Act 2002 (POCA) have also enabled law enforcement to seize and forfeit a wider range of items under the definition of cash. This includes gaming vouchers, fixed-value casino tokens, and betting receipts. Other 'listed assets' can also be recovered and this is defined as: precious metals, precious stones, watches, artistic works, face-value vouchers, and postage stamps.

Box 13.A: Case study 1

13.19 In July 2020, UK law enforcement undertook one of its most significant operations to date. Operation Venetic, a collaboration between the NCA, Regional Organised Crime Units and police forces, successfully infiltrated the encrypted criminal communications system EncroChat. EncroChat was one of the largest providers of encrypted communications and offered a secure mobile phone instant messaging service for criminals to communicate. This operation has led to the arrest of 746 suspects and the seizure of over £54 million in criminal cash and cash proxies, including 73 luxury watches.

Chapter 14

Money service businesses

Money service businesses risk scores		
	2017 Risk Score	2020 Risk Score
Money laundering	High	High
Terrorist financing	High	High

Summary and risks

- The risks associated with Money Service Businesses (MSBs) have not changed since the 2017 NRA and the overall risk of exploitation for money laundering and terrorist financing purposes remains **high** overall. We continue to see criminals taking advantage of the services provided by MSBs, in particular those providing money transmission services.
- The 2017 NRA assessed that the money laundering risks varied across the different types of services provided by MSBs, with currency exchange found to be usually lower risk than money transmission. Money transmission also remains higher risk than money exchange and cheques cashing. This is due to the large volume of money they can transfer across borders and the vulnerabilities associated with their reliance on a complex network of agents and subagents to deliver their services.
- This NRA brings more nuance to the finding of previous NRAs and highlights the variations in risks within the money transmission subsector depending on firms' operating models, types of customers, and their level of compliance with the Money Laundering Regulations (MLRs).
- In particular, we find that the risk of MSBs being exploited by criminals is enhanced by key vulnerabilities including the increasing adoption of complex business models by some MSBs. This is partly a consequence of the difficulties MSBs face to access banking facilities in light of de-risking by many banks. The continued prevalence of cash in parts of the sector, the challenges associated with the principal/agent operating model are also key vulnerabilities.
- The MSB sector continues to be assessed as **high** risk for terrorist financing, as key risks identified in 2017 persist. The low cost of transferring funds and the ability to reach a wide number of jurisdictions linked to terrorism continue to make MSBs attractive for moving terrorist funds in small volumes.

- The sector's compliance with the MLRs tends to be poor among small and medium size MSBs as low profit margins may incentivise them to minimise compliance cost. By contrast, large principals tend to make substantial investments in compliance activities.

Money laundering

14.1 MSBs offer a cheap, convenient and easily accessible method to move money anywhere in the world. Cash is common in MSBs, with some customers who may not have ready access to bank accounts at point of dispatch and/or at point of receivership, or some who prefer the use of cash. This makes MSBs attractive to criminals as they can launder the cash proceeds of their crime without attracting suspicion. This risk is exacerbated when the appropriate levels of customer due diligence (CDD) are not followed. The business model of money transmission MSBs, in particular those providing remittance services to high street customers, usually consists of complex networks of principals and agents, as well as agents with multiple principal relationships.[1] While principals may be compliant with Money Laundering Regulations (MLRs) in relation to the activities conducted at their principal premises, not all principals have sufficient oversight of their agents' activities and are failing their obligations with regards to the compliance of their agents. Key issues include a lack of visibility over patterns of transactions, agents with multiple principal relationships that deliberately split transactions to circumvent controls, and a lack of mechanisms to share information between these principals or the agents, making them vulnerable to money laundering.

14.2 MSBs tend to have a high volume of casual customers who they do not maintain long-term business relationships with or formalise such relationships through customer accounts. This makes it more difficult for MSBs to establish the legitimacy of a customer's funds or to detect unusual or suspicious transactions in the absence of a customer transaction history.

14.3 Medium and large commercial businesses that offer currency exchange, global commercial payments and forex services are also high-risk. This is because of the extremely large amounts of money they transfer quickly for lower fees than through a bank; the industry trades £5.1 trillion a day globally, and between 30-40% of that trade is in the City of London. Likewise, their immediate access to foreign, often high-risk jurisdictions enhances the risk. We lack data on the overall percentage of MSBs remitting money to high-risk jurisdiction. However, the Gambling Commission found that out of the 39 jurisdictions MSBs in casinos remitted to and from, 33 were high-risk for money laundering or terrorist financing.

De-risking

14.4 MSBs have been particularly affected by de-risking by many banks, and an increasing number of MSBs no longer have access to banking facilities. As a

[1] The use of the principal-agent model is widespread within the money transmission subsector. Third party businesses, acting as agents on behalf of the principal, typically accept payment and collect identification details from customers, which are then passed on to the principal for electronic transmission. It is the principal's responsibility to ensure their agents' compliance, including the completion of due diligence.

result, more MSBs have opened accounts overseas, rely on other MSBs with a bank account to carry out transactions, or rely on cash couriers to move funds out of the UK. These methods can increase the money laundering risks within the sector. While relying on the account of another MSB is a legitimate business practice, it can also be abused by criminal enterprises. Money from multiple MSBs can be combined and moved together, disguising both origins and destinations. In some cases, payments may move through several MSBs before reaching the banking sector or the final beneficiary. An MSB that receives funds from another MSB is only obligated to conduct its due diligence on its immediate customer, i.e. the MSB, rather than the original source of the funds, although the MSB receiving the funds should consider the wider risk context and apply appropriate policies, controls and procedures to mitigate the risk.

14.5 Criminals exploit weaknesses in this area in order to distance themselves from transactions, confuse audit trails, and provide a plausible deniability for complicit MSBs when confronted on their knowledge of criminal money. It is also likely that de-risking has pushed some MSBs to change their business model to use intermediary payment service providers and informal value transfer mechanisms (IVTS) such as hawala. IVTS providers should all be registered as an MSB, but many operate unregistered. Unregistered MSBs, tend to be hard to detect by supervisors or law enforcement as they can use a mixture of reconciliation processes, such as personal bank accounts, third-party invoice settlement or physical cash movement with little audit trails. It is highly likely IVTS networks launder over £2 billion per year in the UK.

Terrorist financing

14.6 The risk of terrorist financing through MSBs remains high due to continued exposure to high-risk jurisdictions, generally poor compliance outside the largest firms and continued evidence of their abuse.

14.7 It is likely that MSBs are one of the preferred methods to move funds out of the UK for terrorist financing purposes. Typically, funds are sent from family members or close associates to those located with terrorist groups overseas. Vulnerabilities outlined above make them attractive for money laundering as well as terrorist financing: they are a fast, cheap and easily accessible method to move funds to high-risk jurisdictions. Likewise, as in retail banking, the small amounts moved are unlikely to be deemed suspicious by MSBs, and funds can be sent via third countries to reduce suspicion further.

14.8 The business models between principal and agent MSBs outlined above can also negatively impact terrorist financing mitigations. A lack of formal business relationships with customers makes it difficult to detect unusual or suspicious transactions or patterns. This is particularly hard for terrorist financing as amounts are often very low, terrorist financing indicators are common and funds sent are often legitimately obtained.

Supervision, compliance and law enforcement response

Supervision and compliance

14.9 Except for large principals, overall compliance of the sector tends to be poor as MSBs minimise compliance costs due to the low margin nature of the work. Larger MSBs tend to invest more in compliance, including related technology, reducing the risk of exploitation and abuse, although the use of large and/or complex agent networks remains high-risk. Money transmission through MSBs is an inexpensive way of moving a large amount of funds and profit margins are low especially for small and medium size MSBs. The number and concentration of MSBs in retail settings means that competition for business is high. The requirement for footfall means that premises tend to be located in high rent areas. Overall most businesses will be unable to achieve higher than one percent gross profit of total value of transactions handled. Compliance costs can further reduce profit margins and incentivise small and medium MSBs to adopt a minimalist approach to compliance or ignore their obligations. Small and medium size MSBs tend to be more vulnerable to exploitation for money laundering and terrorist financing when they do not invest sufficient resources in compliance.

14.10 Due to the breadth and size of the MSB sector, the oversight of compliance is spread across numerous different supervisors and many different government agencies have an interest in this area. Supervision of the MSB sector is mainly split between HM Revenue & Customs (HMRC) and the Financial Conduct Authority (FCA); HMRC is responsible for supervising most MSBs except those that are financial institutions which are supervised by the FCA. The Gambling Commission also supervises MSBs in casinos. To date, only small numbers of MSBs have been closed or struck off the supervised register as a result of compliance activity and few penalties and warnings applied.

14.11 However, HMRC is increasing its supervisory resource, combined with a more robust approach, underpinned by enhanced targeting, which is resulting in an increase of case closures and sanctions applied. These include prohibitions of management, suspension and cancellation of registrations and significant financial penalties. For example, in May 2019, HMRC imposed a £7.8 million fine on a London-based money transmitter for failure to comply with the regulations.[2]. It found the director no longer fit and proper and cancelled the business' registration. In addition, HMRC imposed a management prohibition on an individual associated with the business.

14.12 Alongside this, HMRC has noted a 19.2% drop in businesses registered and a 19.8% drop in operating premises since August 2017. This is due to a combination of factors including "de-risking" by banks, commercial factors and HMRC's harder-edge approach to supervision.

14.13 The extension of the Fit and Proper test to include all agents of MSBs has improved how these businesses screen agents when onboarding them. The new regulations require that applications for registration must be refused if

[2] See https://www.gov.uk/government/news/money-sender-fined-record-78-million-in-money-laundering-crackdown.

an agent's beneficial owner, officer or manager is determined not to satisfy Fit and Proper standards and HMRC robustly applies this. HMRC has contacted principals showing which agents are not fit and proper, enabling the MSB to exist that relationship. HMRC is also able to cancel a principal's MSB registration if they do not adequately check their agents.

14.14 The Gambling Commission has high levels of capability and adequate levels of capacity to supervise and conduct law enforcement activity against MSBs in casinos. The Gambling Commission has commissioned academic research on MSBs in casinos to gain a detailed understanding of the risks posed by MSBs in their supervised population.

Law enforcement response

14.15 The response to the risks of money laundering through MSBs has been strengthened by greater collaboration between law enforcement agencies, supervisors and the private sector. In 2019, a week of coordinated action between HMRC, the Metropolitan Police Service and the FCA targeted MSBs at risk of being used for money laundering to fund organised crime such as drug trafficking, violent crime and terrorism. While in 2020, joint action between HMRC and City of London Police[3] resulted in 19 MSB registrations being cancelled.

14.16 Likewise, to improve interagency coordination and response to the risks in the MSB sector, an interagency MSB working group was set up in early 2020 led by HMRC. This is important for ensuring all relevant bodies share the same understanding of the risks. Greater systematic intelligence sharing on MSBs between agencies will strengthen this further. To build on these activities and increase coordination across key partners, HMRC, with the support of the National Economic Crime Centre, is also developing an MSB Strategy to reduce illicit finance risks across the sector. The strategy will incorporate input from all supervisors and law enforcement agencies targeting a number of issues, including unregistered MSBs and those identified or suspected of being criminally complicit.

14.17 The overall number of Suspicious Activity Reports (SARs) submitted by MSBs in 2019 to 2020 has decreased by 6.5% compared with the previous year, and 16.5% compared with the 2017 to 2018 reporting period. The decrease is far greater among bureau de changes and cheque cashers, where SAR submissions in 2019 to 2020 fell by 41% and 63% respectively compared with 2017 to 2018. In addition, bureau de change and cheque casher reporting is comparatively low when compared with other MSBs and financial services.

[3] See https://www.nationalcrimeagency.gov.uk/news/multi-agency-action-targets-city-money-laundering.

Box 14.A: Case study 1

14.18 West London money transmitter, Touma Foreign Exchange Ltd, was fined £7.8 million by HMRC for a wide range of serious failures under the MLRs. Between June 2017 and September 2018, the business breached rules on:

- risk assessments and associated record-keeping
- policies, controls and procedures
- fundamental customer due diligence measures
- adequate staff training

14.19 Mr Hassanien Touma was banned on 20 May 2019 from any management roles at a business governed by anti-money laundering regulations after he acted as an officer for the MSB. Individuals are required to pass a vetting test to ensure they are fit and proper to carry out the role, and Mr Touma failed to do this. [4]

[4] For more information, see https://www.gov.uk/government/news/money-sender-fined-record-78-million-in-money-laundering-crackdown.

Chapter 15
Non-profit organisations

Non-profit organisations risk scores		
	2017 Risk Score	2020 Risk Score
Money laundering	Low	Low
Terrorist financing	Low	Low

Summary and risks

- The risks of money laundering and terrorist financing through the non-profit organisation (NPO) sector remains similar to those in 2017.
- The UK's NPO sector is large and diverse. Charities are the most significant component of the sector, by income, risk and by profile. As of February 2020, there were over 214,000 registered charities in the UK with a combined income of over £50 billion. The majority (80%) of UK charities are located in England.
- Consistent with the findings of the previous NRA, this NRA assesses that the NPO sector is not attractive for money laundering and assesses the risk to be low.
- There has not been a significant change in the vulnerabilities or mitigations of the charity or wider NPO sector to terrorist financing since the 2017 NRA. These vulnerabilities are not spread equally across the sector. Rather, among the large number of charities which operate internationally, a significantly higher risk continues to face the small number of charities that operate in or in close proximity to conflict zones. These charities are likely to be exposed to the greatest risk of abuse through misappropriation of legitimate donations by individuals, including nationals stripped of their citizenship due to their prior or continued links or association with terrorist groups, or individuals acting as a partner to the charities themselves. Other inadvertent forms of abuse occur though skimming, incidental theft or opportunistic looting. Overall, the risk of terrorist financing through the NPO sector continues to be assessed as low.
- In the context of the global public health crisis in 2020, the Financial Action Task Force (FATF) has highlighted the crucial work of charities around the world to combat Covid-19 and its effects. The UK government also continues to recognise the work of charities in providing vital services, as well as the difficulties faced in providing that assistance.

Money laundering

15.1 Use of third parties to receive funds, anonymous donations, loans and online fundraising websites are vehicles that could facilitate money laundering in the NPO sector. However, there is limited evidence of abuse of the NPO sector for money laundering and therefore the risk is assessed as **low**.

15.2 There have been no prosecutions for money laundering through the NPO sector in the past 3 years. While vulnerabilities exist within the sector which could be exploited for money laundering purposes, robust financial controls within NPOs should mitigate many of these.

15.3 Anonymous donations are a vulnerability in the sector, but NPOs should have financial controls to verify the identity of all large donors. Donations can be exploited for money laundering purposes if NPOs receive donations from suspicious sources, or donors seek the return of funds. Criminals could also launder funds if NPOs accept a loan in cash then return the loan to the criminal later as a bank transfer.

15.4 The vast majority of donations in the sector are very small. However, criminals may also look to make large donations with their criminally derived funds. Failure by charities to identify the source of these funds mean they receive criminally derived funds, even if they are the end user, rather than a layer within a money laundering process.

15.5 The sector is not very exposed to high-risk jurisdictions, except for those outlined below in relation to terrorist financing. However, there is a risk that high-risk individuals such as non-domestic PEPs may make donations where the source of their funds is unknown, or where third parties make payments on their behalf. This is the case for a number of suspicious donations including to universities, and the payment of services such as independent school fees.[1] In the money laundering scheme known as the 'Azerbaijani Laundromat', funds are reported to have passed through several companies before being used to pay fees for private education in the UK.[2] Due to this laundering method, the school in question would not have immediately known that there was any cause for concern around the ultimate source of these funds.

Terrorist financing

15.6 The NPO sector in its entirety is assessed as **low** risk for terrorist financing. Charities operating and using overseas partners in high-risk jurisdictions face a greater risk of abuse by terrorists that seek to misappropriate their funds or assets than other charities. However, the full scale of abuse is assessed to be low. There have not been significant changes in the vulnerabilities of the sector since the 2017 NRA.

---

1 'At Your Service', Transparency International, October 2019.

2 For example, see https://www.theguardian.com/world/2017/sep/04/uk-at-centre-of-secret-3bn-azerbaijani-money-laundering-and-lobbying-scheme.

15.7 While the level of risk differs with each charity's operating model, a lack of capacity to provide proportionate financial management and organisational assurance could lead to greater risk for smaller charities seeking to operate in high-risk jurisdictions.

Area of operation

15.8 The geographic areas of operation are a key factor in determining the terrorist financing risks faced by charities. There are several thousand charities registered with the Charity Commission for England and Wales (CCEW) and the Office of the Scottish Charity Regulator (OSCR) that operate in areas in close proximity to terrorist groups, such as Syria and Iraq. These are the charities most exposed to terrorist financing risks. The ongoing crisis in the region and the threat from ISIL and other terrorist groups means that these charities are likely to continue to be exposed to inadvertent abuse of funds, including through skimming, incidental theft or opportunistic looting.

15.9 There is a risk that, given the close proximity to Northern Ireland, west Scottish charities may be used to raise money to support Northern Ireland related terrorist activity.

Overseas partners

15.10 Charities often work in difficult and dangerous contexts overseas. Since the NRA in 2017, the majority of terrorist financing abuse in the charity sector is concerned with the suitability of charity partner organisations. Charities often work with overseas partner organisations or individual agents to facilitate their activities. This includes sending funds to international bank accounts for partners to purchase goods more cheaply in country, or to support a partner's project. While charities will have a programme of due diligence in place to assess the suitability of partners, charity partner organisations may be at risk of exposure to designated actors due to the context in which they operate in, including individuals subject to sanctions or citizenship deprivation orders. This can lead to legitimate charitable resources being misused by individuals pretending to be associated with charities, although the risk of this occurring continues to be low. Many NPOs are subject to strict controls and there is no evidence of widespread or systemic abuse in this part of the sector.

Aid convoys and freight containers

15.11 Aid convoys and freight containers continue to be used to transport a combination of goods and cash from the UK overseas which are vulnerable to ending up in the hands of terrorist groups. Although there continues to be a significant decline in the number of land-based aid convoys leaving the UK since 2015, these have largely been replaced by freight containers being sent to Syria via Turkey. There is a risk that funds will be siphoned off by or unwittingly made available to terrorist organisations, including through incidental theft or opportunistic looting of assets.

Cash couriering

15.12 Cash couriering out of the UK continues to be vulnerable to abuse for terrorist financing purposes (see chapter 14 for more details). De-risking by banks or operating in areas without formal banking channels may push some charities towards less regulated and high-risk methods to move funds, including transacting through cash or unregulated MSBs. This will be difficult to detect by law enforcement.

Supervision, compliance and law enforcement response

NPO compliance

15.13 The 2018 FATF Mutual Evaluation found that the UK has a good understanding of the terrorist financing risks associated with NPOs and has been effective in applying a risk-based approach to mitigating those risks and taking action to protect the sector from abuse. In line with the FATF standards, the risk-based approach ensures that legitimate charitable activity is not unnecessarily delayed, disrupted or discouraged.

15.14 Charities are not subject to the money laundering regulations but they, their trustees, employees and volunteers are subject to the Proceeds of Crime Act (POCA) and terrorism legislation. In the UK, charities are also subject to robust civil regulatory regimes by one of 3 charity regulators: CCEW, the OSCR, and the Charity Commission for Northern Ireland (CCNI). The activities that many NPOs undertake such as education or care are also regulated by other government bodies or regulators.

15.15 The number of compliance cases conducted by the charity regulators regarding terrorist financing or money laundering is very low compared with the size of the sector. There have also been no terrorist financing prosecutions related to charities since the 2017 NRA. In a number of cases, when anti-money laundering or counter-terrorist financing (AML/CTF) measures have failed, this has been due to the actions of third parties exploiting weaknesses in unwitting charities' controls, such as weaknesses in governance, inadequate monitoring of overseas partners or insufficient financial controls.

15.16 Smaller charities have fewer resources available which may impact their capacity to employ professional staff and access third-party expertise or advice. Smaller charities operating in high-risk areas are also more likely to be de-banked or experience transaction delays, denials or account closures by their banks due to terrorist financing concerns. As a result, charities may seek alternative methods to transfer funds to speed up the payments to overseas partners which could unintentionally increase the risk of funds ending up in the hands of terrorist groups.

15.17 Since 2017, charities have improved their understanding of the money laundering and terrorist financing. Charities are also increasingly sharing their experience and engaging with both government and regulators, as well as financial institutions. As outlined in paragraph 2.65, this growing

partnership through the Tri-sector Group is building a more open, collaborative and confident approach to understanding and managing terrorist financing risks.

15.18 In his Report on the Terrorism Acts in 2018, the Independent Reviewer of Terrorism Legislation commended the joint efforts of the Tri-sector Group as a welcome recognition that government and the aid sector have a shared interest in ensuring that aid is delivered in hard-to-reach and dangerous places such as Syria and Somalia. He urged continued progress in addressing the problems faced by international non-governmental organisations, noting that the need to ensure counter-terrorism laws do not stifle legitimate humanitarian activity is of international concern.

15.19 The UK government acknowledges the concerns of charities operating overseas in areas subject to counter-terrorist financing measures and sanctions, including the problems of bank de-risking and other potential impacts of over-compliance which may inadvertently increase the terrorist financing or money laundering risk. We are committed to ensuring that the AML/CTF regulations are applied in a clear, effective and proportionate manner and in such a way that does not compromise other government priorities or unnecessarily impede legitimate, often life-saving, activities.

Supervision

15.20 Of the over 214,000 registered charities in the UK, over 180,000 are registered in England and Wales and regulated by CCEW. CCEW has addressed vulnerabilities in the charitable sector in a number of ways to reduce the risk of abuse of, and from within, charities. The mitigations include an effective outreach programme focused on charities identified as higher risk of terrorist financing, issuing guidance[3] on the risks of terrorist financing and money laundering, publishing regulatory alerts when new risks emerge, sharing information and intelligence with partners, ensuring a robust registration process and robustly investigating allegations of terrorist financing or money laundering abuse within the charitable sector.[4]

15.21 The number of terrorist financing and money laundering cases have been broadly consistent in the period since the last NRA in 2017 and as set out above is proportionately low given the size of the sector. The total number of all CCEW cases identified as related to alleged terrorism for the period 1 August 2017 to 6 February 2020 was 1% of the CCEW's total number of compliance cases, and for money laundering was less than 1%. Most of these cases were allegations of money laundering or terrorist financing rather than proven abuse.

15.22 There are approximately 24,800 charities on the Scottish Charity Register, operated by OSCR. All charities in Scotland are required to be on the Register – in contrast to certain exemptions from registration with the CCEW in

3 Guidance: Protecting charities from harm: compliance toolkit, September 2013

4 Regulatory alerts: Charity Commission

England and Wales.[5] Approximately 50% of Scottish charities have low income (less than £25,000 a year). 408 charities operate overseas only, 23 of which are cross-border charities registered with CCEW as well as OSCR. 2,772 charities work both in the UK and overseas, 479 of which are cross border charities.

15.23 Despite the very low incidence and risk of money laundering and terrorist financing through Scottish charities, OSCR provides general guidance, support and outreach activities to mitigate the risks.[6] Since October 2017, OSCR has participated in or run 128 events on a range of regulatory issues, and the guidance has been viewed over 12,400 times over the last 12 months. There have been very few cases where OSCR has been required to take formal action, with only 3 occasions where formal powers were used in 2019. In 2019 to 2020, OSCR implemented a new risk assessment process that deals with concerns about charities to more effectively mitigate potential risk of incoming information being incorrectly assessed. This risk assessment process is based on OSCR's published risk framework. Despite the potential risks and vulnerabilities that do exist, OSCR has not undertaken any investigations into allegations of terrorist financing since the NRA 2017. OSCR dealt with one allegation of money laundering but the case concluded no evidence of money laundering was identified.

15.24 Charities registered with the CCNI are primarily domestically focused. In February 2020 the Northern Irish Court of Appeal issued a ruling into CCNI's delegation of powers to staff. This has raised great uncertainty due to decisions made by staff being ruled to be unlawful. Northern Ireland's Minister for Communities is currently determining how best to mitigate the impact of the judgment to ensure that the regulatory framework established by the Charities Act (Northern Ireland) 2008 can function as effectively as possible until longer term solutions are determined. This represents a change in CCNI's supervisory mitigations since the 2017 NRA and, at this time, means meaningful figures in relation to compliance cases are not available for CCNI.

15.25 There is independent scrutiny of annual accounts of charities, and all independent examiners and auditors have a legal duty to report any matter of material significant to the relevant charity regulator. The UK charity regulators have collectively prepared guidance on this to ensure the reporting duty is fulfilled.[7]

Law enforcement response

15.26 There is close cooperation between the CCEW and law enforcement, particularly the National Terrorist Financial Investigation Unit, including on outreach, engagement, and significant intelligence sharing. Historically,

[5] In England and Wales all charities are required to register with the CCEW unless exempt, excepted or below the annual income threshold of £5,000. The exception to the annual income threshold is Charitable Incorporated Organisations which only come into existence at the point of being entered onto the CCEW's register of charities.

[6] See OSCR

[7] UK Charity Regulators Guidance: Matters of Material Significance reportable to UK charity regulators, April 2020

there have been few Suspicious Activity Reports (SARs) submitted by the charity and wider NPO sector relative to its size.

Box 15.A: Case study 1

15.27 The CCEW conducted an inquiry into a charity, the Anatolia People's Cultural Centre, following concerns that it was being used to promote the actions of the proscribed terrorist group Revolutionary Peoples' Liberation Party Front, aka DHKP/C. The CCEW concluded that the charity was abused for terrorist purposes and that there had been misconduct and/or mismanagement by the trustees as they either consented to or failed to take action to prevent this. In court proceedings orders were granted under Schedule 1 to the Anti-Terrorism, Crime and Security Act 2001 to forfeit the amount of £822.30. In securing the forfeitures, the police told Westminster Magistrates Court that it was their belief that the funds were being collected under the charity's name with the (i) intention to be used for the purposes of terrorism and (ii) that the funds forms part of the resources of a proscribed organisation (the DHKP-C). The police's applications to forfeit the seized funds were uncontested. The charity's trustees were all either removed or disqualified from being trustees and the charity was removed from the register of charities as it did not operate.

Box 15.B: Case study 2

15.28 The CCEW was made aware of an organisation which presented itself as a charity and appealed for funds, despite being unregistered. The sole trustee of the organisation was part of a police investigation into terrorist financing by abusing charitable aid convoys to support a terrorist fighting in Syria. The trustee and 3 other people were charged and stood trial for terrorist financing offences. The trustee and one other defendant were found not guilty; the 2 other defendants were found guilty of terrorist financing offences and sent to prison. Given the serious concerns, the CCEW opened a statutory inquiry into the charitable funds raised on behalf of the organisation. During the police investigation approximately £8,000 of charitable funds were seized from the trustee's properties and assets which the CCEW used its powers to protect, before later using its powers to redistribute the funds to 2 charities with similar objects to the organisation. Due to the trustee's misconduct and/or mismanagement regarding the organisation's funds, they were disqualified as a trustee and/or senior manager for a period of 7 years.

Chapter 16
Gambling

Gambling risk scores		
	2017 Risk Score	2020 Risk Score
Regulated gambling (casinos) risk scores[1]		
Money laundering	Low	Low
Terrorist financing	Low	Low
Other Gambling Risk Scores		
Money laundering	Low	Low
Terrorist financing	Low	Low

Summary and risks

- The gambling sector consists of remote and non-remote licensed casinos, remote and on and off-course betting, remote and non-remote bingo and lotteries, and arcades. Currently, only remote and non-remote casinos are subject to the Money Laundering Regulations (MLRs), with all remaining gambling (referred to here as "other gambling") subject to the Gambling Act 2005 regulations.
- Overall, the money laundering risks in the sector remain **low.** However, within the sector, we consider casinos, off-course betting[2] and all online gambling (excluding lotteries) to pose a higher risk, compared with other sub-sectors. This is due to multiple changes in the services offered since 2017, and the ways businesses operate, which have all created a greater number of vulnerabilities. The key risks within the sector continue to be:
    - poor compliance with the MLRs for casinos and limited application of Proceeds of Crime Act (POCA) requirements for the remaining gambling sectors
    - the sector's exposure to criminals' lifestyle spending
    - criminals using products and services to store and move the proceeds of crime

[1] Regulated gambling includes all online (remote) and land-based (non-remote) casinos.

[2] Off-course betting refers to licensed land-based gambling outside of a racecourse (i.e. in a betting shop).

- high-risk customers (non-domestic PEPs) and high-risk jurisdictions
- peer to peer gambling
- access to multiple remote and non-remote gambling businesses;
- the ability to mask the source of funds

- Despite the increase in vulnerabilities, we assess that the low likelihood of the sector being abused due to its unattractiveness for money laundering purposes and the strong mitigations by the Gambling Commission are enough to keep the overall risk score, for both casinos and other gambling, as low, relative to the wider regulated financial sectors.
- We continue to assess that gambling is not attractive for terrorist financing purposes and therefore, there is a low risk of abuse for terrorist financing.

Casinos

16.1 Vulnerabilities within the casino sector have increased since 2017 due to the diversification of business models. The range of services offered has become more complex, the speed money can be moved has increased, UK-licenced casinos are operating in higher-risk jurisdictions as well as online, they are outsourcing MLR checks more and we know more about the range of methods that can be used to mask the source of funds. However, we assess that the low likelihood of abuse and strong regulatory mitigations in place are enough to keep the overall risk score for casinos as low, relative to the wider regulated financial sectors.

16.2 The number and complexity of services offered by casinos has increased since 2017, which has made them more vulnerable to money laundering. Many casinos are operating in multiple jurisdictions, and many offer money service business (MSB) services which can provide a convenient and quicker method to get funds into and out of casinos and the country. The Gambling Commission has found that money has been sent to and from at least 39 different countries through MSBs in UK casinos, including high-risk jurisdictions. Criminals could consider in-house MSBs attractive as they may perceive there to be less checks, particularly if the customer is already known to the casino. Likewise, an increasing number of casinos are offering concierge-style services, which could increase the money laundering risk, particularly for example, if services include the purchase of luxury goods.

16.3 There is also an increase in the number of casinos using the services of third-party providers, and many are expanding the scope of services that they outsource through them. In previous years, third parties have usually only been responsible for corporate activity such as advertising and marketing. However, an increasing number of casinos are beginning to use third parties for sources of fund and wealth checks. While the outsourcing of this activity is permitted under the MLRs, the casinos retain ultimate responsibility and therefore must ensure the third-party provider is competent to avoid increasing the money laundering risk.

16.4 The speed with which payments can be made to and by a casino have increased since 2017, due to the wider number of payment methods available, which continue to evolve. New payment methods can also increase the ability to mask the source of funds. Casinos, for example, are seeing an increase in payments from pre-paid cards and their use in ATMs located in casinos, which can be more vulnerable to money laundering than bank cards. Industry have noted that it can be difficult to differentiate between a pre-paid card and a bank card, which prevents additional checks being conducted to mitigate the additional risk. For example, pre-paid card transactions through casino ATMs currently cannot be separated from debit cards transactions at the point of withdrawal. A minority of casinos also accept fiat currency payments into customers' accounts from third-party payment providers, where the customer's original deposit to the third-party is in cryptoassets. Casinos remain responsible for ensuring adherence with the MLRs, whether or not third parties are utilised; for example, in satisfying source of funds for customers depositing via a third-party provider.

16.5 Casinos' exposure to high-risk customers and countries has also increased since 2017. The sector has grown since 2017 with gross gambling yields increasing by 10.9%.[3] Most casinos have grown their global footprint, both in terms of international customers and operating in multiple jurisdictions; these often include high-risk jurisdictions. Just under 57% of current casino licence holders are based outside of the UK, across 19 jurisdictions, including 14 jurisdictions the Gambling Commission deems to be high-risk. Likewise, casinos have high-risk customers (one London casino has 110 PEPs as customers) and offer complex services.

16.6 It is also assessed that some cash spent in casinos is linked to South East Asian underground banking. Due to capital flight controls, some South East Asian nationals wishing to gamble in the UK may utilise the services of underground bankers to make cash available for them in the UK, which would not be possible using the regulated banking sector. The South East Asian national would make a bank transfer to the underground banker within their domestic jurisdiction. Once they arrive in the UK, they can then collect the equivalent amount of cash from the underground banker's contact. However, this cash is usually the proceeds of criminality, which the contact has laundered on someone else's behalf.

16.7 The 2015 NRA noted that casinos are vulnerable to criminal control. While we have seen no evidence of casinos under criminal control, the Gambling Commission has identified increasingly innovative attempts to enter the gambling market and have implemented regulatory measures to mitigate this risk. To keep entry to the gambling market rigorous, the Gambling Commission screens applications for both businesses and individuals working in key positions, refuses applications and monitors changes in ownership and where concerns exist with licensees takes necessary steps to mitigate risks. Between 2017 to 2019, the Gambling Commission refused 249 licensing applications, with common themes for those decision being: inadequate evidence for source of funds for the business, revealed criminal

3 'Industry Statistics, March 2017-September 2019', Gambling Commission, May 2020.

convictions for applicants and concerns with inadequate identity for key persons or shareholders within the application.

16.8 All gambling operators in Great Britain are licensed and regulated by the Gambling Commission, with casinos being subject to additional supervision through their inclusion in the MLRs. We assess that widespread adherence to these regulations, and rigorous regulatory and supervisory actions by the Gambling Commission restrict the risks posed by these vulnerabilities. Compliance of firms, and the role of law enforcement and supervisors in mitigating the sector's risk is discussed further in paragraphs 14.10 – 14.17.

Other gambling

16.9 As with casinos, the money laundering vulnerabilities have also increased within all other gambling sectors, due to service providers offering an increased and more complex range of services and accepting a greater number of payment methods, including cryptoasset conversion to fiat currency via third party providers, which increases the speed money can be moved. The sector also continues to grow, in part due to the weaknesses in restrictions on the amount of funds that can be bet online, and the unlimited number of customers that can play at one time. This can increase the likelihood of abuse. However, we still assess that the majority of criminal funds gambled are for recreational purposes rather than laundering, and that there are regulatory measures in place which prevent wide-spread exposure to money laundering.

16.10 The 'other gambling' sector includes many varied sub-sectors. While on balance, we still assess the risk for other gambling to be **low**, we recognise that some sub-sectors pose a higher risk and are demonstrating similar risk levels to casinos. In particular, we assess that retail and online betting, online bingo and peer to peer gambling, such as poker and betting exchange, pose a higher risk, compared with others, such as bingo halls or racecourse betting. As required by the MLRs, we will continue to review whether more sub-sectors should be regulated for anti-money laundering and counter-terrorist financing (AML/CTF) purposes.

16.11 Since 2017, the number and complexity of services offered both in-store and online has increased. It is common for firms to hold multiple licences to offer a wide variety of games, such as betting, bingo, casino and gaming machine style activity. Across all gambling offers, there are around 10 providers offering wide-ranging services, making up 90% of the market. Likewise, as with casinos, firms are also increasingly using third-party providers.

16.12 Like casinos, the diversity of payment methods accepted by retail betting and online betting and bingo firms has also increased, which increases the speed of payments and the ability to mask the source of funds where methods offer greater anonymity.

16.13 We have also learned more about the gambling sector's large exposure to high-risk jurisdictions since 2017. Firms are frequently licensed in multiple jurisdictions with varying standards of AML and CTF frameworks and the UK's framework is challenging for some firms to comply with. Shareholders,

company registrations, bank accounts and licence holders' headquarters are sometimes based in high-risk jurisdictions. The current licensing regime stipulates that any global gambling outlet that services customers in Great Britain must be licensed with the Gambling Commission, regardless of whether it has a physical footprint within Great Britain.

16.14 The Gambling Commission has evidence of laundering of criminally derived monies in the online betting and bingo sector and has assessed there is a high likelihood of the event occurring. Criminals can launder money by placing low risk bets or cashing out funds with little or no play. However, it is unlikely criminals would look to launder large sums using these methods. While criminals may play large sums through online betting or bingo, we assess that this is predominantly for the recreational spending of the proceeds of crime, especially where an addiction to gambling is present, rather than the 'washing' of funds.

16.15 While the barriers to play are comparatively less robust than in casinos, there are still stringent measures in place to mitigate the risk posed by these vulnerabilities and to protect against other crime types and gambling harm. These are implemented through the Commission's Licence Conditions and Codes of Practice framework and include: ID verification for anyone wanting to gambling online; requiring all gambling businesses to conduct a money laundering and terrorist financing risk assessment; and a requirement on businesses with multiple subsidiaries to create a 'single customer view' across its gambling services, to inform decisions about crime and harm.

Terrorist financing

16.16 The risk of terrorist financing in the gambling sector is **low.** We continue to assess that gambling is not attractive for terrorist financing and there remains limited evidence of it being abused for terrorist financing purposes.

Supervision, compliance and law enforcement response

Supervision and compliance

16.17 The Gambling Commission continues to have high levels of capability and adequate levels of capacity to supervise the gambling sector, helping to mitigate the risk of the sector being abused for money laundering and terrorist financing purposes. The Financial Action Task Force (FATF) UK Mutual Evalutation Report in 2018 found that the Gambling Commission had a good understanding of the money laundering and terrorist financing risks in the gambling sector and applied a risk-based approach to supervision. In 2018 to 2019, the Commission carried out an increased level of supervisory activity, compared with the previous year.[4] They have continued to build their understanding of the sector's risks, using their robust powers to collect relevant data from their supervised population, and then interrogate the data with innovative data analysis techniques. However,

[4] 'Anti-money laundering and counter-terrorist financing: Supervision report 2018-19', HM Treasury, August 2020.

their lack of access to Suspicious Activity Reports (SARs) data for regulatory purposes is one limiting factor, which they are working with the National Crime Agency (NCA) and the UK Financial Intelligence Unit (UKFIU) to resolve.

16.18 Their competency has also been reflected in a number of extensive investigations leading to record fines. In 2018 to 2019, the total value of financial penalties issued to the supervised population for AML/CTF failings under section 121 of the Gambling Act (or in lieu of) was £17,005,018. This includes a regulatory settlement of £2,024,046 made by one casino operator, relating to a case of AML/CTF failings.

16.19 While there are strong regulatory and supervisory measures in place, compliance is not consistent across the sector. In 2018 to 2019, c.48% of the casinos subject to a review or onsite visit were assessed to be non-compliant with the MLRs. The Gambling Commission's annual enforcement reportalso notes that compliance activity and enforcement cases revealed that some operators' AML risk assessments, policies, procedures and controls are not fit for purpose.[5] This is particularly true for those operating in multiple jurisdictions, who sometimes assume all gambling regulators' requirements are the same and therefore fail to implement the United Kingdom's MLR requirements.

16.20 The primary AML compliance issue identified for casinos is the frequent disconnect between operators' money laundering and terrorist financing risk assessments and their policies, procedures and controls, including customer risk profiling, customer due diligence and ongoing monitoring; enhanced customer due diligence and enhanced ongoing monitoring, when required. For many operators, this has become a tick-box exercise, without due consideration given to the importance of adopting a risk-based approach and how this impacts upon their ability to implement fit for purpose policies, procedures and controls, and effective employee training.

16.21 While regulated gambling is assessed to be low risk, and the sector continues to make positive improvements, these are not yet extensive enough to have reduced the risks nor do they show a consistent improvement towards the sector's approach to its AML obligations. For example, there is an increased effort to upskill staff, but it is hampered by a lack of training specific to the sector. Likewise, a tension remains between regulatory requirements and commercial drive. Some businesses looking to maximise profits, may look to minimise compliance costs and time, which could negatively impact their compliance with the MLRs and fail to identify money laundering activity.

16.22 The money laundering risks in the gambling sector are exacerbated by the lack of requirement for providers other than casinos to abide by the MLRs. However, recognising the need to achieve parity, where possible, the Gambling Commission has introduced new licence conditions resulting in policies to address customer identity and verification. Likewise, through the Gambling Commission's licensing regime, firms are required to have regard to guidance issued relating to their compliance with POCA and the Terrorism

[5] 'Raising Standards for Consumers - Enforcement report 2018/19', Gambling Commission, 2019.

Act 2000 (TACT), to prevent gambling being used for crime. This includes the requirement to produce a risk assessment. However, these measures are not sufficiently embedded by licensees to fully address the money laundering vulnerabilities within the sector.

16.23 The Gambling Commission is currently consulting upon increased reporting requirements, in compliance with the MLRs, to assist in mitigating both problem gambling and money laundering or terrorist financing. The government will continue to keep the position of other gambling providers under review, as required by the MLRs.

16.24 There has been an upward trend in the casino sector reporting SARs. In 2017, 36% of casino operators submitted SARs, with this increasing to 53% by 2019. The individual number of SARs submitted in 2019 to 2020 by casinos jumped by 24% on the previous year, likely as a result of better outreach and education. There has also been an upward trend in all other gambling sectors reporting SARs. In 2017, 1,848 SARs were submitted by gambling operators (other than casinos), with this increasing to 5,743 by 2019.[6] The individual number of SARs submitted by other gambling operators in 2019 to 2020 jumped by 28% on the previous year, likely as a result of novel engagement methods. For example, in September 2018, the Gambling Commission created a series of 5 videos in partnership with the NCA to improve operators' understanding of the suspicious activity reporting process, which cumulatively have over 3,000 views.[7] While these are positive improvements, there is still more to be done to increase the number of gambling operators reporting SARs, in line with the sector's risk profile. The Gambling Commission and the UKFIU will also continue to work with the sector to emphasise the importance of pro-active reporting, in order to reduce the incidents of defensive reporting in the sector, where businesses only submit SARs after the police have contacted them.

Law enforcement response

16.25 Overall, law enforcement has extensive powers to investigate money laundering through the gambling sector. The Gambling Commission has adequate capacity and capability to conduct these investigations. However, wider law enforcement agencies' work in this sector has been more limited, with a reliance on the Gambling Commission to assist investigations. As a result, it is likely not all opportunities to investigate and use powers are fully explored. For example, under the Criminal Finances Act, police gained the power to seize ticket-in ticket-out tickets and casino chips. However, there have been no reports of these being seized to date.

6 Suspicious Activity Report figures supplied by Gambling Commission covering the period between 2017 to 2019,

7 'Raising Standards for Consumers - Enforcement report 2018/19', Gambling Commission, 2019.

Chapter 17
High value goods and traders

High value good and traders risk scores		
	2017 Risk Score	2020 Risk Score
High Value Dealers risk scores		
Money laundering	Low	Medium
Terrorist financing	Low	Low
Art Narket Participants risk scores		
Money laundering	N/A	High
Terrorist financing	N/A	Low

Summary and risks

- Money laundering through high value luxury and lifestyle goods is one of the oldest money laundering methodologies used by criminals. Goods are purchased and then exchanged back into fiat currency at a later date.
- High Value Dealers (HVDs)[1] are assessed as **medium** risk for money laundering because of vulnerabilities created by anonymity of transactions, portability across borders, exposure to high-risk jurisdictions and level of cash used in the sector, which makes it attractive for trade-based money laundering. The inherent vulnerabilities assessed in the 2017 NRA remain, though the understanding of vulnerabilities has increased. Furthermore, as the registered HVD population declines, and legitimate HVDs move away from cash-operated business activity, proportionately more criminally-inclined HVDs will make up HM Revenue & Customs (HMRC)'s register.
- Art Market Participants (AMPs)[2], from 10 January 2020, are a newly regulated entity under the Money Laundering Regulations 2017 (MLRs). Previously art dealers would only be captured by the MLRs if they were in scope of the HVD definition (dealing in cash transactions of at least €10,000). This NRA therefore assesses AMPs separately to HVDs as their risk profile and their definition differs. The ability to conceal the beneficial owners and final destination of art, as well

[1] The Money Laundering Regulations define a HVD as any business receiving or making high value cash payments of € 10,000 or more, in a single or linked transactions, in exchange for goods.

[2] The Money Laundering Regulations define an AMP as a firm or sole practitioner who by way of business trades in, or acts as an intermediary in, the sale or purchase of works of art and the value of the transaction, or series of linked transactions, amounts to € 10,000 or more.

as the wide-ranging values involved, the size of the market and the international nature of the market make it attractive for money laundering. Likewise, it is too early to fully assess the effectiveness of new mitigations in place by AMPs. Therefore, this NRA assesses the risk of money laundering through AMPs to be high.

- Consistent with the findings of previous NRAs, there remains no evidence of HVDs being abused by terrorists. HVDs and AMPs are not assessed to present an attractive option for moving terrorist funds. Therefore, this NRA assesses that the risk of terrorist financing through HVDs and AMPs is low.

Money laundering in the HVD sector

17.1 At the end of 2019 there were around 470 registered HVD businesses with HMRC. However, it remains inherently difficult to assess the extent of under registration. A HVD could operate in any business sector involving goods; HMRC breaks them down into 18 different sub-sectors.

17.2 The risk profile across the sector is assessed as medium for money laundering because of vulnerabilities created by anonymity of transactions, ability to conceal ultimate beneficial ownership, portability across borders, exposure to high-risk jurisdictions and level of cash used in the sector. Understanding of these vulnerabilities has increased since the last NRA.

17.3 Consistent with the 2017 NRA, the 3 HVD sub sectors which remain to be considered the highest risk of criminal abuse are jewellery and precious metals, cars and vehicles, and cash & carry / alcohol. These sub-sectors account for approximately 55% of registered HVDs. Other sub-sectors considered by HMRC as medium to high risk within the HVD sector risk range include caravans and static vans, high-end retail, and food processing such as abattoirs.

17.4 Volumes of money laundered inevitably vary but the ability to launder significant sums of money through HVDs makes it attractive to criminals. HMRC cases involving registered HVDs found guilty of money laundering offences demonstrate the sums involved when laundering money through high value goods. Case studies shared by HMRC detail many cases involving several million pounds being laundered over one year (see case study section below). Suspicious Activity Reports (SARs) data revealed a 93% increase in the number of SARs involving HVDs between 2017 to 2018 and 2018 to 2019, just after the government's update of the MLRs in 2017. This preceded a 23% decrease between 2018 to 2019 and 2019 to 2020. While variable, this trend does indicate an overall increase in HVDs being targeted by criminals.

Portability of luxury and wholesale goods across borders

17.5 Goods hold their value beyond a country's borders. Therefore, any businesses dealing in high value goods offers a convenient asset that can be used by criminals to transfer and move value, creating a risk of trade-based money laundering and exposure to high-risk jurisdictions. Recent data points

to laundering goods via China and West Africa, with actual payment taking place in the UK.

17.6 HVDs are increasingly vulnerable to elaborate cross-border export laundering schemes. One such scheme involves Chinese underground banking networks providing illicit funds to Chinese university students to purchase high value luxury items in the UK. They then export these to Asia for re-sale.

17.7 HMRC has also seen evidence of money laundering through the sale of general household goods at scale. Such items include toiletries, general clothing and food. Such goods are sold in high volume by registered HVDs to countries, which have strict cash export limits, before cash later arrives in the UK to pay for these goods. Amounts involved can sometimes be inconsistent with expected trading with such countries. This trend is considered an emerging risk and will be monitored further.

17.8 Transparency International's 2019 investigation into a Russian laundromat scheme detailed 422 payments made to 118 luxury goods outlets for services totalling £17.6 million. This case demonstrates the continued attractiveness of high value luxury goods to criminals. Although, some purchases of luxury goods with criminal funds may just be an expression of a criminal lifestyle and realisation of profits, rather than as a money laundering mechanism.

Terrorist financing

17.9 The risk of terrorist financing through high value dealers is **low.** We continue to assess HVDs are not an attractive option for generating or moving terrorist funds.

Money laundering in the art market

17.10 Recent amendments to the MLRs to implement the Fifth Money Laundering Directive extended anti-money laundering and counter-terrorist financing regulatory obligations to Art Market Participants (AMPs) in the UK. The UK art market is considered at **high** risk of money laundering because criminals can conceal the ultimate beneficial owner of art, as well as the source of funds used to purchase art. This can be achieved by using complex layers of UK and offshore companies and trusts, agents or intermediaries, with agents and intermediaries commonly used in the market. Also, the value of art varies greatly, making it attractive to varying levels of criminals, as well as providing options to launder money through a small number of high value purchases or a large number of low value purchases. Furthermore, the international nature of parts of the market likely makes art an attractive commodity for money launderers seeking to move illicit finance into or out of the UK.

17.11 Because the money laundering regulations have only been introduced recently, it is too early to fully assess the effectiveness of new mitigations in place by AMPs. As there has been limited focus by law enforcement or regulators on AMPs until now, there is limited evidence of abuse in the sector. Over time, greater supervisory and law enforcement scrutiny will

allow a better understanding of the level of abuse and the effectiveness of mitigations in place.

17.12 The UK art market is estimated to be worth $14 billion and accounted for 20% of global art sales by value in 2019.[3] According to the United Nations Office on Drugs and Crime, £2.3 billion of the global art market could be linked to money laundering or other financial crime annually.[4] While we are unable to assess the full extent of money laundering through the art market in the UK, the size of the sector, combined with a previous lack of consistent regulation, means the global art market has been an attractive option for criminals to launder money.[5]

17.13 The introduction of AMPs into the MLRs will go some way to mitigate abuse of the sector however, inherent vulnerabilities remain that can expose the sector to risk. As with other regulated sectors, criminals are likely to adapt their modus operandi to circumvent new regulations.

17.14 Under the MLRs, AMPs are now required to conduct customer due diligence on the buyers and sellers in transactions. This includes exhausting all possible means to verify the identity of the customer, or the ultimate beneficial owner. However, as outlined in other chapters (see paragraphs 11.1-11.6 and 12.1), criminals seek to circumvent these requirements using shell companies, companies or other legal arrangements with concealed beneficial ownership (such as those based in secrecy jurisdictions), and other complex arrangements with many layers to disguise the ultimate owner and the source of funds. Third parties involved in the sale of art can complicate and distort this trail further.

17.15 A key element of art transactions involves tracing and verifying the provenance or ownership history of a piece of art. However, this process may not always reveal the ultimate beneficial owner or the source of funds used to purchase the art previously. Likewise, some pieces of art will attract a lot of public interest and scrutiny, but this is likely only for the most expensive transactions; in 2017, art priced at over $1 million, represented just under 1% of the number of individual transactions in the UK's art market.[6] There is therefore a high volume of transactions which are at greater risk of abuse, due to the lower level of attention and scrutiny those sales are likely to attract.

17.16 The price of art varies drastically, from hundreds to millions of pounds, making it accessible and attractive to a wide range of money launderers. Art provides opportunities for both the concealment of large amounts of funds in single transactions, as well as regular trades at lower prices, particularly under the €10,000 threshold for AMPs, which will avoid extensive anti-money laundering scrutiny. In 2017, it was assessed that 61.7% of art sales in the UK were under $5,000.[7]

---

3 'The Art Market 2020', Art Basel & UBS, March 2020.

4 'The Art of money Laundering', International Monetary Fund, September 2019.

5 Ibid

6 'The British Art Market 2017: An Economic Survey', The British Art Market Federation, 2017.

7 'The British Art Market 2017: An Economic Survey', The British Art Market Federation, 2017.

17.17 The high amounts of money that can be moved in one transaction and the appreciation in value as a long-term investment, alongside the enjoyment or status gained by owners makes art very attractive to criminals. It is likely that art purchased with criminal proceeds will often be the realisation of these proceeds, with art kept for a long time, rather than a stage within a layering process requiring a fast resell.

17.18 Art is also assessed to be attractive for money launderers due to the ease with which items can be transported within the UK and across borders. This provides a convenient way to launder high volumes of funds across borders, through relatively small items. While some items of art are subject to individual export licences, to prevent items of cultural significance leaving the UK, a large number are not. Likewise, an export licence is unlikely to verify the final destination of the art or the ultimate beneficial owner. Art is also likely to be less suspicious to law enforcement, when compared with gold or cash.

17.19 The transnational nature of the market means that it is common practice for art to regularly move to other jurisdictions. It is estimated that in 2019, the US art market accounted for 44% of global sales by value, totalling $28.3 billion. After the UK (at $14 billion in 2019 and 20% of global art sales by value),[8] the Chinese market (which includes mainland China, Hong Kong, Macau and Taiwan) has the third largest share of the sector, accounting for 18% at a value of $11.7 billion. The majority of trade in the UK art market is either domestic or with the US, EU countries and Hong Kong. Neither the US or the Chinese market have any anti-money laundering regulations in place for their art markets, meaning transactions with those countries can pose a higher risk. Likewise, paragraphs 4.16 – 4.22 of this report notes that China and Hong Kong pose an increased risk to the UK from a money laundering perspective, due to the extensive business links and the opportunities to disguise illicit funds within these.

17.20 An increase in online art market places and trading platforms, where buyers and sellers can interact directly, could also increase the risks in the sector, representing an even greater move away from face-to-face transactions. These have seen a particular growth since the start of 2020 due to businesses adapting to COVID-19 restrictions.

Terrorist financing

17.21 The risk of terrorist financing through the art market is **low.** The money and knowledge required to purchase and sell these assets in the UK is not conducive to terrorist activity in the UK. Terrorist attacks in the UK in recent years have demonstrated that the costs involved are very low, involving just shop bought knives or the cost of a hire vehicle. Likewise, the amount of time involved in obtaining and selling art is not suitable for quickly organised and executed attacks. The time and liquidity required to use these assets effectively for terrorist financing purposes makes them less attractive than other forms of financing.

8 'The Art Market 2020', Art Basel & UBS, March 2020.

Compliance, supervision and law enforcement response

HVD compliance

17.22 Overall, mitigations against money laundering in the HVD sector are assessed to be limited. Trade in high value goods can give criminals a channel to place illicit cash at high volumes, while appearing legitimate.

17.23 Despite regulatory obligations on the sector to mitigate the vulnerabilities, compliance among the remaining HVD population is assessed to be poor. Many businesses also operate without registering as a HVD with HMRC or operate just beneath the threshold required by the MLRs. Furthermore, many legitimate businesses are choosing to move away from cash-based operations with the growth of alternative payment methods. It makes it increasingly unclear why a business may wish to legitimately maintain HVD registered status. Therefore, it is possible that a greater proportion of HMRC's register will be made up of more criminally inclined HVDs or encounter proportionately more applications from criminally-inclined prospective HVDs.

17.24 Poor compliance and under-reporting have remained unchanged since 2017. At the end of 2018 to 2019 there were 368 HVDs in the UK registered with HMRC. HMRC investigations suggest there are many cash-intensive businesses. Some may deal in high value goods transactions above the cash threshold and have not registered with HMRC, meaning they are operating illegally. HMRC undertakes activity to identify and sanction these dealers. Of HVDs which are registered with HMRC, there is a poor sector capability based on a lack of understanding of risk and poor controls. In 2017 to 2018, HMRC recorded its highest ever number of compliance penalties for HVDs, with HVDs involved in meat processing displaying particularly poor controls, especially record-keeping and critically monitoring and verifying due diligence materials. This reinforces FATF'S 2018 Mutual Evaluation of the UK, which argued HVDs have an inconsistent understanding of their risk. HMRC has found some criminals seeking HMRC registered status to legitimise their criminal activities, further adding to the variance in capability and intent of the sector to mitigate risk.

Supervision of HVDs

17.25 HMRC has been effective at mitigating risks within its registered population of HVDs. However, intelligence gaps remain for those entities dealing in cash just below the threshold or above the threshold but not registered with HMRC, who could be laundering funds through high value cash transactions. However, changes introduced by the 2017 amendments to the MLRs, now cover HVDs making cash payments, as well as those receiving them. This change has brought the whole supply chain into scope, helping HMRC identify a greater number of unregistered HVDs.

17.26 In addition, HMRC applies robust scrutiny to HVD applications. This is enhanced by HMRC's approvals and pre-registration checks. Anyone with a relevant criminal conviction is barred from owning or running a HVD business. Since 2014, only 27% of new HVD applications have been

approved, highlighting the robust scrutiny of applications and extent of inadequate or even fraudulent firms attempting to register. HMRC has also seen examples of HVDs being short-term phoenix companies. The increase in regulatory penalties raised to HVDs visited since the last NRA highlights HMRC's improving capability to mitigate money laundering activity in the sector. It is increasingly difficult for bad actors to gain legitimacy by registering as a HVD. HMRC's effectiveness is limited by its capacity and limited resources, the complicated nature of HVDs means high levels of expertise and skills are required for compliance staff.

Art market compliance and supervision

17.27 Previously, art dealers would only be captured by the MLRs if they dealt in cash above the HVD transaction threshold, with only a handful of registered HVDs involved in art. The 2019 amendments to the MLRs imposed obligations on AMPs when acting in any transaction whose value is equivalent to or exceeds €10,000, not just in cash. AMPs are now legally required to identify and assess the risks of money laundering and terrorist financing in their business and register with HMRC, as well as carry out customer due diligence and report suspicious activity. AMPs who are within scope must register before 10 June 2021, but must carry out their MLR obligations irrespective of their registration status during the transition period. Guidance for AMPs to aide compliance was published by the British Art Market Federation and on Gov.uk in February 2020.

17.28 As the art market is very newly regulated, it is too early to fully assess AMPs' capability and capacity to mitigate the risks and comply with the MLRs. While many AMPs, including the biggest art houses, had controls in place before the anti-money laundering and counter-terrorist financing (AML/CTF) requirement came in, it will take time for all firms to consistently implement appropriate controls. This gives money launderers time to adapt to regulations and maximise opportunities in the market. While the majority will comply with regulations, it is likely that a portion of art market participants will not fully comply with the MLRs as has been observed in other newly regulated sectors, either due to a lack of understanding, or intentionally to encourage trade. For example, some AMPs have expressed concern that customer due diligence and the resulting attempts to increase transparency in the market will reduce trade. Likewise, some AMPS may attempt to continue operating unregistered to avoid scrutiny.

17.29 HMRC, the AML/CTF supervisor for AMPs, is building capability and expertise in order to effectively take action and mitigate risks in the sector. It is also too early to fully assess the effectiveness of supervision in the sector.

Law enforcement response to high value traders

17.30 Law enforcement have specialist financial investigation tools to investigate criminal activity using high value traders and identify criminal assets. There is a good track record of HMRC and law enforcement cooperation to identify unregistered HVDs, some registered HVDs are not even registered with the National Crime Agency to submit a SAR.

17.31 While some specialist knowledge of the art market exists within law enforcement, including the Metropolitan Police Service's Art and Antique's Unit, this resource is small. Limited current focus from law enforcement on the market means there is insufficient intelligence or operational and investigational evidence to draw robust conclusions on the full scale of money laundering the UK's art market. As there was no legal requirement until January 2020 to submit a SAR, intelligence from art market participants has previously been slim.

Box 17.A: Case study 1

17.32 HMRC identified a HVD jeweller purchasing bags of gold in cash without performing a risk assessment or conducting CDD on the seller. The bags of gold were delivered to the business several times. The gold was weighed, and then high value cash payments were made to these persons for the gold, totalling over £2.1 million in 10 months.

Box 17.B: Case study 2

17.33 HMRC visited a well-established cash and carry specialising in toiletries and household products. Records selected for testing showed the business accepted £4 million in relevant cash payments from export customers based in high-risk jurisdictions, in particular Ghana, Pakistan, Nigeria and Sierra Leone. The risks posed by these customers had not been identified or addressed and no consideration given to prohibitions in place surrounding movements of cash from these countries. For example, the removal of cash from Ghana exceeding $10,000 is prohibited, however the business accepted £2.4 million in cash payments from its customers over a 2-year period. As well as direct movements, unknown third parties resident in the UK delivered cash on behalf of the overseas customers without considering the origins of the cash or how the third parties were reimbursed. The business's policies, controls and procedures were insufficient to mitigate the risks of money laundering and terrorist financing.

Annex A
Glossary

5MLD	EU Fifth Money Laundering Directive
AASG	Accountancy AML Supervisors Group
ABP	Alternative banking platform
ACE	Asset confiscation enforcement
AFO	Asset freezing order
AML	Anti-money laundering
AMP	Art market participants
ASP	Accountancy Service Providers
ASD	Automated Services Devices
BEIS	Department for Business, Energy & Industrial Strategy
CATM	Cryptoasset automated teller machine
CCEW	Charity Commission for England & Wales
CCNI	Charity Commission for Northern Ireland
CD	Crown dependency
CDD	Customer due diligence
CFA	Criminal Finances Act 2017
COPFS	Crown Office and Procurator Fiscal Service
CRS	Common Reporting Standard
CSEW	Crime Survey for England and Wales
CSOSG	Economic Crime Civil Society Organisations Steering Group
CTF	Counter-terrorist financing
CPS	Crown Prosecution Service
CTU	Counter-Terrorism Unit
CVIT	Cash and valuables in transit
DAML	Defence Against Money Laundering
DEX	Decentralized exchange
EAB	Estate agency businesses
ECSB	Economic Crime Strategic Board
EPG	Enablers Practitioners Group
EU	European Union
EWLP	England and Wales limited partnerships
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
FCDO	Foreign, Commonwealth & Development Office
FIS	HMRC Fraud Investigation Service
FMLIT	Fraud and Money Laundering Intelligence Task Force
FPS	Faster Payments Service
GCHQ	Government Communications Headquarters
GHR	Global Human Rights
HMRC	Her Majesty's Revenue and Customs
HVD	High value dealer
ICO	Initial Coin Offering
ICU	International Corruption Unit
IEU	Initial Exchange Offering
IVTS	Informal value transfer system
IWT	Illegal wildlife trade

JMLIT	Joint Money Laundering Intelligence Task Force
LAB	Lettings agency businesses
LASIT	Left-wing, anarchist and single-issue terrorism
LLP	Limited liability partnership
MER	Mutual Evaluation Report
MLR	Money Laundering Regulations
MLRO	Money Laundering Reporting Officer
MoRILE	Management of Risk in Law Enforcement
MSB	Money service bureau/business
NCA	National Crime Agency
NECC	National Economic Crime Centre
NILP	Northern Ireland limited partnerships
NIRT	Northern Ireland-related terrorism
NPO	Non-profit organisation
NRA	National Risk Assessment
NTFIU	National Terrorist Financial Investigation Unit
OAC	Organised acquisitive crime
OCG	Organised crime group
ODA	Overseas Development Assistance
OFSI	Office for Financial Sanctions Implementation
OIC	Organised immigration crime
OPBAS	Office for Professional Body AML Supervision
OSCR	Office of the Scottish Charity Regulator
OT	Overseas territory
P2P	Peer-to-peer
PBS	Professional Body Supervisor
PEP	Politically exposed person
PIS	Payment Initiation Service
POCA	Proceeds of Crime Act 2002
PSC	Persons of Significant Control
PSD2	EU Second Payment Services Directive
PSNI	Police Service of Northern Ireland
PPSG	Public-Private Steering Group
PPTU	Public-private threat update
RART	Regional Asset Recovery Team
ROCU	Regional Organised Crime Unit
RECU	Regional Economic Crime Unit
SAMLA	Sanctions and Anti-Money Laundering Act 2018
SAR	Suspicious activity report
SLP	Scottish limited partnership
SOC	Serious and organised crime
SRA	Solicitors Regulation Authority
TACT	Terrorism Act 2010
TAFA	Terrorist Asset Freezing etc. Act 2010
TBML	Trade-based money laundering
TSCP	Trust or company service provider
UKFIU	UK Financial Intelligence Unit
UNSCR	United Nations Security Council Resolution
UWO	Unexplained wealth order

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.gov.uk