



Home Office



HM Treasury

# **National Risk Assessment of Money Laundering and Terrorist Financing 2025**

July 2025

# National Risk Assessment of Money Laundering and Terrorist Financing 2025

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

---



© Crown copyright 2025

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit [nationalarchives.gov.uk/doc/open-government-licence/version/3](https://nationalarchives.gov.uk/doc/open-government-licence/version/3).

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

This publication is available at: [www.gov.uk/official-documents](https://www.gov.uk/official-documents).

Any enquiries regarding this publication should be sent to us at [public.enquiries@hmtreasury.gov.uk](mailto:public.enquiries@hmtreasury.gov.uk)

ISBN: 978-1-917638-34-0 PU: 3536

# Contents

|   |           |
|---|-----------|
| <b>Section 1 - Introduction</b>             | <b>6</b>  |
| <b>Ministerial Foreword</b>                 | <b>6</b>  |
| <b>Introduction to the NRA</b>              | <b>8</b>  |
| Purpose of the NRA                          | 8         |
| Structure of the NRA                        | 9         |
| Methodology                                 | 9         |
| <b>Section 2 - UK AML/CFT Structure</b>     | <b>11</b> |
| <b>UK AML/CTF structure</b>                 | <b>11</b> |
| <b>Section 3 – Money Laundering</b>         | <b>20</b> |
| <b>Money laundering</b>                     | <b>20</b> |
| <b>UK wide Money Laundering risks</b>       | <b>20</b> |
| <b>Money Laundering threat</b>              | <b>22</b> |
| Fraud                                       | 22        |
| Sanctions Evasion                           | 23        |
| Acquisitive Crime                           | 23        |
| Drugs                                       | 23        |
| Cyber Crime                                 | 24        |
| Organised Immigration Crime                 | 25        |
| Tax Evasion                                 | 25        |
| Modern Slavery and Human Trafficking (MSHT) | 25        |
| Online Child Sexual Exploitation and Abuse  | 26        |
| Environmental                               | 26        |
| Bribery and Corruption                      | 27        |
| <b>Money Laundering typologies</b>          | <b>29</b> |
| Cash  | 30        |
| Informal Value Transfer Systems             | 35        |
| Cryptoassets                                | 39        |
| Trade-Based Money Laundering                | 43        |
| Property                                    | 46        |
| Companies and Trusts                        | 50        |
| Professional Enablers                       | 57        |
| <b>Section 4 – Terrorist Financing</b>      | <b>58</b> |

|  |            |
|--|------------|
| <b>Terrorist Financing threats</b>                               | <b>58</b>  |
| <b>Terrorist Financing Mechanisms</b>                            | <b>58</b>  |
| UK SOC – Terrorist financing links                               | 60         |
| International SOC-Terrorist finance links                        | 60         |
| UK-based terrorists  | 61         |
| Terrorist financing by ideology                                  | 61         |
| <b>Section 5 – Sector Specific Risks [ML and TF]</b>             | <b>64</b>  |
| <b>Regulated Activities risks</b>                                | <b>64</b>  |
| Retail Banking   | 67         |
| Wholesale Banking and Markets                                    | 72         |
| Wealth Management  | 77         |
| Insurance  | 79         |
| Electronic Money Institutions and Payment Service Providers      | 81         |
| Cryptoasset Service Providers                                    | 87         |
| Money Service Businesses   | 95         |
| High Value Dealers   | 99         |
| Art Market Participants  | 102        |
| Casinos  | 107        |
| Non-Profit Organisations   | 113        |
| Legal Service Providers  | 118        |
| Accountancy Service Providers                                    | 122        |
| Trust or Company Service Providers                               | 126        |
| Estate Agency Businesses   | 132        |
| Letting Agency Businesses  | 136        |
| <b>Section 6 - Cross Cutting Risks</b>                           | <b>139</b> |
| Artificial Intelligence (AI)                                     | 139        |
| Schools and Universities   | 141        |
| Football Clubs and Football Agents                               | 143        |
| <b>Annexes 145</b>   |            |
| Annex A – Glossary   | 145        |
| Annex B – Legislation, Law Enforcement Agencies, and Supervisors | 150        |
| Annex C – Diagrams   | 157        |
| Annex D - Boxes  | 160        |

# Section 1 - Introduction

## Ministerial Foreword

The integrity and resilience of the UK's financial system are fundamental to our country's prosperity and security. A strong financial system supports jobs, businesses, and families up and down the country. However, the same openness that makes the UK attractive for trade and investment can be exploited by criminals and terrorists who try to move and hide illicit money through our financial system. These activities are not victimless crimes—they fund serious criminal activity, undermine trust in our economy, and threaten the safety and wellbeing of our communities, and can also threaten our national security, making it easier for dangerous groups to plan and carry out attacks.

The National Risk Assessment of Money Laundering and Terrorist Financing (NRA) is a vital tool in our ongoing work to understand and disrupt the evolving threat posed by criminals and terrorists who try to move their illicit money through our financial system. By providing a clear and comprehensive picture of current and emerging risks, the government, supervisors, law enforcement, and businesses can work together to stop money flowing to criminals or those who threaten our security.

The threat from money laundering and terrorist financing continues to evolve, shaped by new technologies, geopolitical tensions, and the increasing sophistication of criminal and terrorist networks. We believe it is important to maintain and strengthen the UK's resilience in the face of these challenges. The NRA is central to this mission; our risk-based approach to assessing and mitigating our money laundering and terrorist financing threats provides us with the evidence base we need to ensure the UK's defences remain strong against these risks, and that we maintain the confidence of our international partners, investors, businesses, and the public.

The NRA contributes to the Strong Foundations pillar of our Plan for Change by helping to prevent money from facilitating crime or reaching actors who threaten our national and economic security. Serious and organised crime – whether fraud, drugs offences, organised immigration crime or other offences, facilitated by money laundering threatens the wellbeing and safety of the British public and communities and undermines the legitimacy and authority of the state. Money can motivate and provide the tools for criminals to carry out their heinous acts. That means it is essential to tackle money laundering so that crime does not pay, victims are compensated, and criminal networks are starved of the funds they need to operate. Targeting money laundering also disrupts kleptocracy, preventing corrupt elites from exploiting the UK's financial system. Similarly, by disrupting all forms of terrorist financing, we make Britain a safer and more prosperous place to live and work.

This NRA highlights both the progress we have made and the challenges that remain. We have seen advances in our collective response, but also a continued increase in risks, including those associated with cryptoassets and other rapidly developing technologies. The NRA reflects the expertise and dedication of partners across the public and private sectors including supervisors and law enforcement, whose work is critical in protecting the integrity of our financial system and economy. We thank all those across government, law enforcement, and the private sector who have contributed to this assessment and urge all partners to continue to engage closely as we implement our response to address its findings.

The findings of the NRA will directly inform our policy, regulatory, and operational priorities and response. For the regulated sector, it provides essential insight into how their services may be exploited for illicit purposes, and guidance on how these threats can be identified and mitigated. By acting on these insights, we are ensuring that everyone involved can respond proportionately to the threats we face, protecting the UK's reputation and making it a safer place to live, work, and invest.

Our commitment to tackling economic crime and illicit finance remains steadfast. This publication sits alongside a range of government strategies, including the Economic Crime Plan 2023-26, CONTEST 2023, our forthcoming Fraud and Anti-Corruption Strategies, and supports our alignment with international standards set by the Financial Action Task Force (FATF). Our aim is clear: to keep criminals' money out of our economy, strengthen the defences of our financial system, and ensure the UK remains a secure and attractive place to do business.

These efforts demonstrate the UK's leadership in the global fight against economic crime and terrorism. Together we can continue to strengthen our defences, protect our economy, and uphold the UK's reputation as a safe and trusted place to do business..

Emma Reynolds

A handwritten signature in black ink, appearing to read 'E Reynolds'.

Dan Jarvis

A handwritten signature in black ink, appearing to read 'Dan Jarvis'.

# Introduction to the NRA

## Purpose of the NRA

- 1.1 The National Risk Assessment (NRA) of Money Laundering (ML) and Terrorist Financing (TF) is the UK's stock-take of our collective knowledge of money laundering and terrorist financing risks. This NRA builds on our understanding of the risks identified in our NRAs in 2015, 2017 and 2020.
- 1.2 The Money Laundering Regulations (MLRs) stipulate that HM Treasury and Home Office must undertake a risk assessment to identify, assess, understand, and mitigate the risks of money laundering and terrorist financing affecting the United Kingdom. Further, the MLRs state that HM Treasury and Home Office must ensure that the NRA is used to consider the appropriate allocation and prioritisation of resources to counter money laundering and terrorist financing. Likewise, the Financial Action Task Force (FATF) expects all countries to conduct NRAs and implement a risk-based regime that responds to the risks identified.
- 1.3 The MLRs also stipulate that supervisors and regulated firms must conduct their own risk assessments, which must take into account this NRA. The NRA and their own risk assessments should be used to put in place effective controls, policies and procedures to mitigate the risks identified and prevent abuse.
- 1.4 The NRA is a central part of the UK's "risk-based approach" to countering ML and TF. The NRA sits alongside System Prioritisation which aims to publish a list of economic crime priorities to inform public-private resource.

### **Box 1.A - System Prioritisation**

As of 2025, alongside the NRA, the UK's economic crime threat priorities are planned to be published annually. These will be published as part of the government's commitments in the Economic Crime Plan 2 2023-26 and will support participating parts of the regulated sector to effectively allocate their internal resources on a cost-neutral basis while maintaining their regulatory responsibilities. More detail can be found [here](#) on this approach.

# Structure of the NRA

## Section 1

1.5 This section covers the purpose and methodology used in the 2025 NRA.

## Section 2

1.6 This section covers the UK's Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) frameworks and how the government has responded to the risks identified in the 2020 NRA.

## Section 3

1.7 This section sets out the overarching ML risks faced by the UK. It explains the main crime threats that generate illicit funds and the main ML typologies. **This section is relevant to all sectors, and should be read in addition to the sector-specific activities section.** There is information in this section about how to relate the NRA to System Prioritisation.

## Section 4

1.8 This section sets out the overarching TF risk faced by the UK. It explains the main nature of the terrorist financing threat in the UK and outlines the layered and often complicated mechanisms through which TF can occur. This includes the mechanisms that are typically used by different types of terrorist organisations.

## Section 5

### Regulated Activities

1.9 This section sets out the ML and TF risk to the UK found in those sectors regulated under the MLRs. This chapter also covers an analysis of risks identified in related sector specific activities not currently covered by the MLRs.

## Section 6

### Cross Cutting Emerging Risks

1.10 This section covers risks in sectors not in scope of the MLRs and activities that have cross-cutting relevance for sectors in scope of the MLRs. **This section should be read by all sectors.**

# Methodology

## **Information gathering**

1.11 The NRA is informed by a wide range of sources and expertise drawn from the private sector, academia, open-source information, law enforcement, supervisors, and expertise within government. Information gathered covers the period since the last NRA.

1.12 Over 250 responses from the regulated sector were gathered via questionnaires and workshops to assess the risks, mitigations, and scale of money laundering and terrorist financing in their sectors and the wider UK economy.

1.13 More than 300 assessments, datasets and questionnaires were received from law enforcement agencies and supervisors. This included Suspicious Activity Reports (SARs) analysis, National Crime Agency (NCA) intelligence assessments of money laundering threats and patterns, His Majesty's Revenue and Customs (HMRC) intelligence and NCA Joint Money Laundering Intelligence Taskforce (JMLIT) alerts. Views were sought from local and regional policing on the particular risks in their areas. Wider data sets including financial, sectoral and demographic trends were also used as part of the data collection exercise.

1.14 Where information referenced can be found in the public domain, a link has been provided. Information that is derived from sensitive intelligence (for example, live case information) has been declassified and, in doing so, it is not possible to link to the origin of this information.

### **MoRiLE methodology**

1.15 An adapted version of the 'Management of Risk in Law Enforcement' (MoRiLE) model has been used to establish risk scores. MoRiLE examines three areas: vulnerabilities, scale and mitigations. Information on vulnerability and scale are used to develop an 'inherent risk' score which is then multiplied by a mitigation factor. Strong mitigations reduce the inherent risk score, but where significant weaknesses exist the score is increased. This exercise generates an overall risk score which is translated to a low, medium or high rating. The same methodology has been used for both money laundering and terrorist financing elements and is in line with the methodology used in the previous NRAs.

1.16 Scores and ratings are moderated by a panel of law enforcement, supervisors and government department sector experts. The thresholds for each level of risk remain the same as those used in 2020. In some cases, the numerical score will have increased or decreased but not sufficiently to change the risk level. Further detail on methodology and factors considered can be found in [section 5](#).

# Section 2 - UK AML/CFT Structure

## UK AML/CTF structure

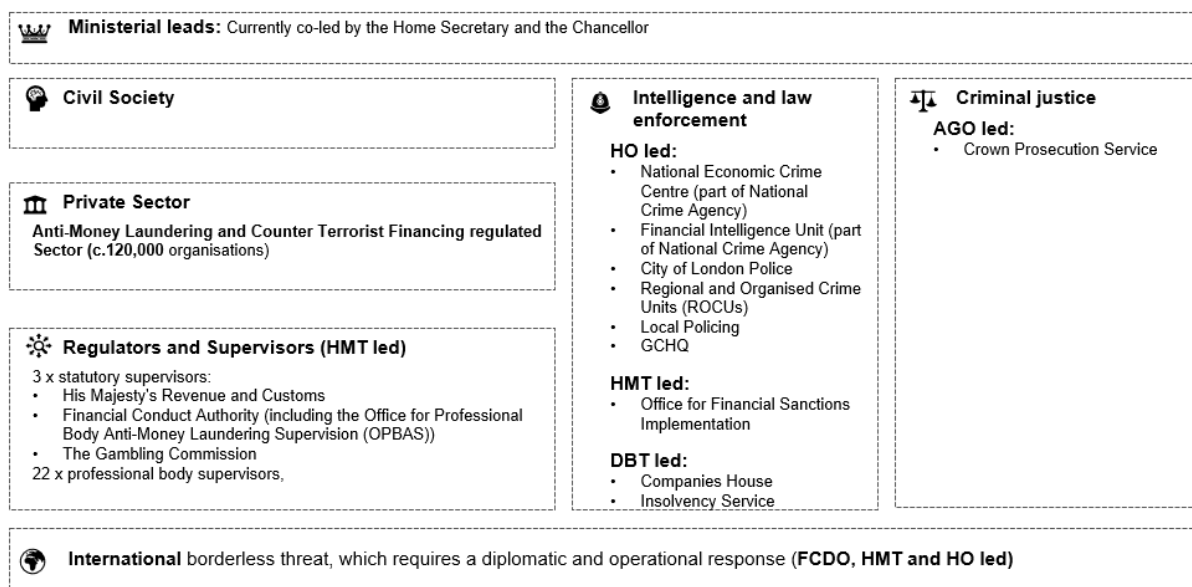
- 2.1 This chapter outlines the legal, regulatory, supervisory and law enforcement frameworks governing the AML and CTF regime in the UK.
- 2.2 The UK has a comprehensive legal and regulatory system which has been regularly reviewed and updated to respond to the changing context and risks faced by the UK. The UK's response to economic crime is a collaborative effort. Policy and legislative ownership lie with central government, led by the Home Office and HM Treasury, with some specific policy areas held by other government departments. The Scottish Government is responsible for criminal justice policy in Scotland. In Northern Ireland, criminal justice policy is overseen by the Department of Justice. These departments work closely with law enforcement agencies and supervisors to provide a comprehensive response.
- 2.3 Legislative measures are complemented by a regulatory framework that supports compliance and oversight. Supervisors, enforcement agencies and intelligence bodies and firms work collaboratively to detect, deter, and disrupt ML and TF. Together, these components form an integrated approach to safeguarding the UK economy from the threats posed by ML and TF.
- 2.4 A large number of law enforcement and government agencies have a role in combatting money laundering and terrorist financing, ranging from local police forces across England and Wales, Northern Ireland and Scotland to national bodies such as the National Crime Agency and HMRC.
- 2.5 There are 25 AML and CTF supervisors which supervise firms to help ensure they comply with the MLRs and other relevant legal and regulatory requirements. Supervision is conducted by three public sector bodies – the Financial Conduct Authority (FCA), HMRC, and the Gambling Commission – alongside 22 professional body supervisors for the legal and accountancy sectors. These 22 supervisors are overseen by the Office for Professional Body Anti-Money Laundering Supervision (OPBAS).
- 2.6 The UK also has a sophisticated and longstanding public-private partnership that underpins our AML/CFT system. Effective public-private partnerships facilitate the sharing of resources, capabilities and knowledge, allowing us to build a whole-system approach to targeting economic crime, which in turn

helps protect businesses and the public. The UK public-private partnership model is underpinned by the second public-private Economic Crime Plan, overseen by the Public-Private Strategic Governance Group.

2.7 The National Economic Crime Centre (NECC) Public Private Partnerships (PPP) coordinates voluntary partnerships between the regulated sector and UK law enforcement. These bring together HM Government, law enforcement and industry, in fora that support information exchange and analysis. This includes thematic pieces of work through focused ‘cells’ that improve understanding of threats, risks, typologies and methodologies, and by developing ways to better detect and disrupt the criminal and terrorist exploitation of the financial system. Public-private threat groups also exist for illicit finance, tax evasion and fraud. Oversight is provided by a multi-sector attended and co-chaired Public Private Operational Board.

2.8 The below diagram sets out the overall structure of the UK’s AML system. Further detail on the individual elements and their responsibilities and a complete list of regulators and supervisors can be found in annex D.

### Box 2.A – UK AML/CFT System Box



2.9 The previous National Risk Assessment in 2020 found the following areas carried the biggest ML/TF risks:

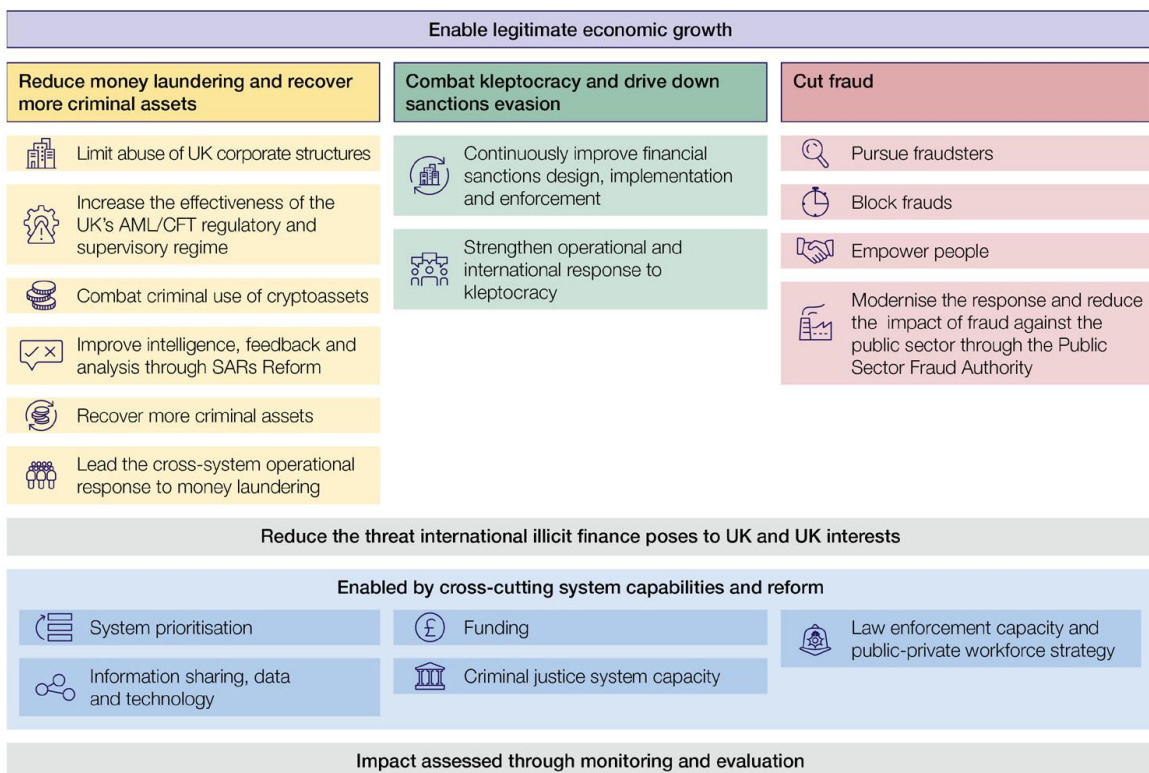
- **Banking and Financial Services:** Identified as a highrisk sector due to its centrality in financial transactions and the potential for money laundering and terrorist financing activities.
- **Real Estate:** Recognised as vulnerable to investments of illicit finance and money laundering, particularly through the use of complex ownership structures and overseas entities.

- **Legal and Accountancy Services:** Highlighted as susceptible to misuse by criminals seeking to facilitate money laundering and other financial crimes, given their role in providing advice and creating legal structures.
- **Trust and Company Service Providers/company structures:** Identified as a risk due to the potential to obscure ownership and control of assets, facilitating money laundering and other illicit activities through complex legal structures and cross-border operations.
- **Cryptoassets:** Identified as a growing risk area due to the anonymity, speed, and continued increasing adoption by consumers, global reach of transactions, making them attractive for money laundering and terrorist financing and other illicit activities.

### Economic Crime Plan 2023-26:

2.10 The UK government has taken significant steps to address the UK’s money laundering risks since 2020. The Economic Crime Plan 2023-26 (Economic Crime Plan 2) sets out the UK’s whole system approach to tackling economic crime. Supported by the introduction of c.£115 million per year additional funding via the economic crime levy, the plan builds on its predecessor, Economic Crime Plan 1, and sets out new actions to transform the UK’s response to ML and TF, targeting the high risk areas identified in the previous NRA and set out in more detail below.

### Box 2.B – Economic Crime Plan 2 Box



## **Limit abuse of UK corporate structures**

2.11 The Government has passed two key pieces of legislation to address gaps in our company law and economic crime frameworks:

### **2.11.1 The Economic Crime (Transparency and Enforcement) Act 2022**

- Allowed the Government to move faster and harder when imposing sanctions.
- Created a Register of Overseas Entities to help crack down on foreign criminals using UK property to launder money.
- Reformed and strengthened the UK's Unexplained Wealth Order regime to better support law enforcement investigations.

### **2.11.2 The Economic Crime and Corporate Transparency Act 2023**

- The phased introduction of identity verification, after which all new and existing registered company directors, people with significant control (PSCs), and those who file on behalf of companies, will need to verify their identity.
- From 4th March 2024, the broadening of powers to enable the querying of information, stronger checks on company names and new rules for registered office addresses.
- More reliable and accurate financial information on the register, which reflects the latest advancements in digital technology and enables better business decisions.
- Providing Companies House with more effective investigation and enforcement powers.
- Increasing the ability to share relevant information with partners, underpinned by a new intelligence hub, and the production of a [Strategic Intelligence Assessment](#) which provides an in-depth analysis of the key threats that Companies House is facing.
- Enhancing the protection of personal information to protect individuals from fraud and other harms, with individuals being able to suppress personal information from historical documents from spring/summer 2025.

## **Increase the effectiveness of our AML/CTF regulatory and supervisory regime**

2.12 The aim of reform in this area has been to ensure that the businesses most vulnerable to money laundering and terrorism financing have strong and proportionate controls preventing their abuse and are subject to effective supervision.

2.13 Following the 2022 [review](#) of the Money Laundering Regulations (MLRs) and package of regulatory changes, HM Treasury ran a further consultation between March and June 2024, seeking to further improve the effectiveness of the MLRs. This gathered valuable feedback on proposed reforms, including

making customer due diligence more risk-based, enhancing coordination and information sharing, clarifying regulatory ambiguities, and reforming the Trust Registration Service. Policy development is ongoing and next steps will be announced in due course.

2.14 The UK Government also committed in Economic Crime Plan 2 to continue strengthening the UK's AML/CTF supervision regime, and in 2023 consulted on four potential options for reform. The government remains committed to supervisory reform and will announce a plan as a priority. While reform is implemented, however, the quality and consistency of the current supervision system remains immensely important. OPBAS continues to drive improvements in supervisory effectiveness through its updated Sourcebook for Professional Body Anti-Money Laundering Supervisors, which was published in January 2023 and aims to deliver a stronger and more consistent standard of supervision of the accountancy and legal sectors.

2.15 The FCA's risk-based supervisory approach has undergone significant enhancements to become more proactive and data-led since 2020. Fighting crime is one of the [FCA's four strategic priorities](#) for 2025-2030 demonstrating the focus on this area.

2.16 The Economic Crime and Corporate Transparency Act 2023 created a new regulatory objective in the Legal Services Act 2007 focusing on promoting the prevention and detection of economic crime. The Act also removed the statutory cap on financial penalties for the Solicitors Regulation Authority (SRA) to ensure the SRA has the necessary enforcement powers and can levy financial penalties that act as a credible deterrent in relation to economic crime matters.

### **Combat criminal use of cryptoassets**

2.17 Several changes have been made to the MLRs to enhance oversight and control of cryptoasset firms since the 2020 NRA. In 2023 the scope of the wire transfer information-sharing regime was extended to cryptoassets (the 'travel rule') for both domestic and cross-border transfers. Further, since 2023, the promotion of certain cryptoassets to UK consumers is subject to the FCA's financial promotion rules. In the first year, the FCA issued 1,702 consumer alerts about illegal promotions, over 900 scam websites were taken down and 56 apps removed from UK app stores.

2.18 The Economic Crime and Corporate Transparency Act introduced additional powers for law enforcement, so they are able to more quickly and easily seize and recover cryptoassets which are the proceeds of crime or associated with illicit activity such as money laundering, terrorist financing, fraud and ransomware attacks.

2.19 Law enforcement has invested in improving both their capacity and capability to investigate the criminal use of cryptoassets. This includes the

rolling out of new training and upskilling to improve law enforcement officers' understanding of cryptoassets, supported by the provision of specialist tooling (i.e. blockchain analytics tools) and the building of a new crypto-specific public-private partnership within the existing Joint Money Laundering Intelligence Taskforce (JMLIT), which brings together law enforcement and members of the regulated sector structure. This public-private partnership has helped develop our understanding of the threat and fomented various joint initiatives (including around data sharing).

### **Improve intelligence, analysis and feedback through SARs Reform**

2.20 Suspicious Activity Reports (SARs) intelligence is a critical tool in our ability to identify and disrupt criminal activity and recover criminal assets. The SARs Reform Programme is delivering a new SARs Digital Service (SDS) and has provided an uplift of staff to Regional Organised Crime Units (ROCU) and the UK Financial Intelligence Unit (UKFIU). The delivery of the new SDS will enable the enhancement of data exploitation, improve feedback and engagement to the regulated sector, enable timelier intelligence sharing with law enforcement agencies, improve capacity and capability across HMG and provide more efficient and effective reporting by the regulated sector.

### **Recover more criminal assets**

2.21 In addition to the new cryptoassets measures, reforms have been made to the unexplained wealth order (UWO) regime. These amendments extended the class of persons who may be subject to an UWO, amended the income requirement provisions, increased the maximum statutory time period afforded to law enforcement to review material, and reformed the cost rules.

2.22 Further, the Anti-Money Laundering and Asset Recovery (AMLAR) Programme (2023-2026) has been established, funded by the economic crime levy, increasing law enforcement capacity and capabilities.

2.23 Since 2020, there has been a sustained level of [assets recovered](#) with £358.4 million recovered in 2021/22, £341.5 million recovered in 2022/23 and £243.3 million recovered in 2023/24.

### **Lead the cross-system operational response to money laundering and terrorist financing**

2.24 The NECC continues to be the operational cross-system leaders. For example, in 2024 the NECC, NCA and OPBAS published the [Cross System Professional Enablers Strategy](#). The aim of the strategy is to galvanise a whole system response to deliver a step-change in reducing the threat posed by professional enablers.

## **Funding and law enforcement capability**

2.25 The Economic Crime (Anti-Money Laundering) Levy was introduced through the Finance Act 2022. Following changes to levy rates in the Spring Budget 2024, it is now expected to raise around £115 million per year from April 2024 onwards to spend on measures designed to tackle money laundering and economic crime. For the first three years of the levy this included:

- £100 million for state-of-the-art technology to analyse and share data on threats in real time, giving law enforcement the tools it needs to stay ahead of criminals.
- Funding to hire 475 new staff across threat leadership, intelligence and investigative and prosecution capacity dedicated to tackling money laundering and asset recovery.
- £60 million to fund new specialist intelligence teams in the NCA and expand the Combatting Kleptocracy Cell.
- Funding for c.89 officers to sustain the increased staffing of the UKFIU and for 22 new financial investigators to analyse SARs embedded in ROCUs.

## **Information sharing, data and technology**

2.26 The Economic Crime and Corporate Transparency Act 2023 included provisions to facilitate private-to-private information sharing to enhance the private sector's ability to detect and prevent economic crime. This allows entities to share relevant information about suspicious activity or potential threats. Similarly, the introduction of the NECC Fusion Cell pilot has enhanced the UK's fight against economic crime through advanced data analytics and collaboration. The pilot combines data at scale from multiple sources, enabling intelligence sharing across the private sector, as well as law enforcement and government. The Data (Uses and Access) Act 2025 also introduces a new lawful ground for processing personal data, giving businesses more confidence to use data for crime prevention.

## **Reduce the threat international illicit finance poses**

2.27 Tackling corruption and broader illicit finance are priorities for our foreign policy approach because of the harm these issues cause to all UK international objectives. The Illicit Finance campaign, launched in November 2024, is focused on demonstrating UK global leadership rooted in robust UK domestic reform to tackle the shared vulnerabilities that enable illicit finance and corruption, and the harms they produce. The government will also publish a new Anti-Corruption Strategy in 2025. It will include measures that address the UK's domestic vulnerabilities to corruption, make it harder for corrupt actors to operate in the UK and overseas, and strengthen global resilience to corruption.

2.28 The government has continued to deepen its partnerships with financial centres also exposed to money laundering and terrorist financing risks. HMG partnerships are focused on deepening policy and operational cooperation to tackle shared threats and to build stronger collective defences. We have provided technical and operational assistance, capacity building and programmatic activity across key jurisdictions, improving responses and international standards.

2.29 For example, the UK and United Arab Emirates (UAE) are working to deliver on the UK-UAE Partnership to Tackle Illicit Financial Flows. We have agreed to increase judicial co-operation and ensure the continuous alignment in our approach to illicit finance. This includes the work of the Combined Anti-Money Laundering Operational Team (CAMLLOT), a joint initiative designed to tackle money laundering operations and identify hidden financial networks tied to illicit activities.

2.30 In addition, we have continued to fund the UK's international law enforcement capabilities. The International Anti-Corruption Coordination Centre supports developing countries to investigate grand corruption cases and trace and recover stolen assets. Since 2017, it has identified [£1.45 billion in hidden assets](#), of which £631 million has been frozen by court orders, and as of November 2024 enabled the arrest of [49 politically exposed persons or corrupt actors](#). The FCDO also funds the NCA's International Corruption Unit, which investigates international bribery, corruption and related money-laundering offences connected to the UK.

2.31 The security of the UK is closely linked to the capacity of key international partners to contribute toward international efforts to counter terrorist financing. The UK works closely with international partners to promote international standards, deliver technical assistance, facilitate financial investigation training and to improve regulation. This includes a range of international partnerships, such as CT Strategic Alignments with the US and EU and engagement in multilateral fora and smaller groupings to influence global and regional partner activity and share best practice.

### **Counter-Terrorism Strategy - CONTEST:**

2.32 The UK Government's approach to tackling terrorist financing is established by [CONTEST](#), and aims to detect and understand, investigate and deter, and disrupt the flow of terrorist financing. The UK's counter terrorist financing system is wide reaching and works across the "4 Ps" set out in CONTEST (Prevent, Protect, Prepare and Pursue) to achieve these aims. The table in Annex B highlights the array of organisations in the counter terrorist finance system, who all work collaboratively to mitigate the risk of terrorist financing in the UK. Since 2020, we have continued to improve our knowledge and mitigations for terrorist financing, including looking at the links between

terrorist finance and other forms of illicit finance, including serious organised crime and fraud.

**Tri Sector Group and working with charitable and financial sectors:**

2.33 HM Government continues to work closely with the charitable and financial sectors through the Tri Sector Group (TSG). This was a recommendation by the former Independent Reviewer of Terrorism Legislation (IRTL), Lord David Anderson KC. Established in 2017, it enables dialogue that supports humanitarian priorities while ensuring compliance with counter-terrorism and sanctions legislation. The TSG is regularly reported in the current IRTL and Independent Reviewer of State Threats Legislation, Jonathan Hall KC's annual reports, where it has been flagged as having a valuable presence that has some impact internationally. Since 2020, the TSG has supported the delivery of several publications, including engaging with the Crown Prosecution Service to deliver their "[\*Humanitarian, Development and Peacebuilding Work Overseas\*](#)", and through working collaboratively to publish the joint Home Office and HMT OFSI "[\*Operating within Counter-Terrorism Legislation\*](#)".

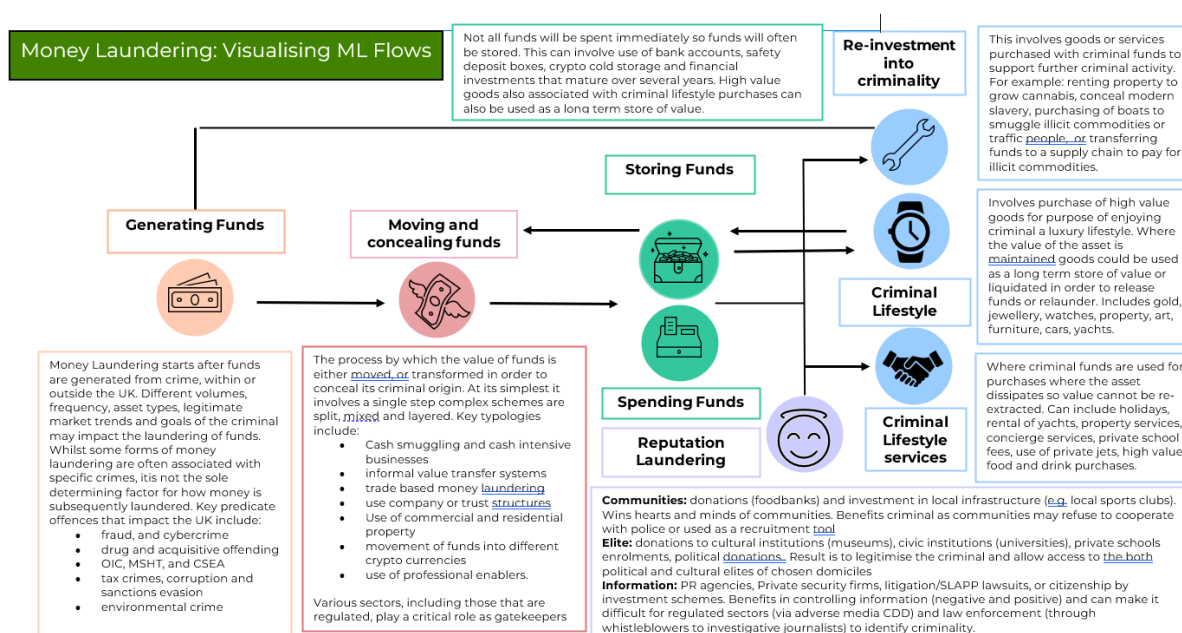
# Section 3 – Money Laundering

## Money laundering

### UK wide Money Laundering risks

#### Box 3.A – UK Money Laundering Flows

[larger version in [Annex C](#)]



3.1 The UK continues to be exposed to a high level of money laundering risk. The UK has one of the largest and most open economies, ranking 6<sup>th</sup> by GDP globally and 2<sup>nd</sup> in Europe. The UK's status as a global financial and professional services centre (financial and insurance activities account for more 9% of total GVA; while the UK's legal services market is the largest in Europe), openness to international trade and investment, and ease of doing business are all powerful drivers of economic growth. However, these same strengths also create vulnerabilities which can be exploited by bad actors to commit money laundering and other economic crimes. In the Home Office's Economic Crime Survey 2024 (forthcoming), one in 43 businesses with employees (2%) had experienced known or suspected money laundering

incidents in the 12 months prior to the survey, equating to around 33,500 businesses.

3.2 The context which the UK and the world faces has changed significantly since 2020, with increasing global instability in part driven by Russia's unprovoked invasion of Ukraine. As a globally connected economy, the UK is particularly impacted by the changing geopolitical landscape.

3.3 In the wake of Russia's invasion of Ukraine, we are seeing increased convergence between money laundering with [kleptocracy](#) and [sanctions evasion](#). Sanctioned entities and individuals aim to conceal the links to their funds by leveraging existing money laundering networks, and using the same [international controller networks](#), [complicit professionals](#) and [complex structures](#) that were previously principally used by those seeking to launder high volumes of criminal funds.

3.4 The increasing adoption of new financial technologies has also played a key role in changing the UK's risk profile since 2020. The UK faces risks from:

- [Electronic Money Institutions and Payment Service Providers](#). The UK is a world-leading fintech hub, with fintech firms such as electronic money institutions and payment service providers now widely embedded in the UK's financial system. While the majority of their transactions will be legitimate, this wide adoption increases criminals' ability to hide in plain sight, which has driven increasing risk.
- [Cryptoassets](#) have grown in popularity; in 2024, [FCA commissioned an online YouGov survey](#) with a nationally representative sample of 2,199 UK adults (including a boost of cryptoasset users), finding 12% of UK adults owned cryptoassets. They have also increasingly appeared in money laundering intelligence since 2020, with a large proportion facilitated by cryptoasset service providers based outside the UK. This may in part be driven by the continued rise in fraud since 2020, and ransomware attacks where payment is extorted in cryptocurrencies.
- [AI](#) has also advanced significantly since 2020. AI can be leveraged to improve the detection and prevention of money laundering. However, it could also be used by criminals to bypass AML controls, or to enhance criminals' capabilities. In particular, AI could enable criminals to commit predicate offences such as fraud with greater ease, and to transfer illicit funds more rapidly and across broader networks.

3.5 Despite these changes, there remain several continuing risks facing the UK:

- [Cash-based money laundering](#) in the UK remains high. Despite a decrease in the use of cash for regulated activity, traditional mechanisms such as cash smuggling, the use of cash-intensive businesses, money mules, and the exploitation of legitimate channels (including Post Offices) for inserting criminal proceeds into the [banking system](#) remain at high levels. There is no indication that criminals are moving away from cash, with criminals

often combining cash-based money laundering with other money laundering techniques.

- [Financial](#) and [professional service](#) firms continue to be vulnerable to organised criminals seeking to integrate illicit funds into the legitimate financial services sector and leverage the legitimacy of the professional services sector to facilitate integration.
- The risk of money laundering through UK [companies](#) remains high. As noted by the [NCA](#) This can occur through UK-based regional OCGs using front companies and cash intensive businesses, as well as through high-end cross-border criminals using UK companies in complex structures to launder tens of millions of GBP.

3.6 All regions of the UK continue to be vulnerable to money laundering. Urban areas with higher levels of overall organised crime activity are likely to have elevated levels of money laundering. Larger cities [and London in particular] often prove attractive to criminals seeking cross-border and complex money laundering services, due to their concentration of large [financial](#) and [professional service](#) firms. Meanwhile, more rural areas of the UK can be vulnerable to local and regional UK organised crime gangs, who primarily use cash and may exploit smaller locally based professional services firms to launder criminal funds.

## Money Laundering threat

3.7 This section sets out common predicate offences that generate criminal funds and highlights harms and trends since 2020. Unless otherwise stated, crime figures are for England and Wales only.

### Fraud

3.8 Fraud is the most commonly experienced crime in the UK, accounting for over 43% of crime in England and Wales, with an estimated 4.1 million fraud incidents in the year ending December 2024, a 33% increase compared with December 2023. Fraud is not limited to any particular part of the economy. High harm fraud types include investment, romance, courier and payment diversion fraud. In the year ending March 2025, 63% of the frauds reported to Action Fraud were cyber-enabled, and it is assessed that over 70% of the fraud perpetrated against UK citizens or businesses emanates from, or is facilitated via, overseas jurisdictions (professional estimation of international fraud offending by NFIB February 2022). Organised Criminal Groups with links to Ghana, Nigeria, India and South East Asia have been identified as being those posing the most significant level of threat, particularly in relation to high-harm frauds, including investment, romance, and payment diversion fraud.

3.9 The proceeds from fraud are criminal funds as soon as the victim has been deceived into sending funds. This means that when using those criminal funds, the offender is then laundering them. The diverse forms and scales of fraud the UK is exposed to means there is no single form of money laundering specifically used by fraudsters. However, retail banking accounts are regularly used to pay out funds to fraudsters. Money muling, which involves employing others to move the proceeds of crime on their behalf, is also frequently used.

## Sanctions Evasion

3.10 The sanctions picture has changed substantially since 2020. The UK implements a range of sanctions regimes under the Sanctions and Anti-Money Laundering Act, including the anti-corruption, global human rights and country specific sanctions. The number of UK sanctioned individuals and entities has increased significantly following the UK's robust response to Russia's invasion of Ukraine. As of April 2025, UK financial sanctions covered over 3600 individuals and 990 entities across 35 sanctions regimes, a large proportion relating specifically to the Russia regime.

3.11 Assets frozen under UK sanctions that are used, transferred or moved without a licence become proceeds of crime and their use can constitute money laundering. Suspected breach cases in relation to UK sanctions recorded by Office for Financial Sanctions Implementation increased from 147 in 2021/22 to 396 in 2023/24. The majority of suspected breach cases recorded by OFSI in 2023/24 related to the financial services sectors, followed by the legal sector. The use of [professional enablers](#), both in and outside the UK regulated sector, and role of [complex ownership structures](#) are commonly associated with sanctions evasion and subsequent money laundering.

## Acquisitive Crime

3.12 [Organised] acquisitive crime includes burglary, vehicle crime, robbery, business crime, heritage and cultural property crime, plant and agricultural thefts, and metal and infrastructure crime, amongst other crime types, including theft and shoplifting. Organised Acquisitive Crime also continues to increase; cost of living pressures have almost certainly led to an increase in offences targeting businesses.

3.13 Stolen goods can either be sold on to generate cash which must then be laundered, often using traditional [cash based money laundering](#) schemes, or used as a store of value.

## Drugs

3.14 A range of illegal drugs are used in the UK including cannabis, cocaine, heroin, synthetic opioids, amphetamines, methamphetamines and ketamine. In the year ending March 2024, an estimated 8.8% of people aged 16 to 59

years, in England and Wales, reported using any drug in the last 12 months, a decrease from 9.4% in year ending March 2020. Drugs are predominantly imported from abroad and trafficked through the UK border, although some are produced domestically in the UK. A range of UK based and international organised crime groups are involved in their production, movement and sale. The cost of harms related to illicit drug use in England is estimated to be £20 billion per year.

3.15 The main motivator for those involved in the illegal drugs trade is financial gain. Whilst there has been some growth in online payments and communications, [cash](#) remains the principal means by which drugs are bought and sold for consumption.

## Cyber Crime

3.16 Cyber crime involves gaining unauthorised access, or causing damage, to computers, networks, data or other digital devices, or the information held on those devices. Cyber crime also facilitates other offences, such as fraud. Estimates from the Crime Survey for England and Wales (CSEW) show there were 757,000 incidents of computer misuse experienced by individuals in the year ending December 2024, a significant decrease of 23% compared to the prior year. The [2025 Cyber Security Breaches Survey](#) estimated that 20% of businesses and 14% of charities were victims of at least one cyber crime in the past year, which was consistent with 2024. However, the prevalence of ransomware crime among businesses significantly increased between 2024 and 2025, from less than 0.5% to 1% of businesses experiencing this type of crime.

3.17 Despite cyber-crimes against individuals decreasing, the UK cybercrime threat remains high. Low-sophistication, high-volume cybercrime such as phishing and social media hacking are most common, but ransomware incidents are the most harmful. Cybercrime is underreported. Only 7% of computer misuse incidents against individuals estimated by the CSEW were reported to authorities in the year ending March 2024. This means the number of cyber crimes reported to Action Fraud will be much lower than the true scale of cyber crime. There were 52,030 cases of computer misuse reported by individuals and businesses to Action Fraud in England and Wales in the year ending December 2024, the number of reports has generally been increasing since year ending December 2015 (14,347 reports).

3.18 Cryptocurrency theft, where cryptocurrency assets are stolen directly from victim's virtual infrastructure or exchanges has also emerged as cryptoasset adoption has grown. The scale in the UK is not fully understood.

3.19 Cyber crime type is not tied to any particular sector or form of money laundering. However, since the last NRA cryptoassets have been the prevalent

form of payment requested by criminals when seeking to profit from cybercrimes, although payment by other means remains a possibility.

## Organised Immigration Crime

3.20 Organised crime groups use multiple methods to facilitate irregular migrants' entry into the UK through abuse of immigration rules, supply of false documents, air travel and other methods such as the use of small boats to cross the Channel. Some of these methods are low cost and readily available. Since 2020, attempts to enter the UK on small boats have accounted for most of the detected illegal migrants arriving in the UK. Criminals will also seek to abuse the immigration system by supporting illegal migrants in the UK for a fee, for example by providing false documentation, statements or other evidence or through use of corrupt enablers within the immigration system including immigration advisors.

3.21 The high fees charged and low costs to OCGs generate significant profits which are used to fund further criminal activity or to support a criminal lifestyle (whether in the UK or by transferring to a criminal's non-UK home country or a third jurisdiction), both of which require the money to be laundered. [IVTS](#), [MSBs](#), mobile money service operators and [traditional bank transfers](#) are known methods of payment for OIC. There are also strong links between OIC and MSHT.

## Tax Evasion

3.22 Tax evasion is any deliberate omission, concealment or misinterpretation of information, or the false or deceptive presentation of information or circumstances to gain a tax advantage. The tax gap (the difference between the tax due and the tax collected by HMRC) for the year 2023/24 is estimated to be £46.8 billion (5.3% of the theoretical tax that should be paid to HMRC), of which £6.4 billion is linked to evasion and £4.4 billion to criminal attacks. The tax gap also covers avoidance and error, which is not relevant to this assessment.

3.23 Where money due to the government as taxes or duties is deliberately not paid it becomes the proceeds of crime and its subsequent use and transfer can constitute a money laundering offence. [Accountancy firms](#), [lawyers](#) and [trust or company service providers](#) are particularly exposed to the risk of being used for the purposes of tax evasion. Criminals may also use [IVTS](#) to launder funds from tax evasion.

## Modern Slavery and Human Trafficking (MSHT)

3.24 Modern slavery encompasses slavery, servitude, forced and compulsory labour and human trafficking where traffickers and exploiters coerce, deceive

and force individuals to carry out acts against their will. It is often interwoven with other forms of criminality, for example, the criminal exploitation of people in drug cultivation or distribution or through regular and irregular migration on the false premise of legitimate work but actually for the purpose of sexual or labour exploitation. There is also a strong link between Organised Immigration Crime and MSHT, due to the vulnerable immigration status of those who arrive in the UK illegally, meaning that OCGs can exploit those people and profit from their misery.

3.25 Modern slavery offences recorded by the police have fluctuated slightly between 2020 and 2024. In 2024, there were 9,036 recorded offences. In 2024, 19,125 potential victims of modern slavery were referred to the Home Office national referral mechanism, representing an 80% increase compared to 2020 (10,613) likely driven by increased awareness. Victims of MSHT can also be used for money laundering purposes as runners and [money mules](#). There is reporting of MSHT OCGs laundering profits via the use of money mules and through front companies such as hairdressers or grocery retailers.

## Online Child Sexual Exploitation and Abuse

3.26 Online child sexual exploitation and abuse is the use of the internet to conduct and share child sexual abuse material, livestream the sexual abuse of children, and groom or extort children online. These activities, mainly where financially motivated, can generate criminal proceeds.

3.27 The proceeds from online child sexual exploitation and abuse are criminal funds as soon as funds are sent in return for access to child sexual abuse material or livestreams, or in the case of child sexual extortion as soon as the victim has been manipulated into sending funds. Victims of extortion can also be used for money laundering purposes as money mules. [Electronic Money Institutions and Payment Service Providers](#) are regularly used to make payments associated with online child sexual exploitation and abuse, although [retail banking](#), [cryptoassets](#), and other payment methods are also used. There is no global estimate for the proceeds generated by online child sexual exploitation and abuse. Often individual transactions or payments are small in value; however, this is in stark contrast to the very high level of harm caused to victims.

## Environmental

3.28 In the UK, environmental crime generally refers to any illegal activity that harms the environment. This can include actions that breach environmental

legislation and cause significant harm or risk to the environment and human health. The UK is particularly exposed to waste crime with [16,773 reports](#) of suspected waste crime from January 2023 to December 2024 in England. It is estimated to cost the UK up to £1 billion per annum. OCGs in the [waste sector](#) often directly take waste below cost and dump it on farmers' land or industrial plots or use [front companies](#) to bid for contracts then misclass waste (e.g. hazardous waste labelled as non-hazardous) to dispose of it illegally, but generate seemingly legitimate profits. Environmental crime in the UK can also be linked to labour exploitation, a form of [modern slavery and human trafficking](#). The [accountancy sector](#) and [TCSPs](#), may be used to provide false legitimacy to front company accounts in order to launder waste crime profits.

3.29 The UK can be a source, transit and destination country for [illegal wildlife crime](#). The highly organised criminal trade can be very lucrative with criminals acquiring and selling illegal goods with various money laundering methods then being used to obfuscate the criminal origins.

## **Bribery and Corruption**

3.30 The UK government defines corruption as 'the abuse of entrusted power for private benefit that usually breaches laws, regulations, standards of integrity and/or standards of professional behaviour'. Whilst there is no single corruption offence in the UK, the UK [Bribery Act](#) defines bribery offences and the [misconduct in public office](#) offence can also apply.

3.31 The scale of domestic bribery and corruption is unknown. Local police forces in England and Wales recorded 203 corruption related offences in the year ending December 2024, comprising 184 Misconduct in Public Office and 19 Bribery offences. However, the true incidence of corruption is likely to be substantially higher. Many corruption incidents, when criminal in nature, may be subsumed amongst other offences such as fraud, or may be difficult to detect or evidence due to their clandestine nature. The Home Office's 2024 Economic Crime Survey (forthcoming) estimated that 117,000 bribes were offered to UK businesses with employees in the previous 12 months by other UK businesses or individuals. The UK is also exposed to international corruption, principally serving as a nexus for international funds, including from corrupt politically exposed persons who seek to invest wealth they have misappropriated from their countries in the UK.

3.32 Bribery and corruption are also cross-cutting enablers of criminality. Corruption and the use of 'insiders' in both the public and private sectors enable OCGs to carry out their criminal activity. Corrupt insiders are used to facilitate the movement of illicit commodities, divulge sensitive information, and circumvent security measures. In the private sector, there is a risk that [professional enablers](#) with a responsibility for anti-money laundering controls

may be corrupt or may be corrupted by criminals in order to evade those controls.

3.33 While both public and private sector corruption can help facilitate money laundering the bribes received also constitute criminal proceeds. The main method used to launder the proceeds of corruption continues to be the layering and placement of assets through [offshore corporate entities and trusts](#) and often into [property](#).

#### **Box 3.B – Politically Exposed Persons (PEPs)**

Politically exposed persons are individuals who have been entrusted with a prominent public function. These individuals, and their close relatives and business associates, face a heightened risk of being targeted by those seeking to exploit their positions, for the purposes of laundering illicit funds, or committing predicate offences such as bribery or other corruption related offending. The term can apply to both UK and foreign nationals, though under UK law the starting point for regulated firms should be to treat domestic (UK) PEPs, their family members and close associates as inherently lower risk than non-domestic PEPs, and therefore apply a lower level of enhanced due diligence to domestic PEPs unless other risk factors are present.

# Money Laundering typologies

3.34 Money laundering networks use a combination of methods to move criminal proceeds and conceal the source of funds, ranging from simple one-off cash transactions to complex international transaction chains involving multiple parties. Money laundering can happen in a variety of contexts: it may involve moving criminal proceeds within the UK, seeking to remove funds from the UK to a foreign jurisdiction or bringing funds into the UK.

3.35 This section outlines the most common techniques identified in the UK. It is not exhaustive and criminals will always seek to innovate to avoid detection. The individual sections below outline:

- how each type of money laundering typically works
- how it manifests in the UK, including cross border links, and
- what has changed since 2020.

3.36 Where possible each typology is linked to predicate offences and regulated sectors particularly associated with the typology. The sectors noted should pay particular attention to the typologies in which their sector is named. Different typologies may still be used to launder the proceeds of different crime types or via different regulated firms not directly referenced. Unless otherwise stated crime figures are for England and Wales only.

## **Box 3.C - System Prioritisation**

We expect the use of these typologies will continue throughout the lifetime of this NRA, but the ways they are used will likely change over time. To account for this and the changing opportunities that will be available to respond to these threats through public-private collaboration, these typologies should be read in conjunction with the priorities published by the NECC & FCA under System Prioritisation. These priorities are intended to provide context to the risks in the NRA and typologies listed below and will provide more detail on the priority areas some sectors should note for certain typologies. The priorities are expected to be reviewed annually as well as on publication of a new NRA. When the priorities are published guidance will be provided on how to relate these to each NRA typology.

## Cash



3.37 It is highly likely that criminal cash generated in the UK from illicit activity is in excess of [£12 billion per year](#). Whilst the use of cash for legitimate transactions continues to decline, the number and value of bank notes in circulation [continues to increase](#) and cash remains widely used by criminals. Cash is commonly used to launder the profits of [drug](#) offences and to facilitate [tax evasion](#), for example, via undeclared cash in hand wage payments. Criminals favour cash for its anonymity and ease of use, helping them hide the link between crimes and profits while enabling both illegal and legal activities.

3.38 Cash is often pooled into larger sums before being integrated into the financial system. This can be done in several ways, including via deposits into [retail banks](#), [money service businesses](#), the Post Office, use in [gambling](#) and the purchase of [high value goods](#). Once integrated the value can be either used in the UK or transferred abroad. Criminals will also seek to physically move cash out of the UK where it can be integrated into foreign financial systems, with an estimated £2 billion in criminal cash moved out of the UK each year. Criminals will also use cash to purchase goods and services. Cash continues to dominate illicit drug transactions, though other criminal activity also generates cash proceeds.

3.39 Cash is often laundered through cash intensive businesses. Once criminal cash has been received it can be used to pay expenses, placed into a bank account as false or inflated takings, or transferred via a Money Service Business. The criminal cash can then be easily moved around the financial system with the appearance of legitimacy. Given the nature of these businesses large deposits of cash are considered less suspicious making it easier to circumvent AML controls and procedures. Cash intensive businesses can be set up or taken over specifically with the intention of using them to launder criminal proceeds under the cover of legitimate activity. This means that where cash intensive businesses are used, they are likely to be complicit

in this activity (although some employees may also be ignorant of the criminal activity).

3.40 Prominent examples include barber shops, car washes and nail salons. The number of barber shops has grown substantially since the last NRA and there has been a year on year increase in the number of SARs being received relating to their activities.

#### **Box 3.D - Case study: Operation Machinize**

In spring 2025 barbershops and other cash-intensive businesses across England were targeted by police and other law enforcement officers responding to the cash based money laundering threat. In total, 380 premises were visited across Operation Machinize, with officers securing account freezing orders over bank accounts totalling more than £1 million and 35 arrests made. In addition, officers seized more than £40,000 in cash, some 200,000 cigarettes, 7,000 packs of tobacco, over 8,000 illegal vapes and two vehicles. The crackdown involved 19 different police forces and Regional Organised Crime Units, as well as national agencies including HMRC, Trading Standards and Home Office Immigration Enforcement.

3.41 The Post Office network plays an important role in allowing the millions of people who depend on cash to continue withdrawing and depositing it, especially due to the closure and reduction of bank branches in both urban and rural areas. However, this service can also be exploited by criminals, and in recent years there has been an increasing use by OCGs of the Post Office's everyday banking facility to deposit large values of criminal cash across the UK. Cash deposits at the Post Office continue to rise, despite a general societal move to use cash less, with between £2-3 billion deposited every month - a 10% year on year increase. Whilst the exact amount of criminal cash within this total is unknown, estimates indicate it could be in the hundreds of millions of pounds. The NECC continue to work with law enforcement partners, and the FCA, to call for the Post Office and banks that make up the Everyday Banking Framework to reduce the ease in which criminal cash can be deposited through the introduction of enhanced know your customer and due diligence provisions at the Post Office, and greater awareness and training of frontline staff, thereby reducing this vulnerability whilst continuing to provide a vehicle for legitimate money to be deposited.

3.42 Criminals may be attracted by the perception that less stringent checks are applied by post office staff. This abuse of the service may also be enabled by negligence, but a small number of instances of suspected complicity from Post Office staff have also been identified. Suspicious deposits and activity are concentrated in urban areas; hotspots include London, the West Midlands, and Glasgow. Once deposited at the Post Office criminal funds are then paid into to multiple bank accounts or alternative payment platforms, in small

deposits to avoid suspicion in the receiving institution. Funds are then available for further layering or use by the account's owner.

### **Box 3.E - Case study: Post Office Money laundering conviction**

In 2024 two individuals were convicted of a £27 million cross-border money laundering scheme using Post Office cash deposits with a business used as a seemingly legitimate front to create false invoices.

- 3.43 Retail sector businesses such as convenience stores, petrol stations and wholesalers have been identified as being linked to this activity.
- 3.44 Criminal money generated in the UK is regularly moved cross-border via passenger and freight routes by land, air and sea including via cash and valuables in transit companies. Cash is concealed in a variety of ways including in luggage and hollow spaces in vehicles. Once outside the UK it can be mixed with other legitimate or criminal funds before integrating into local financial system. Once in a financial system it becomes relatively easy to transfer funds internationally at speed.
- 3.45 Cash is moved out of the UK through transit countries, with immediate neighbours such as France, Belgium and the Netherlands being common points of entry before cash moves to its final destination. Romania and Türkiye are noted as common transit hubs with Türkiye serving as a common final destination. Significant volumes of criminal cash are seized from flights and road vehicles en route to Türkiye at the UK border and in transit countries (e.g. by Bulgarian law enforcement working in partnership with the UK). Suspected criminal cash is regularly moved to the Middle East and Far East via air freight, often by UK based money service businesses to MSBs in the receiving jurisdiction. The UK itself serves as a transit country for criminal cash. The UK's shared land border means the proceeds of crime from the Republic of Ireland often pass through the UK en route to mainland Europe and onwards.
- 3.46 Large volumes of cash generated in the UK are integrated in the Western Balkans, notably Albania. Cash is often transported to the region by road or air and then typically integrated through Money Service Businesses or through the purchase of valuable goods and property. These funds are often generated by Western Balkans OCGs operating in the UK drugs market. Once criminal cash is successfully introduced into the financial system the value may then return to the UK via a range of financial mechanisms. The significant increase in the repatriation of sterling from Albania in recent years reflects Albania's position as a common destination for criminal funds generated in the UK. HMG has prioritised engagement with the Albanian government and authorities to help address these issues.

3.47 Cash integrated in the UK is often laundered by international controller networks. Global financial centres with open economies and large licit gold markets may be exploited by criminals who seek to launder both cash and gold. These can include transit points, such as Dubai and China, including the special administrative region Hong Kong, where it can be further layered before transfer onwards or as an end destination. Cash is also crucial in informal value transfer systems, which see value transferred often without the physical movement of cash across borders. This will be discussed more fully in the [next section](#).

### **Box 3.F - International controller networks**

International controller networks (ICNs) provide professional money laundering services to criminals by collecting funds in one jurisdiction and making equivalent value available in another. This can be done by using pools of funds which are kept in balance by settling transactions on behalf of criminals in multiple locations at the same time. They are typically used where there is a complex network of payments, transactions and accounts and a need to have access to funds or make payments in multiple jurisdictions.

3.48 Incoming cash seizures are much less frequent than outgoing cash seizures which likely reflects the smaller scale of criminal cash coming into the UK vs leaving. Incoming cash may be intended to fund criminality here or integrated for use in the UK economy; including the purchase of goods and services that might be of particular appeal to [politically exposed persons](#).

3.49 Cash alternatives also remain attractive to criminal groups and include gold, precious metals and stones, watches and other portable items. They can be used as an alternative store of value and are particularly appealing when their price is high. These goods can also be used in trade based money laundering, which is often characterised by heightened levels of complexity as opposed to the relative simplicity of transporting cash across borders.

3.50 Since 2020 there has been a rise of gold seized at the border, with some intelligence suggesting Outward Processing Relief is being abused to provide false legitimacy for the export of gold money out of the UK. Outward Processing Relief allows for a reduction in customs duty and import VAT on goods that are exported from the UK for process or repair and are re-imported at a later date.

### **Box 3.G - Case study: safe custody services**

There have been a number of examples of criminal actors using safety deposit boxes as a means of storing criminal property including cash, firearms and drugs.

A safe custody service provides secure storage such as safety deposit boxes for high-value physical items like jewellery, precious metals or documents of title. There remains a legitimate demand for safety deposit box services to safeguard valuables from events such as house burglaries, fire, flood etc.

Most businesses offering this service are Annex 1 financial institutions who are registered with the FCA and supervised for adherence to the MLRs.

## Informal Value Transfer Systems



3.51 'Informal value transfer systems' (IVTS) is a general term that refers to a wide range of networks used to transfer value from one location to a third party in another. As such, IVTS is a form of money remittance and all UK-based IVTS providers are required to register with HMRC as a money service business and to adhere to the requirements of the Money Laundering Regulations. IVTS have a long history and have emerged in many different parts of the world, generally serving as an alternative for communities where traditional banking systems do not exist or are difficult to access. IVTS are often linked to and used by particular ethnic, national or geographic communities and their diaspora members, who utilise IVTS to send remittances to their home country. Use of IVTS for legitimate purposes is legal in the UK, provided money transmitting money service businesses are registered with HMRC as required under the MLRs, and with the FCA under the Payment Services Regulations. In some countries, such as China, where UK linked IVTS operate, their use is illegal.

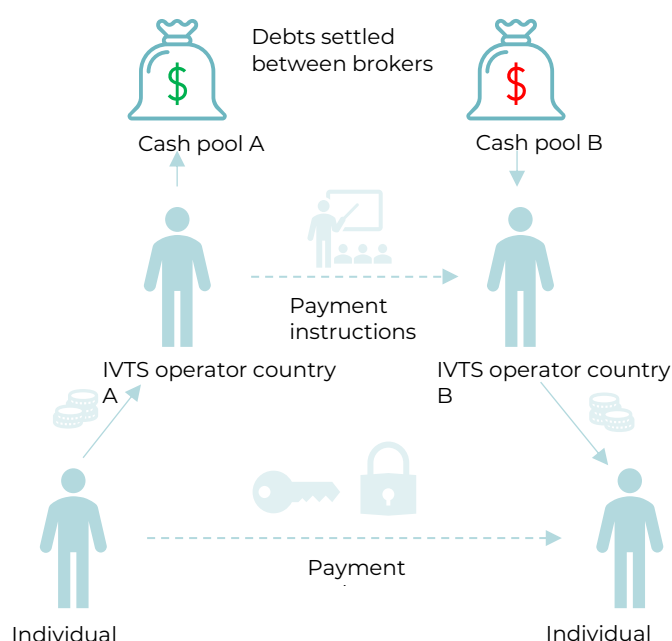
### Box 3.H - Notable forms of IVTS

| IVTS network                   | Historically linked regions/countries |
|--------------------------------|---------------------------------------|
| Chinese underground banking    | China                                 |
| Hawala                         | Middle East, Afghanistan, Pakistan    |
| Hundi                          | India, Burma, Myanmar                 |
| Padala                         | Philippines                           |
| Vietnamese underground banking | Vietnam                               |
| Phoa Kuan                      | Thailand                              |

3.52 IVTS rely on a network of operators and intermediaries who act as facilitators in the transfer process. To make an IVTS payment an individual will

approach an operator, often a trusted member of their community, to give them cash or goods and a payment instruction. That operator will contact an operator in a second location who will issue the payment to the recipient, with one or both charging commission (see Box 3.1). This does not require the immediate physical movement of cash or assets, instead the IVTS operator in the destination country will release funds from their own cash pool to the customer. As such, only value has transferred. At a later stage, the IVTS operators will reconcile imbalances on their ledgers, and this may be done through a variety of means. This could include making use of non-bank payments and movement/sale of goods.

### Box 3.1 – IVTS flows



### Criminal use

3.53 IVTS are used by criminals for money laundering and terrorist financing because of the perception by criminals that less stringent checks are applied by the IVTS providers. Alternatively, criminals can establish their own IVTS networks, ensuring total control of the overall process. IVTS traditionally relies on trusted networks which make IVTS appear less vulnerable to detection by law enforcement than other means of laundering.

3.54 Where identified in UK money laundering investigations, IVTS are principally linked to international laundering networks given their access to stores of value in numerous locations which is useful to criminals. UK criminal funds laundered through IVTS are often **drug** based. IVTS is also a more trusted way for illegal migrants to pay smugglers for the journey than handing

over [cash](#), although the scale of this is unclear and transactions relatively small. IVTS are often part of International Controller Networks given their access to stores of value in numerous different locations which is useful to criminals. The following IVTS processes are considered to be the most prominent in the UK, but given the diversity of communities in the country, it is likely some or all of the other networks listed above are used.

### Hawala

3.55 Hawala is a form of IVTS that is popular with many communities in Africa and the Middle East and is commonly used to pay remittances by diaspora members in the UK. Criminal use of hawala networks – either through abuse of existing networks or setting up of criminal networks – is linked to a range of jurisdictions, particularly international controllers operating in the Middle East. Western Balkan based OCGs have also been identified as using hawala networks to move criminal proceeds to their own region, the UAE and other jurisdictions.

### Chinese Underground Banking and Daigou

3.56 Chinese underground banking is a form of IVTS commonly used by the UK's Chinese community. Chinese underground banking is driven by Chinese foreign exchange restrictions which limit the money that Chinese residents can send abroad to \$50,000 a year. Chinese individuals use Chinese underground banking to send money abroad for a variety of purposes, such as paying tuition fees or purchasing properties. Chinese underground banking is legal in the UK but if the Chinese underground banking entity is not registered under the MLRs, then it is operating illegally.

3.57 There is a need for significant funds to be accessible to the Chinese underground banking networks in the UK due to the extent of its use by Chinese communities in the UK, notably amongst students and for the purchase of property. This can make the proceeds of OCGs an attractive source of physical cash for Chinese underground banking networks. In exchange for access to this criminally derived cash, these networks may make payments to international suppliers of the OCG or make funds available to members of the OCG in other countries where they can then be used. Due to the complexity of transactions, these networks often use professional money launderers and international controllers.

3.58 Criminal Chinese underground banking networks are noted for their use of Chinese students to operate as money mules and cash couriers, receiving money into their accounts before transferring it on to a third party. Criminal Chinese underground banking networks are known to seek to integrate cash into the financial system via [traditional financial institutions](#) and through deposits at the Post Office, as well as using [electronic money institutions](#), payment service providers and challenger banks to move their funds. These networks have also used [accountancy firms](#), [solicitors](#) and [letting agents](#). The

financial services sector and law enforcement bodies have noted that Chinese underground banking networks now place cash into the financial system in smaller amounts and through more accounts. This little and often approach is highly likely to make it more difficult for the financial sector to identify suspect accounts.

3.59 Another common element of criminal Chinese underground banking activity in the UK is the criminal exploitation of Daigou activity to generate and move value. Daigou is a Chinese term which translates to 'buying on behalf of'. It traditionally describes the practice of cross-border e-commerce activity involving surrogate shoppers purchasing luxury and other consumer goods overseas, to resell to East Asian consumers (usually exported to China, including the special administrative regions of Hong Kong and Macau, Vietnam, South Korea).

3.60 This activity is legal in the UK, however, criminal exploitation can take place by the integration of criminal proceeds into the purchasing process. Further abuse can include facilitation of tax evasion, for example when tax on profits is not appropriately declared, or VAT is fraudulently reclaimed when the goods are exported overseas.

## Cryptoassets



3.61 The risk of money laundering through cryptoassets has increased significantly since 2020 with cryptoassets increasingly appearing in money laundering intelligence over this period. Cryptoassets are increasingly used for laundering all forms of proceeds of crime. In addition, there have been increasing levels of cryptoassets obtained through illicit means such as [cybercrime](#), ransomware and cryptoasset thefts which are then laundered. Whilst Bitcoin remains an attractive cryptoasset for illicit finance and serious and organised crime (SOC), stablecoins such as Tether are now most commonly used to launder money. [This is due](#) to the assets' price stability, fast transaction speed and wide adoption. Decentralised finance (DeFi) continues to be a relatively small part of the cryptoassets ecosystem. DeFi is a blockchain-based system in which users can borrow, earn interest, lend and trade without the need of a third-party intermediary, such as a bank. Whilst criminal use of Ethereum based tokens is increasing due to their prominent role in decentralised finance, it still only represents a small volume of activity compared to the use of stablecoins or Bitcoin.

3.62 Cryptoassets are also increasingly being used by a wider range of OCGs to launder proceeds from crimes such as [drugs](#) offences. However, the top identified categories of illicit activity on the blockchain are still from [sanctioned](#) entities (33% of illicit volume), and scams and [fraud](#) (24% of illicit volume). Criminals appear to be shifting to using less regulated exchanges and services to launder criminal funds, potentially due to the increased regulation in the UK and other jurisdictions. This includes exchanges based in less compliant or regulated jurisdictions, decentralised-finance based exchanges, and those run solely for criminal purposes (such as exchanges operating through darknet marketplaces).

3.63 There is limited evidence that criminal use of cryptoassets has displaced other laundering methodologies. Criminals still need to disguise the origin and nature of illicit cryptoassets funds to extract them as seemingly 'clean' money or assets, as well as layering of funds. Cryptoassets have primarily

added an additional means by which criminals can do this. The international nature of the blockchain and cryptoasset transactions present unique difficulties in conducting effective enforcement against criminal actors. This can make cryptoassets more appealing to criminals as they perceive a lower likelihood of detection. Criminals and professional money launderers continue to increase the sophistication of their techniques, adapting quickly to law enforcement intervention. For example, there is [evidence](#) to suggest privacy wallets are now used more commonly than mixers to launder funds.

#### Peer-to-peer cryptoasset exchanges (P2P), Over the Counter (OTC) brokers and Decentralised Exchanges (DEX).

3.64 Over the counter trades can occur through peer to peer transactions, via a trading desk or on a decentralised exchange. It is often unclear if brokers are operating via a peer to peer network, trading desk or a decentralised exchange.

3.65 The NCA assess that it is likely hundreds of millions of pounds per year are being laundered through Over the Counter cryptoasset brokers in the UK. Over the counter brokers are used to convert cash into cryptoassets and vice versa. Trades take place between two parties, who agree a price and method of transferring the government issued fiat currency and cryptocurrencies. Over the Counter trading desks are specialised businesses dedicated to trading cryptoassets in large volumes. Most over the counter brokers are legitimate and will require clients to complete Know Your Customer checks. It is highly likely that those brokers operating outside of regulated exchanges present the highest risk of money laundering and may specialise in providing money laundering services to criminals. These services are used particularly for [cash-based](#) offences such as [drugs](#) or [excise](#) crime, given the large values that can be laundered via this method. Clients may leverage initial relationships established through regulated over the counter desks to subsequently conduct peer-to-peer transactions through informal networks, to bypass oversight.

3.66 Over the counter broker-facilitated trades in the UK have been identified as being cashed out in countries such as Albania, Colombia, Russia, Singapore, UAE and Vietnam. The ability to operate internationally and use local associates, dead drops, front companies or escrow accounts to collect and exchange money within the UK makes such services appealing to OCGs looking to exchange large volumes of cash in one jurisdiction and access it in another.

3.67 In peer-to-peer exchanges, traders are introduced online or by word of mouth. Brokers build trust within the community and show their reliability with smaller test trades. Peer-to-peer exchanges can enable criminals to launder potentially large volumes without the need for criminal contacts or

access to financial infrastructure. Some peer-to-peer exchanges have been set up specifically for criminal purposes. [International Controller Networks](#) (ICNs) are known to use peer to peer brokers to exchange cash into cryptoassets and vice versa. The current need for trust limits the use of peer-to-peer networks at scale. However, the introduction of smart contracts effectively removes this need for trust as it automates transactions, which may increase the usefulness of peer-to-peer exchanges to criminals.

3.68 No peer-to-peer trading platforms are currently registered with the FCA. UK-based criminals may be able to circumvent the Money Laundering Regulations by accessing offshore peer-to-peer exchanges using virtual private servers and networks.

3.69 The growth of Decentralised Finance (DeFi) has made cryptoasset money laundering activity more complex. Decentralised Exchanges (DEXs) are services on a blockchain that provide automated cryptoasset transactions between two parties, matching buyers with sellers. These exchanges run on smart contracts which are automated protocols that conduct trades using the liquidity pool of an exchange. DEXs appeal to criminals as they generally do not require identity verification. Most DeFi services operate on public blockchains which have made tracing criminal funds easier. However, criminals continue to adapt, utilising new concealment techniques. One popular technique that allows cryptoasset users to move their cryptoassets from one blockchain to another (chain-hopping) involves using cross-chain bridges. Cross-chain bridges allow different blockchains to securely share data and assets. They employ a messaging system that permits blockchains to pass information to each other in a verifiable way. The cryptoassets remain traceable in most cases, but following transactions is more complex.

#### Mixers and obfuscation services

3.70 There are several tools used to further disguise the source, movement and ownership of cryptoassets. Given the visible nature of cryptoasset transactions, these tools are used by criminals to further conceal their links to criminal funds. Privacy wallets limit law enforcement attempts at seizure. These can take the form of virtual wallets, such as Wasabi, or offline storage devices which need to be connected to a computer to be accessed.

3.71 Mixers and tumblers are used to increase privacy and anonymise transactions to prevent tracing of the cryptocurrency origin. Mixing, tumbling and 'CoinJoin' systems and services include Mixerio and Samurai Wallet. These act as an intermediary to disguise the link between the source and beneficiary. In cases of theft and money laundering, these services are used to hide the source and flow of funds by breaking the link between the sender and receiver. Automated tumbling services enabled by smart contracts on decentralised finance protocols add a further security element by removing any human interaction with funds. Tumbling services have increasingly been the subject of law enforcement activity. While academic and [private sector](#)

research has been conducted on detecting and de-anonymising mixer transactions, transactions involving mixers are still very difficult to trace with the process being lengthy and labour intensive for law enforcement agencies.

#### Other exchange routes

3.72 International controller networks are increasingly accepting cryptoassets derived from cybercrime in return for cash. This cash is sourced from international cash pools generated using IVTS, some of which will represent the proceeds of crimes such as drugs, OIC or tax offences. Cryptoassets have been increasingly used in conjunction with money mules, often in fraud cases. Cases have been identified of mules being instructed to move criminal funds to cryptoasset exchanges before transferring funds into wallets in the control of the mule handler or OCG.

## Trade-Based Money Laundering



3.73 Billions of individual trade transactions take place daily across the world. The primary aim of trade-based money laundering (TBML) is the movement of money or value which is disguised as trade in legitimate goods or services. The UK has considerable exposure to TBML because it is a significant market for trade in goods and services (In 2024, [UK exports](#) totalled £873.5 billion and imports £905.8 billion). The NCA assess it is likely that over £10 billion is laundered through UK TBML schemes each year.

3.74 Criminals can exploit the international trade system to disguise criminal funds and move value using trade transactions to legitimise their criminal origin. The complexity, scale, and relative anonymity of the global trade system make it attractive to criminals who seek to hide the movement of criminal funds within the high volume and value of trade transactions. Criminals can also take advantage of the fact that no single authority or organisation has full sight of the threat. TBML is, however, rarely used in isolation; it is often part of a wider scheme of money laundering such as [informal value transfer systems](#) and [cash smuggling](#). It is often linked to predicate crimes, including tax evasion, fraud, drugs, and MSHT.

3.75 There are a variety of processes currently employed by criminals to integrate criminal funds into trade:

- Mis-declaration of the goods including over and under-invoicing which involves the misrepresentation of the price of goods or services to transfer value; or
- Mis-stating the quality or type of good to justify value differences;
- Issuing multiple invoices for the same transaction to justify multiple payments for the same shipment of goods or delivery of services;
- Fictitious trading (also known as ghost or phantom shipping) which can involve the misrepresentation of the quantity of good or services, but regardless of any other attempts at manipulation, ultimately no goods are actually traded.

3.76 Financial institutions play a vital role in transferring funds between the importer and exporter, but techniques used by launderers can make detection of TBML challenging. Accountants and other financial advisors can be at the frontline of suspicious activity detection in noting changes to how a business trades - for example, if it significantly diversifies from one sector (like textiles) to an entirely unrelated sector (like specialist computer parts), or an entirely unrelated third party becomes involved in payment settlement. Criminals and professional money launderers can also exploit company formation and related services to add further complexity to their schemes.

#### Open Account Finance

3.77 Open account trade finance involves exporters extending credit directly to the importer of the goods without the direct involvement of third-party finance (like a bank). Goods are usually shipped before payment is due. It is the most common trade facilitation method, accounting for more than 80% of all trade transactions worldwide.

3.78 As financial institutions are involved solely in transferring funds between importer and exporter, they may have limited opportunities to identify suspicious activity. Complicit importers and exporters might launder the proceeds of crime through an ostensibly legitimate relationship.

3.79 In certain circumstances, a traditional financial institution isn't involved at all, and the settling of trade debts can be facilitated through Informal Value Transfer Service providers. Through these means criminals might avoid international banking costs, secure preferential exchange rates, and access markets that might otherwise be difficult to enter.

#### Trade Financing

3.80 Trade Financing accounts for the remaining 20% of global trade facilitation, covering several different types of financial instruments. In these situations, importers and exporters negotiate terms, including payment methods and the use of financial instruments.

3.81 These types of trade relationships involve financial institutions, as they can facilitate the movement of goods by releasing funds subject to mutually agreed trade-related documents. For example, a bank might insist on seeing the bill of lading which includes information about the goods being transported, payment and the sender and receiver. TBML in trade financing often involves complicity between the importer and exporter. The same methods, such as goods mis-description, still occur but criminals are likely to employ increasing levels of sophistication to avoid raising suspicions of the trade finance provider.

## Factoring

3.82 Factoring is a type of financial transaction where a business, such as an exporter, will sell its debt to a third party called a factor, in return for the provision of an immediate cash injection – usually an amount lower than the debt owed. The factor will then pursue payment of the debt directly with the importer. Invoice factoring firms can be financed by banks with the loans secured over the factored invoices.

3.83 In TBML schemes factoring can make cash available from a legitimate source in the financial services sector, while a complicit importer can integrate the proceeds of crime through structured repayments to the factor. Some loss is anticipated, given the cash made available is lower than the debt owed, but it can be an effective process to further complicate trade relationships and associated financial transactions.

## Third-party payments

3.84 Separate to the involvement of a factor as a third party, who is not complicit in the laundering scheme, some TBML schemes identified involve an unrelated third party (usually a shell or shelf company), who receives payment from the importer but where the relationship with the exporter is unclear. The risk is heightened if third parties are situated in jurisdictions with perceived limited compliance oversight. Whilst the presence of a third party does not fundamentally alter how funds are laundered, it can make oversight of trade finance more difficult.

## Trade in services

3.85 Trade in services refers to the exchange of intangible products between a service provider and a consumer (for example a specialist IT consultant). Assessing a fair market price for services is less clear, as the value of professional expertise or intellectual property is subjective. The value or description of services provided can easily be manipulated, whether over-valued or completely made up, to hide suspicious payments. Similar methods can be used to conceal illicit payments, including bribes.

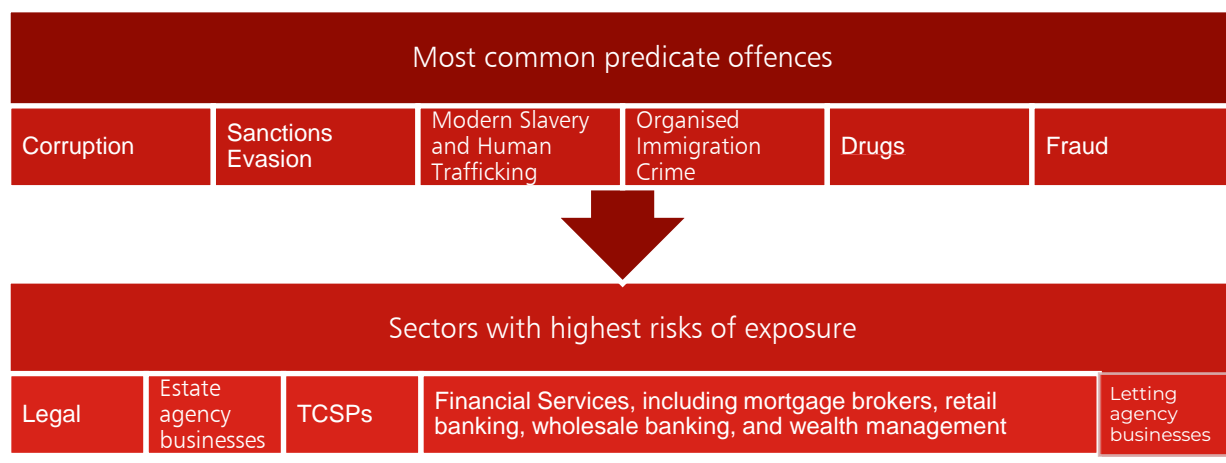
### **Box 3.J - Case Study: Trade Based Money Laundering scheme**

A stand-alone cash seizure led to the identification of alcohol diversion fraud using TBML to launder the funds. The supposed trade was in a well-known energy drink. A USB pen drive recovered during the investigation listed transactions totalling millions of pounds, but there was no evidence of a warehouse or other storage facility in the UK, nor any transport logistics or physical shipping of goods which might support legitimate trade.

None of the businesses had applied for an Economic Operators Registration and Identification number (EORI) – which is necessary to move goods in all but a few limited circumstances – or made any import declarations. In effect, profits from the alcohol diversion were being laundered through “phantom shipping.”

Cash was deposited into multiple UK business bank accounts (through “smurfing”) which were under the control of the suspects, before being electronically transferred to the United Arab Emirates (UAE). In total £26 million was transferred to the UAE, using counterfeit business documents to support the movement of funds.

## Property



3.86 Property purchases remain an attractive method to launder illicit funds due to the large amounts which can be moved and the stability of property as an asset. Property also offers an opportunity for criminals to continue to profit from their criminality by either renting out a property they have purchased, renovating a new property and re-selling it quickly, or leaving the property to appreciate over time. UK property has been seen in all predicates and typologies; all criminals need somewhere to live and base their operations. The NCA estimate there is a realistic possibility up to £10 billion could be laundered through the UK property market annually.

3.87 Many of the sectors in scope of the MLRs will have some role in property transactions, whether directly involved in the purchase, securing the funds, or setting up structures to hold or control property. There are some methods of purchasing property which bypass the regulated sector, for example by transferring a company that holds property. However, there is little evidence that criminals are currently using these methods.

3.88 Criminals often buy property after using other money laundering methods. These methods increase the distance between the property purchase and the criminal source of funds, providing a veneer of legitimacy. This veneer could help them avoid triggering stricter enhanced due diligence checks by [estate agents](#) and [conveyancers](#).

### Residential property

3.89 There are money laundering risks for residential properties at all values. Prime and super-prime (the top 5% in value of property in a geographical area/postcode) residential property continue to be attractive to criminal actors as a stable asset to store value without depreciating in the medium-long term, or for the prestige and high living standards associated with criminal lifestyle. High-value property is frequently identified in relation to overseas predicate offences, with examples including the proceeds of [corruption](#) and [fraud](#) in Eurasia, Angola, Ghana, Nigeria, China, Pakistan, Russia and Ukraine. These properties are frequently purchased using [complex structures](#) to distance the purchase from the criminal origin of the funds. There are also legitimate

reasons to use corporate structures to purchase property, so the use of a complex structure in and of itself may not be enough to trigger suspicion.

3.90 Where these structures are used to purchase property, the same or linked structures can often be used for the purchase of other high-value lifestyle purchases including private jets and [fine art](#). In the period 2010 to 2021, overseas ownership of UK property [nearly trebled](#), sitting at 0.7% of all UK properties. The introduction of the Register of Overseas Entities requires all overseas entities who buy, sell, or transfer UK land or property to register with Companies House and declare registrable beneficial owners or managing officers.

3.91 This has improved the transparency of UK property ownership, but we have not yet witnessed any significant changes to criminals' property ownership models. Trusts, where data is available on the Register of Overseas Entities on request, or [renting](#) could be used as alternatives for those wishing to avoid public scrutiny. Nevertheless, oversight of these activities from law enforcement agencies and money laundering regulated sectors may limit opportunities for misuse. The higher levels of transparency in the UK may displace criminal property ownership to other global financial centres with rapidly growing real estate sectors that offer similar lifestyle benefits to the UK, such as Dubai, Hong Kong and Singapore. Alongside the use of corporate structures, criminals investing into super-prime property may make use of associates who warrant less scrutiny than if they purchase property in their own right.

3.92 Lower or mid value properties still represent an attractive investment for criminal funds although they cannot individually be used to launder the same volumes as super-prime properties. Lower value residential properties can also be purchased or let to commit further criminal offences (more detail in the [Letting Agents](#) chapter).

#### **Box 3.K - Case study: PEPs**

The spouse of a former foreign PEP who moved funds into the UK to purchase a property was initially not identified through screening as a PEP, owing to the use of an alternative surname that was not detailed in screening tools. This meant that they avoided enhanced due diligence at on-boarding. It was not until after the spouse had opened their account that the flow of funds was identified as not aligning to the spouse's stated profile as a 'homemaker' and flagged as high risk.

#### Commercial Property

3.93 Commercial property of any value can be used for money laundering purposes. This ranges from high street shops (discussed in the [cash](#) typology chapter), to properties used as factories, office blocks and hotels. The value of property varies throughout the UK, with the highest value properties typically concentrated in London.

- 3.94 Some characteristics of high-end commercial property limit its use to certain types of criminals. There are fewer transactions than in residential property, and the high value - reaching up to tens or hundreds of millions of pounds - often requires financing through regulated financial products. It can also be slower and harder to sell on compared to super-prime residential property. However, for criminals looking to profit from their criminality over a longer period of time, investing in or renting out high-end commercial property offers higher dividends than residential or lower-end commercial property. Complex, opaque company structures are also less likely to raise suspicions in the commercial sector than in the residential market. The use of unit and investment trusts, Real Estate Investment Trusts (REIT) and Open-Ended Investment Companies (OEIC) are common vehicles to invest in commercial real estate.
- 3.95 An REIT is a vehicle that allows an investor to obtain broadly similar returns from their investment as they would have had they invested directly in property. The REIT is a limited company, or group of companies, that elects into the REIT regime. The REIT is required to invest mainly in property and to pay out 90% of the profits from its property rental business as measured for tax purposes as dividends to shareholders. The REIT is exempt from UK tax on the income and gains of its property rental business. An [OEIC](#) is a collective investment scheme that is structured as a company with variable capital and satisfies the property and investment condition in section 236 Financial Services Management Act 2000. Once authorised by the FCA, it is incorporated as a company under The Open-Ended Investment Companies Regulations 2001.
- 3.96 Whilst vehicles managed by authorised Asset Managers are subject to limited regulatory oversight by the FCA, there is often less transparency in investment in property funds than in outright ownership of a property. Investment into high-end commercial and residential property is often found at the end of the money laundering process, where funds have been laundered through several jurisdictions before reaching the UK.
- 3.97 The exact scale of money laundering through high-end commercial real estate is unknown. Identified examples have included the use of professional services and criminals financing property purchases with [bridging loans](#), which are then replaced by mortgages from UK financial institutions (bridging finance is a short-term loan used to bridge the gap between money going out and money coming in). Criminals have set up bridging loan companies to launder their funds, issuing their criminal capital as bridging loans which are then repaid as legitimate investments. Bridging finance is characterised by speed and flexibility, making it a popular choice for property transactions. However, the rapid nature of these transactions also makes bridging finance susceptible to money laundering risks. Bridging finance firms are supervised by the FCA, many as annex 1 activity under the MLRs. Some bridging finance is regulated under FSMA.

### **Box 3.L - Case study: Use of property to launder funds**

A loans and financial services company set up by a Chinese national in China created Chinese shell companies between 2006 and 2020 to fraudulently acquire over a thousand complex loans worth RMB hundreds of billions (GBP tens of billion) from Chinese banks. In 2017, the criminally derived funds were used to purchase and invest in property development in the UK. This investment used UK corporate structures.

3.98 Lower-value commercial properties are more frequently exploited by UK-based organised crime groups associated with [drugs, waste crime](#), and [modern slavery and human trafficking](#). These premises can be purchased or rented to be used as a base for [cash](#)-based money laundering or used to commit further criminal offences. Large scale cannabis cultivation using commercial premises is increasing in the UK. These setups have the capacity to produce high yields of cannabis contributing to high profits. Further information on the use of rental properties to facilitate criminal activity is found in the [Letting Agency Business](#) chapter.

## Companies and Trusts



### Companies

3.99 Intelligence suggests there is widespread abuse of otherwise lawful corporate structures and legal arrangements (e.g. trusts) by criminals for money laundering purposes. Corporate structures are used in a range of money laundering typologies, to conceal the origin and destination of funds and to falsely legitimise money movements so they appear to be normal business transactions. The separation of personal identity and the alleged business activity provides an additional layer of complexity during investigations and prosecutions.

3.100 Corporate vehicles can be created and run by the criminal themselves, but frequently require the input of third-party nominees and professional service firms. Reforms under the Economic Crime and Corporate Transparency Act aim to make it more difficult for corporate structures to be exploited and reduce vulnerabilities.

#### Use of companies for UK-generated criminal funds laundered within the UK

3.101 The UK is a popular environment to register private limited companies and limited liability partnerships. Registering a UK company has historically carried prestige. In addition, the low incorporation and running cost increases their attractiveness to legitimate investors. However, these same features are also attractive to a wide range of criminal actors, operating at different scales of criminality.

3.102 UK companies can be used as used as 'fronts' by local and regional UK criminals generating lower volumes of funds via [acquisitive crime](#), [drugs](#) offences and [waste crime](#). In some cases of [fraud](#), [tax evasion](#) and [environmental crime](#), the UK corporate structure is used both to generate the income and launder the funds simultaneously.

3.103 To avoid detection, the criminals may use phoenixing to continue their criminality without the bad reputation associated with the previous company. Phoenixing refers to the practice of carrying on the same business or trade successively through a series of companies where each becomes insolvent in turn. Each time this happens, the insolvent company's business, but not its debts, is transferred to a new, similar 'phoenix' company. The use of [nominee directors](#) not associated with the previous firm, or 'off the shelf companies' who have previous trading history and licenses, may also be used to offset obvious indicators for phoenixing. A UK 'shelf' company is a company incorporated at Companies House, usually by a formation agent, but which is inactive. They are often marketed as reputable, established companies, with some having shareholders and directors, sometimes being publicly traded. Although the companies are sold complete with all the requisite registration, documentation, and licenses of a legal entity, they are not yet trading.

3.104 Criminals also continue to use corporate structures as a useful cover for paying large sums of criminal cash into [bank accounts](#). This is frequently linked to cash intensive businesses.

#### Use of companies to launder UK-generated criminal funds cross border

3.105 Criminal funds generated in the UK are also moved cross border via both UK and non-UK corporate structures. Moving funds across borders is more likely to involve a network of companies which are often set up and run by [complicit professional](#) enablers. Structures are set up in the UK, in intermediary jurisdictions, and in the destination jurisdictions to receive the funds. Since 2020 there has been an increase in the use of scrap metal dealer companies to move criminal funds outside the UK. Criminal cash is passed to a complicit scrap metal dealer company, who then purchases off-book and/or stolen metal and sells it into the legitimate supply chain to realise its value. A network of companies is often used to send this money overseas, with the UAE, Netherlands, China, Spain, Poland, Türkiye and Cyprus all identified as destination countries for the criminal funds.

#### Use of companies to launder criminal funds generated from overseas

3.106 UK companies have also been used as fronts to opaquely move or store assets from criminal funds generated overseas. This involves UK companies being set up under the guise of a legitimate business purpose, to more easily open bank accounts with UK or overseas financial institutions. In many of these cases, little to no funds move into or through the UK financial system.

3.107 Companies House records show examples of mass incorporations of UK limited companies, often purporting to be linked to foreign nationals. These companies are often dissolved within twelve months with minimal interaction with Companies House. How these companies are used and their exposure to criminality is an intelligence gap, but it is highly likely they are being used to deliberately hide the true ownership and control.

3.108 Criminally complicit TCSPs have also been identified advising clients to exploit the UK company formation process, including by registering as dormant. UK corporate structures also continue to be exploited by Russian serious and organised criminals, both to commit criminal offences and to launder criminal funds. It is likely that many of those seeking UK companies for criminal purposes use TCSPs, based either in the UK or overseas.

### **Box 3.M – Case Study: Operation Hammerhead**

The Insolvency Service’s Operation HAMMERHEAD began in 2022. Initially identifying 41,000 UK corporate structures, most of which had a single director, were registered as dormant, and shared addresses (over 10,000 structures were identified at one flat address). These were either set up by UK TCSPs (one of which set up c30,000 of the 41,000 companies) or TCSPs that appeared to be based in China. Payment for registration often came from China, including Hong Kong.

- Some HAMMERHEAD companies were used in TBML. The UK companies used bank accounts in China and UK electronic money institutions (EMIs). TBML transactions were always in EUR or USD. The total transactions averaged EUR 800,000 per account (but went as high as EUR 3,600,000) over a period of less than a year.
- Other HAMMERHEAD companies were used to move suspicious funds into the UK. This was done via bank transfers for buying property, education or T1 investment visa fraud.
- Another HAMMERHEAD-linked corporate director and corporate service provider was identified by the United Nations as the owner of the North Korean shipping fleet.

The NECC co-ordinated the response, seeking to identify and take enforcement action against high-risk company incorporation locations and corporate entities believed to be enabling criminality. This project involved the NCA, HMRC, Companies House, the Insolvency Service, FCA, OPBAS, Home Office, and UK police.

HMRC led the first intensification exercise under HAMMERHEAD, joining with other Law Enforcement Agencies to visit 11 suspect addresses. Relevant information was shared with fellow agencies, including referrals to Companies House which up to April 2025 has fed into the striking off of more than 8,000 companies and facilitated the defaulting of more than 22,000 company addresses (placing roughly 11,500 in the strike off path).

### Overseas Companies

3.109 Overseas companies identified in law enforcement investigations are frequently part of complex arrangements involving numerous shell companies and trusts across multiple jurisdictions, including the UK, with long, complex chains of transactions. Companies identified in UK law enforcement cases are frequently incorporated in countries with [close ties to the UK](#), including some of the UK’s Overseas Territories and Crown

Dependencies, other global financial centres like Hong Kong, and European jurisdictions including Malta and Cyprus.

3.110 The use of these complex arrangements is often associated with high value overseas predicate offences, including [corruption](#) and [fraud](#), where funds are routed through varying combinations of transit and end points making it difficult to isolate any one single jurisdiction. The UK is frequently not the sole 'end destination' for these criminal funds.

3.111 There has been a fall in the number of new company registrations in the BVI, dropping to a 25-year low in 2023. Nonetheless, BVI companies continue to feature in UK money laundering cases, often as part of a complex chain of corporate structures and linked to the purchase of UK property. The BVI continues to be the jurisdiction receiving the highest number of requests for beneficial ownership information from UK investigators under the exchange of notes agreement (whereby the UK and the Crown Dependencies and Overseas Territories allow company beneficial ownership information to be shared between law enforcement agencies on request). 36 single requests and 39 multiple company requests were made in 2023. These requests to BVI exceeded the sum of requests to all other Crown Dependencies and Overseas Territories in 2023. There are also risks around BVI Trust and Corporate Service Providers' (TCSPs) use of third parties (also referred to as introduced business relationships), who instruct BVI TCSPs on behalf of their own clients. Whilst these relationships are mainly used for legitimate purposes, they can be exploited by those seeking to hide beneficial ownership and [illicit financial activity](#).

3.112 Isle Of Man and Jersey companies have also featured in complex business structures alongside the Overseas Territories and other overseas jurisdictions. These often involved the movement of funds linked to suspected corruption, drug trafficking, fraud and tax evasion, as well as to hold UK property.

## **Trusts**

3.113 The misuse of trusts for money laundering remains a global problem. They are rarely used in isolation, but as part of complex structures layered with corporate structures. Trusts are often used as the last step in the money laundering process after other laundering methods have been used to disguise the origin of funds. Trusts can provide the appearance of distance between the settlor and the assets, when in reality the settlor may maintain a level of control over the assets.

3.114 Trust arrangements are often more complicated than corporate structures and likely require professionals to establish. This, and the longer-term nature of trusts, mean they may not be useful for those criminals looking to move small to mid-levels of funds quickly and cheaply. While trusts have been identified in significantly fewer cases than corporate structures, they tend to

be of higher value, frequently in the tens of millions of pounds and often linked to [international corruption](#), [sanctions evasion](#) and [serious fraud](#).

### UK Trusts

- 3.115 Trusts have been a feature of the UK legal system for centuries, and are widely used for charitable, pension, investment and vulnerable person protection purposes. Although the exact number of UK trusts is unknown, as of March 2024 over 733,000 were registered with HMRC's Trust Registration Service (the register of beneficial ownership of trusts). Whilst some features of trust structures may be attractive to criminals, we continue to assess the overall risk for UK trusts to be low – although the level of risk varies between different types of trusts. Our low risk assessment is driven by the UK's regulatory requirements, the low scale of abuse identified by law enforcement, and the differences between UK trusts and higher risk offshore trusts.
- 3.116 In the UK, those providing trustee services must register as a TCSP under the MLRs, and the requirement for trust details to be registered on the Trust Registration Service ensures their information is available to law enforcement. The Trust Registration Service requires trustees to provide and update information on the parties involved in the trust, and it requires tax-paying trusts to provide information on the assets held at the time of registration. This is likely to make UK trusts less attractive for money laundering.
- 3.117 Identified instances of misuse of UK trusts are very low. Since 2020, the MLRs-regulated sector have reported fewer higher risk clients using complex arrangements such as trusts. These may have been displaced to service providers outside the UK with more attractive trust structures and less robust regulatory frameworks, although further work is needed to better understand the drivers of this trend.
- 3.118 Some higher risk trust structures, such as private purpose trusts, are mostly not permitted in the UK. There are other types of UK trusts that may pose a higher risk, including trusts used to hold UK property. Whilst the vast majority of these trusts likely hold property legitimately, there is a risk they may be attractive to conceal the true owners of UK property, or avoid public scrutiny on the Register of Overseas Entities. [Transparency International UK's](#) analysis of evidence collected since 2016 found at least 170 properties – worth £2.5 billion – were bought with suspicious wealth and owned using UK or offshore trust structures. These properties have ties to sanctioned individuals, politically exposed persons (PEPs) from high-corruption-risk countries, and individuals charged or accused of corruption-related offences. There is no distinction between UK or overseas trusts in the report, but at least two of the trusts identified were UK trusts.
- 3.119 Other types of UK trusts that have a realistic possibility of posing a higher risk include discretionary trusts (with trustees able to make payments or

provide access to assets at their discretion) or interest in possession trusts (which allow one beneficiary to receive income earned from assets while the assets themselves are held for a second beneficiary), as they allow quicker access to assets.

### Overseas Trusts

3.120 It is highly likely that criminals favour overseas trusts for money laundering in the UK. Trusts from the British Virgin Islands, Gibraltar, Guernsey, and Jersey have been identified frequently in UK law enforcement investigations, with trusts from USA, Liechtenstein, and Luxembourg less frequently appearing. The features that make trusts in these jurisdictions attractive to legitimate customers in the UK - the use of English common law, their cultural and financial links with the UK, their lower tax liabilities, and their highly developed infrastructure for complex trust products - likely also drive their attractiveness to criminal actors.

3.121 The UK CDs and OTs provide beneficial ownership and tax information on corporate structures to the UK when requested under the Exchange of Notes system, but trusts do not fall under this system. There is also no requirement to register trusts in most CDs and OTs. Unless these trusts incur a UK tax liability, have other UK business or property links which trigger registration with HMRC's Trust Registration Service, or are part of UK-property holding structures reportable on the Register of Overseas Entities, UK law enforcement agencies must obtain this information via mutual legal assistance. This means UK law enforcement agencies may find it more difficult to identify the beneficial owners of these overseas trusts compared to UK trusts, increasing their attractiveness. This can be mitigated by strong cooperation between the UK and overseas partners, such as that between the UK and the Crown Dependencies.

3.122 Like UK trusts, overseas trusts used to hold [property](#) and land present a heightened money laundering risk with suspected links to the proceeds of corruption and kleptocracy. There are around 17,000 properties in the UK where an overseas entity is subject to a trust structure.

3.123 Some Jersey trusts have featured in complex corporate networks, covering several jurisdictions and associated predicate crimes including suspected fraud and corruption. Approximately half of Jersey trusts ([50.8%](#)) are discretionary trusts. Discretionary trusts are likely to be favoured by criminals as they afford greater autonomy to the trustee, thereby further distancing the settlor from the assets.

3.124 Further vulnerabilities exist for Private Trust Company businesses. Private Trust Companies are mainly used to support Family Office structures administered on behalf of Ultra High Net Worth families by a TCSP. A Private

Trust Company can also act as the corporate trustee to a Jersey Property Unit Trust, commonly used to acquire and hold interests in UK property.

3.125 Some Guernsey trusts also feature in UK intelligence as being exploited by criminals, including concealing assets linked to suspected bribery, fraud and [embezzlement](#). The Guernsey trust landscape is similar to that of Jersey. Guernsey offers Private Trust Foundations and Private Investment Funds. Private Trust Foundations offer the features of both a company and a trust which make them attractive for estate planning purposes.

3.126 Private purpose trusts are more common in other common law jurisdictions such as Cayman Islands 'STAR' trusts, BVI 'VISTA' trusts, and Cook Island purpose trusts. Private purpose trusts are assessed to pose a heightened money laundering risk because they do not have an identifiable beneficiary (instead, they have a 'purpose'), which could increase anonymity in who or how the funds from the trust are benefitting.

## Professional Enablers

3.127 When a criminal generates illicit proceeds, they need to decide how to launder the funds so they can spend the proceeds and continue their criminality. Some criminals will choose to 'self-launder', but depending on the scale, form of the funds, and seriousness with which the criminal wishes to conceal the funds, self-laundering is not always preferable. The skills and expertise of professional services can be valuable for criminal purposes in addition to legitimate endeavours. Criminals will frequently 'outsource' laundering to 'full time' third parties, who are rarely involved in the proceeds-generating illegal activities. Instead, they provide expertise to disguise the nature, source, location, ownership, control, origin, movement and/or destination of funds to avoid detection.

3.128 A professional enabler is **defined** as "an individual or organisation that is providing professional services that enables criminality. Their behaviour is deliberate, reckless, improper, dishonest and/or negligent through a failure to meet their professional and regulatory obligations". Professional enablers can come from a range of sectors but are most likely to involve skilled professionals such as accountants, lawyers and Trust and Company Service Providers. Details of the risks that different regulated activities are exposed to is found in the sector specific risks chapter.

# Section 4 – Terrorist Financing

## Terrorist Financing threats

4.1 The threat to the UK from terrorism (apart from the Northern Ireland-Related Terrorism threat in Northern Ireland) has remained “substantial” since February 2022, meaning “an attack is likely”. While this is indicative of some elements of the threat from terrorist financing in the UK, it does not provide the full picture. Terrorist financing is not always for the purposes of attack planning; and all or some of the steps in financing terrorism can happen outside of, but still pose a threat to, the UK.

4.2 Where money is raised in the UK, it is typically through legitimate means (like salaries or loans), rather than illicit mechanisms (like fraud or drug trafficking). For example, funds may be received through a regular salary and used to buy and sell cryptoassets. These cryptoassets can then be off-ramped (changed into fiat currency) before being sent abroad via a payment service provider. Funds can be sent overseas to another individual or an account or wallet linked to a particular “cause” or organisation. This individual or “cause” could be based on the border of a high risk jurisdiction, where the funds may then be used to top up a prepayment card and smuggled over a border to benefit a terrorist organisation.

## Terrorist Financing Mechanisms

4.3 Terrorist financing involves the use, possession or raising of funds or assets, for the purposes of terrorism, or for the benefit of a proscribed organisation. This is purposefully broad because terrorist financing can, and does, take a multitude of forms. Terrorist financing can involve illicit or legitimate mechanisms to raise, move and store funds; there can be very small or very large amounts of funds involved. The funds or assets can be used directly to finance terrorist attacks or for more ancillary purposes like living expenses for members of a terrorist organisation or radicalising propaganda.

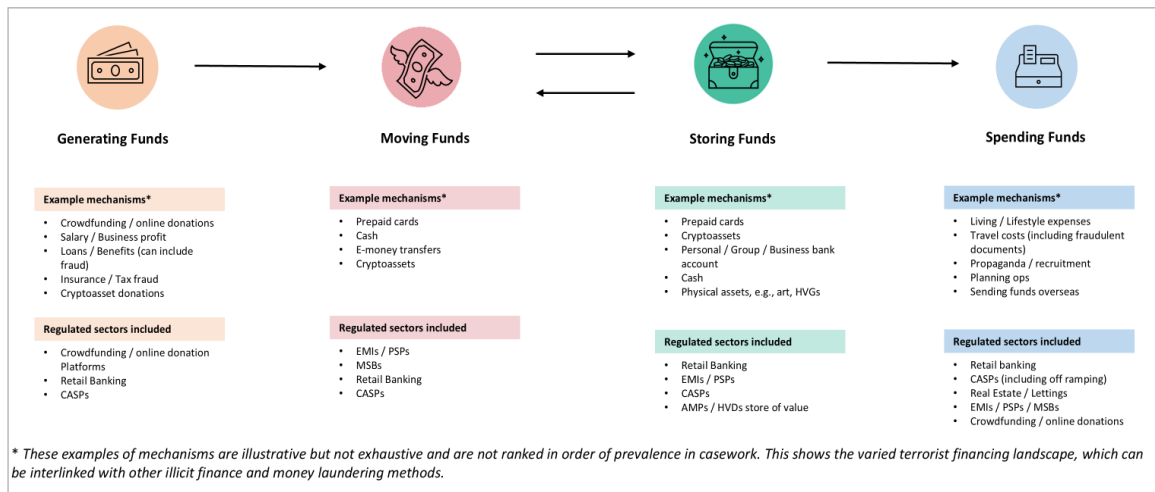
4.4 While the diagram “*Terrorist Financing: Visualising TF Flows*” highlights only a few examples, it demonstrates the wide variety of ways that funds can be generated, moved, stored and used for terrorist purposes. Any of these

mechanisms could be used in the UK or overseas and still constitute a terrorist financing offence. We have, to make it clearer, provided real-life case studies below to show how legitimate funds can be used for terrorist financing (see examples 1 and 2).

### Box 4.A – Examples of terrorist financing mechanisms in the UK.

[larger version in [Annex C](#)]

#### Terrorist Financing: Visualising TF flows



### Box 4.B - Case Study: COVID bounce back loans

Tarek Namouz, a barbershop owner, received thousands of pounds of Covid-19 bounce back loans, which he transferred abroad using a MSB in late 2020 and mid-2021. This was to help organise terror attacks in Syria.

Mr Namouz was found guilty of eight counts of terrorist funding (section 17 TACT 2000) and sentenced to 12 years imprisonment.

### Box 4.C - Case Study: Payments via an MSB

Farhad Mohammad, a businessman, sent two payments in late 2017 and again in early 2018, via a third-party intermediary to his nephew, via an MSB. His nephew was fighting in Syria with a proscribed terrorist organisation.

Mr Mohammad was found guilty of two counts of terrorist funding (section 17 TACT 2000) and was sentenced to a three-year community order, 250 hours of unpaid work, a three-month curfew between 9pm and 8am, and a 30-day Rehabilitation Supervision Order.

## UK SOC – Terrorist financing links

- 4.5 There are some clear links between serious and organised crime (SOC) and terrorist financing. There is an enduring threat to the UK from Northern Ireland-Related Terrorism (NIRT), driven mainly by the threat from violent Dissident Republicans (DRs). The NIRT Threat Level in Northern Ireland has remained 'substantial' since March 2024. DR groups continue to undertake a range of activities to raise funds for sustained violence, including cigarette smuggling, fuel laundering, extortion and robbery, benefit fraud, and both legitimate and semi-legitimate business activity. This is not always for terrorist purposes; the lines between raising finance for DR groups and personal gain are also often blurred.
- 4.6 The vague lines between SOC, paramilitary groups, and terrorist funding in Northern Ireland continue to dictate how law enforcement responds to the risks. Across the UK, predicate offences often fall under the category of organised crime, with the law enforcement response more likely to address this activity through a proceeds of crime offence framework. For example, law enforcement will utilise the powers under the Police and Criminal Evidence Act 1984, rather than TACT, even if the group is a proscribed organisation.

## International SOC-Terrorist finance links

- 4.7 The links between SOC and terrorist financing exist beyond NIRT. For example, the Kurdistan Workers' Party (PKK) in the UK are known to use a hierarchical structure under which there is a network of young OCG members who fundraise, assess, collect, enforce or courier, with the collection of multiple small payments which total millions of pounds. There is evidence that some of these funds benefit attack planning against the government of Türkiye which can include civilian targets, led by attacker planners either in-country or in bordering countries.
- 4.8 The PKK's objectives have been to gain UK public support to put pressure on Türkiye and influence UK foreign policy. They also want to recruit UK nationals, and to fundraise. Fundraising is usually by collection through Kurdish family events, businesses and community events or through organised crime and, more recently, through "charitable" crowdfunding donation-based platforms or shared crypto wallets. The fundraising collections for the PKK are facilitated by either a youth group or a series of 'collectors', supported by PKK-linked OCG members. These OCGs also facilitate the importation of firearms and drugs and have been linked to both the facilitation of illegal migration and trafficking for the purposes of exploitation. OCGs will often use violence to ensure payment or exact punishments for non-payment.
- 4.9 When considering the movement of funds, this activity is mainly from the UK to overseas jurisdictions. We continue to see the use of traditional mechanisms, such as the physical carrying of cash usually below the declaration threshold of £10,000 into/out of the UK, bank transfers, and the use of money service businesses. We are also seeing the increasing use of less

traditional methods, like virtual assets, prepayment cards and crowdfunding donations. Such transfers typically involve low amounts to relatives or associates, currently or previously linked to overseas terrorist organisations. While it can be judged that the funds are not typically being used for attack planning and instead fund general living or operating expenses, the risk remains that the expenses enable the terrorist actor to exist and operate and, therefore, can still pose a direct threat to the UK. The funds sent abroad can also have a UK impact, if the funds are used by an overseas terrorist organisation for propaganda or recruitment.

4.10 Since the 2020 NRA, we have increased our understanding of terrorist financing risks to the UK from organisational terrorism, for example Al-Qaida or Daesh. Organisational level terrorist financing involves raising funds to maintain the core operational functions of terrorist groups. This type of terrorist financing may take place through the extortion of businesses by terrorist groups in high-risk locations, or through the exploitation of ineffective market entry controls by authorities in high-risk locations to prevent terrorist actors having significant interest in businesses. The proceeds from these businesses may then be invested in, or used to provide services to, UK-based entities.

## UK-based terrorists

4.11 Evidence from historic terrorist offender cases suggests that UK-based terrorists generally fund their lifestyles through legitimate methods such as a salary, loan or state benefits, or through online donations via payment services or crowdfunding donation-based platforms. While these funds predominantly contribute to their living expenses, some may use the funds to travel, sponsor the release of individuals of terrorism concern from internally displaced people camps, design and prepare weaponry, or to prepare and carry out attacks.

4.12 The threat from terrorist finance for attack planning in the UK aligns closely with the threat from terrorism in general. The Counter Terrorism Strategy (CONTEST) was refreshed in 2023 and summarised that the primary terrorism threat to the UK continues to be from low sophistication attacks by lone actors or small groups, with perpetrators likely inspired or encouraged by terrorist organisations but without direction or material support, i.e. training, money, or weapons. Attacks of this nature, including their financing, are harder to detect and intercept. The financing involved is typically low-value and often raised through legitimate sources. There is a limited number of terrorist finance cases where funds have passed through the UK from overseas locations for attack planning.

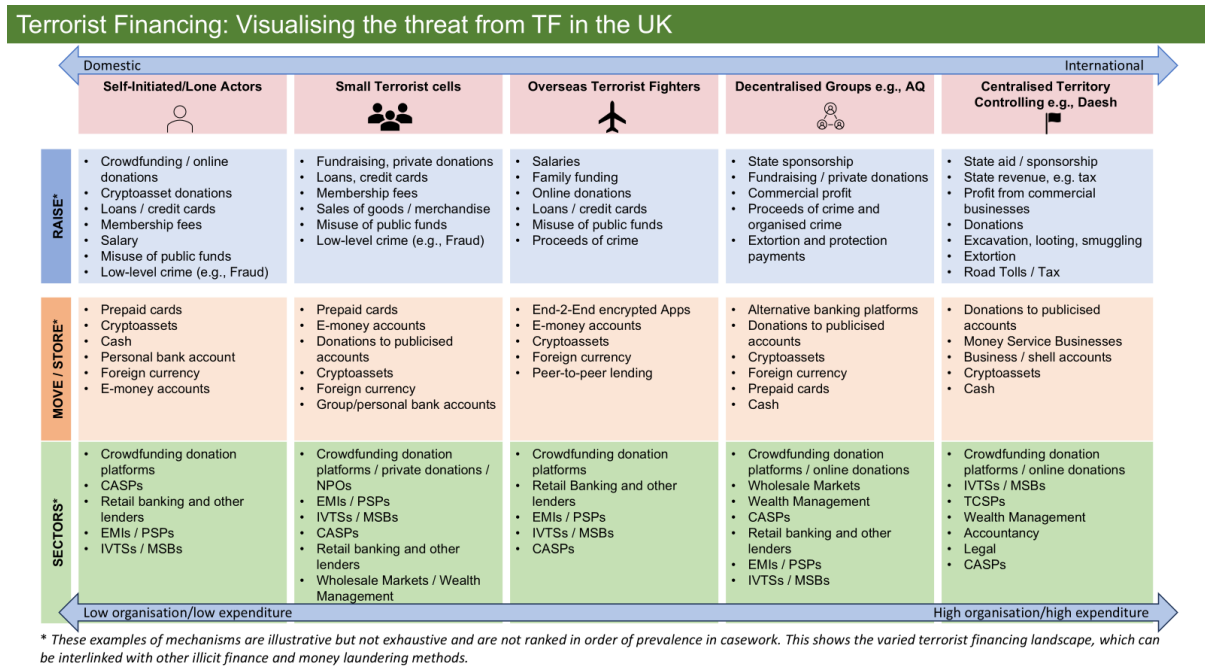
## Terrorist financing by ideology

4.13 The nature of the terrorist actor, such as their level of organisation or strategic intent, will impact the terrorist financing mechanisms that they are likely to use. Diagram “*Terrorist Financing: Visualising the threat from TF in the UK*” shows how the typical methods used to raise, move, and store funds overlap between types of terrorist actors but become increasingly complex

and higher value, as the actor's level of organisation increases. The more sophisticated threat often aligns to a threat being internationally based, rather than domestic.

### Box 4.D – Terrorist financing mechanisms: UK actors versus overseas organisations

[larger version in [Annex C](#)]



## Islamist Terrorism

4.14 CONTEST 2023 highlighted Islamist terrorism as the primary terrorist threat to the UK, accounting for approximately 67% of attacks since 2018. These have been mainly Daesh and Al-Qaida inspired. Since 2020, Islamist terrorism has accounted for the majority of terrorist financing investigations in the UK. Islamist terrorists have either carried out UK-based attacks, travelled overseas to join terrorist organisations and take part in the fighting, or have committed other terrorism offences. Predominantly, funding for Islamist terrorism is likely from legitimate sources such as salary, benefits, applying for credit cards or loans, or by receiving funding from their families or from online donations. However, only low levels of funding are required for bladed weapon or other low sophistication attacks, or for spreading propaganda via social media or messaging channels, whereas higher levels of funding will enable travel overseas or to carry out more organised and sophisticated attacks.

## Extreme Right-Wing Terrorism (ERWT)

4.15 The second greatest domestic terrorism threat is from Extreme Right-Wing Terrorism (ERWT), accounting for approximately 22% of attacks in the UK since 2018. Since 2020, ERWT has accounted for a quarter of terrorist financing investigations. ERWT in the UK has predominantly been associated

with individuals (rather than groups) who have either carried out lone-wolf style attacks or committed other terrorism offences. ERWT appears to be less well-organised in the UK than it is in other countries where it is more prevalent. While UK-based ERW terrorists have generally utilised legitimate methods to generate regular revenue, this is to support their lifestyle rather than to fund attack planning. Methods of funding have included the sale of merchandise, the use of crowdfunding donation-based platforms, and payment service links uploaded onto gaming chat rooms or online forums, which may also include buying and selling cryptoassets.

## Northern Ireland Terrorism

- 4.16 The funding picture for NIRT has not changed significantly since 2020. Remaining DR groups do not require significant amounts of money to conduct small scale attacks, but they 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. Financial arrangements are not standardised within DR organisations, with different sub-groups and individuals receiving and controlling different portions of money. There is judged to be a greater likelihood of centralised control over finance, in addition to localised funding pools in larger DR groups.
- 4.17 The below case studies show how terrorist financing may be carried out differently depending on the ideology or organisation.

### **Box 4.E - Case study: Demonstrating terrorist financing through different ideologies/groups**

Example 1: ERWT - Andrew Dymock, at the time aged 24 (in 2017/2018), was a neo-Nazi who created two now proscribed groups, System Resistance Network (SRN) and Sonnenkreig Division. Mr Dymock was convicted of 15 offences, including five charges of encouraging terrorism (section 1 TACT 2006), two charges of terrorist fundraising (section 15 TACT 2000), four charges of disseminating terrorist publications and one charge of possessing a terrorist publication (section 2 TACT 2006) and other offences of a racial nature. Mr Dymock was jailed for seven years, with a further three years on licence.

Example 2: Islamist Terrorism – Mohammed Owais Sabir, an insurance clerk, was an Islamist extremist whose aim was to further the ideology of Daesh. Mr Sabir sent money to help free Daesh members and supporters from detention in Syria in 2021. Mr Sabir was convicted of nine terrorism offences, including one count of terrorist fundraising (section 15 TACT 2000), five counts of entering into terrorist funding arrangements (section 17 TACT 2000) and the possession of articles for terrorist purposes (section 57 TACT 2000). SABIR was sentenced to seven years imprisonment, with a further one year on licence, and a 15-year terrorist Part 4 Notification Requirement.

# Section 5 – Sector Specific Risks [ML and TF]

## Regulated Activities risks

### Using this section

5.1 This section provides a broad overview of the risks in each sector for firms and supervisors both within and outside the sector and draws links to wider relevant factors such as methods of money laundering that are discussed elsewhere in this NRA. The assessments in this section are designed to be read alongside the regulated sector supervisor's assessments which contain more detail and address elements, such as red flag indicators, that are not included here.

### Risk Scores

5.2 Risk scores are developed using an adapted version of the 'Management of Risk in Law Enforcement' (MoRiLE) model which examines vulnerability, scale and mitigations. Several factors are taken into account, listed below.

$$[\text{Sum of vulnerabilities}] \times [\text{scale}] = \text{inherent risk}$$

$$[\text{Sum of strength of mitigations}] \triangleq \text{mitigation multiplier}$$

$$\text{Final Risk score} = \text{inherent risk} \times \text{mitigation multiplier}$$

### **Box 5.A – MoRiLE methodology**

| <b>MoRiLE category</b> | <b>Risk Factor</b>  |
|------------------------|---|
| Vulnerability          | <ul style="list-style-type: none"><li>• The volume of money in transactions and speed with which it can be moved through the sector</li><li>• The sector's exposure to high risk jurisdictions and individuals (both internationally and those living in the UK)</li><li>• The level of anonymity of ownership of funds that it is possible to maintain whilst transacting with the sector</li><li>• The complexity of the services offered by the sector and how easy it is to access the services offered by the sector</li></ul> |

|            |   |
|------------|---|
| Scale      | <ul style="list-style-type: none"> <li>• How frequently a sector is used for ML/TF and is reflective of the sector's popularity with criminals as a means to launder criminal funds</li> </ul>  |
| Mitigation | <ul style="list-style-type: none"> <li>• Capacity and capability of law enforcement agencies to mitigate the ML/TF risks</li> <li>• Capacity and capability of supervisors or regulators to mitigate the ML/TF risks</li> <li>• Capacity and capability of firms to mitigate the ML/TF risks</li> <li>• This can include staffing, legal powers, technological solutions or other processes or techniques that help to mitigate the threat</li> </ul> |

5.3 Scores are reflective of the assessed risk exposure in typical business activity in the sector but recognise that activity will vary significantly within a sector and edge cases and behaviour may present differing ML/TF risks. Individuals and firms do, however, need to remain vigilant towards the threat of ML/TF and to have in place effective policies, controls and procedures that are compliant with relevant regulations and law. **Where controls are not in place or are inadequate, this will increase the risks to which a firm is exposed to.**

5.4 Each section sets out:

- **A brief description of the characteristics of the sector**
- **The risk rating** and a brief examination of the MoRiLE factors that have contributed to the overall risk rating.
- **Areas of particularly high risk.** Firms should also refer to their supervisor's assessment for more detail.
- **Activities currently outside the scope of the MLRs,** where evidence has been made available since the 2020 NRA to enable a more thorough assessment of the ML/TF risks.

## Box 5.B - Risk Scores

| SECTOR                        | ML Risk Rating | Change Since 2020 |  | TF Risk Rating | Change Since 2020 |
|-------------------------------|----------------|-------------------|--|----------------|-------------------|
| Retail Banking                | High           | No Change         |  | High           | No Change         |
| Wholesale Banking And Markets | High           | No Change         |  | Low            | No Change         |
| Wealth Management             | High           | No Change         |  | Medium         | Increase          |
| Insurance                     | Low            | New               |  | Low            | New               |
| EMI/PSPs                      | High           | Increase          |  | High           | Increase          |
| Cryptoasset Businesses        | High           | Increase          |  | Medium         | No Change         |
| MSBs                          | High           | No Change         |  | High           | No Change         |
| HVD                           | Medium         | No Change         |  | Low            | No Change         |
| Art Market Participants       | Medium         | Decrease          |  | Low            | No change         |
| Casinos                       | Medium         | Increase          |  | Low            | No Change         |
| NPOs                          | Low            | No Change         |  | Low            | No Change         |
| Legal Service Providers       | High           | No Change         |  | Low            | No Change         |
| Accountancy Services          | High           | No Change         |  | Low            | No Change         |
| TCSPs                         | High           | No Change         |  | Medium         | Increase          |
| Estate Agency Businesses      | Medium         | No Change         |  | Low            | No Change         |
| Letting Agency Businesses     | Low            | Decrease          |  | Low            | No Change         |

## Retail Banking

| Retail Banking      | NRA 2017 | NRA 2020 | NRA 2025 |
|---------------------|----------|----------|----------|
| Money Laundering    | Medium   | High     | High     |
| Terrorist Financing | High     | High     | High     |

### Introduction

5.5 Retail banking is defined as banking that offers core services to individuals and smaller businesses. Retail banking is a cornerstone of the UK's economy. The sector underpins individuals' everyday access to crucial financial services, such as personal current accounts, savings accounts, debit and credit cards, loans, mortgages, and overdrafts, with c. 97% of people over the age of 15 in the UK owning a debit card. The sector includes building societies, traditional high street banks and challenger banks. The Financial Conduct Authority is responsible for the conduct of the sector and as of 2025 covers around 150 retail banking firms. Challenger banks – newer types of banks outside traditional high street banking, many exist online-only – remain a significant component of the financial sector, and their rapid growth contributes to the sector's overall risk profile, particularly due to concerns that their expansion may outpace the development of effective anti-money laundering controls.

### Money Laundering Risk

5.6 The ML risk for retail banking remains **high**. There is persistent targeting of the sector by criminals as integrating illicit funds into the legitimate financial services sector is often necessary to spend, store and use criminal funds.

5.7 The risk rating is assessed as high due to the structural nature of the sector: its transaction volume, simple onboarding processes and mass market nature. The continued decline in face-to-face retail banking (over 5,000 high-street bank branches are planned to or have shut down since 2015) has changed banks' ability to conduct face-to-face checks when customers open accounts. The increased use of online banking (including online only banks/accounts) has led to concerns AI could be misused to create fraudulent documents or circumvent identification controls (such as deepfake videos) when customers create new accounts.

### Vulnerabilities

5.8 The speed of high-volume cash movement through faster payments increases the sector's vulnerability to ML risks, allowing the layering of criminal proceeds. Whilst the sector may have access to more information on their customers' habits and transactions than some other sectors, the increasing diversification of customers having multiple accounts across different service providers and access to services such as crypto assets has created gaps where often no single bank has the full picture of a customer's finances.

## Scale

5.9 Most forms of money laundering will have a touch point with retail banking at one, or all stages of the money laundering process. The sector faces a high scale of abuse, with a particular focus on those that accept high levels of cash deposits. SARs submitted by the sector continue to be high, and in 2023/24 SARs submitted by banks continue to exceed the sum total of all other sectors' SARs combined. However, it is not possible to link increased reporting of SARs from the retail banking sector with increased money laundering – the increase may simply be attributable to better awareness and use of SARs from this sector. Whilst the scale remains high, there are some indications that the growth of the Electronic Money Institutions (EMIs) and Payments Service Providers (PSP) sector has displaced a small volume of legitimate and criminal activity away from banks to the growing EMI/PSP sector.

## Strength of mitigations

5.10 Broadly, the sector sees good indicators of strong ML controls, such as clear risk management standards, and a positive culture set by effective governance and AML knowledge. Large established banks generally have a good understanding of the ML risks and control requirements, but there is a possibility that strong growth in challenger banks could see volumes and risks outpacing the strength of controls. Many challenger banks are online only, and traditional banks are increasingly adopting online banking. There is a possibility that automated systems can be abused or do not work effectively, meaning the AML functions are not effectively fulfilled.

5.11 The Economic Crime and Corporate Transparency Act introduced new [information sharing provisions](#) which allows firms to voluntarily share customer information when there are financial crime concerns, allowing for a network view of the ML risk linked to their platforms. Successful implementation of these new measures will give firms richer information sources when undertaking their reporting obligations.

## Money Mules

5.12 Money muling is when an individual wittingly or unwittingly (under the guise of a job or as exploitation/coercion) moves criminal funds in exchange for payment/benefits or in response to threats. This typically involves moving money to one or more bank accounts, then withdrawing cash or cashing-out through other means, such as debit card payments, crypto or international payments.

5.13 In 2023, Cifas estimated 37,000 bank accounts had behaviour associated with muling. A further [FCA review](#) found 194,084 money mules were offboarded by 25 firms between January 2022 and September 2023, only 37% of whom were [reported](#) to the National Fraud Database. This muling is often high volume, involving daily transactions of moderate value. The [Cifas figures](#) suggest under 30s account for 64% of intelligence indicative of money muling.

Difficult socio-economic circumstances may also risk making individuals more susceptible to targeting, particularly through [social media](#) making it [easier to recruit](#).

5.14 Business accounts are increasingly targeted by money mules and now account for [1 in 5 cases](#) reported to Cifas. Business accounts are able to utilise larger amounts of funds without arousing suspicion, particularly in cash intensive businesses. The NCA's [Operation Destabilise](#) saw action against a multi-billion-dollar money laundering operation including the use of business bank accounts through a company called ISM Scaffolding Limited which had £4.31 million passing through its account in just ten months.

#### Use of Post Offices to make bank deposits

5.15 [Cash deposits](#) into the banking system through the Post Office increases the level of vulnerability to ML. The FCA, NECC, industry and Post Office have taken new measures to help limit the risk of abuse of Post Office systems by OCGs. Since April 2023 there has been a move towards card-based transactions, reducing cash deposit limits and improving intelligence sharing. As with money mules, students can act as facilitators for OCGs through depositing cash. One case saw a student (latterly convicted of ML) deposit £84,912 through Post Office accounts, despite having no visible source of income.

### **Terrorist Financing Risk**

5.16 [Terrorists](#), like all criminals, require money to operate, although it may not be immediately apparent how funds are used for terrorism purposes. Not all terrorist financing is large volume; it may be small amounts of money over a period of time that could be stored for future use or used for low-value or 'unremarkable' transactions such as to pay living costs like rent and food. If the funds are also used to benefit a proscribed organisation, or to fund a low sophisticated attack, all the threat actor's funds are considered to be [terrorist property](#) and liable for forfeiture. Recent UK terrorist attacks have not required large amounts of money to mount and have been carried out through low-cost and low-sophistication methods.

5.17 The risk of the retail banking sector being used to finance terrorism remains **high**. As with the ML risk, the sector has an inherent vulnerability due to the ubiquity and accessibility of retail banking products and services: the sector is often used as an "on" or "off" ramp for other sectors (e.g. used to store or move funds before or after the funds have flowed through another sector). This risks the sector being directly or indirectly engaged in the flow of funds for terrorist financing, even where another sector (with perhaps weaker mitigations) has facilitated most of the illicit activity, including the entry or exit of the funds into or from regulated sectors.

## Vulnerabilities

- 5.18 The characteristics of retail banking that make it attractive to legitimate users and underpin the sector's ubiquity can also make it vulnerable to exploitation for terrorist financing. Typically, the products and services offered are easily accessible (a point also raised in the 2020 NRA), reflecting the importance of access to banking services in the UK.
- 5.19 Domestic terrorism-linked purchases are increasingly likely to be small and, when seen in isolation from other behaviours, not easy to associate with terrorist financing activity. Not all banks have visibility over all end purchase data, e.g. where products are low value and from mainstream retailers. This challenge is reflective of the terrorism threat assessment made in the UK's counter-terrorism Strategy "[CONTEST 2023](#)": *"the UK's main terrorism threat is from individuals or small groups outside of organised terrorist network. This makes terrorists less predictable and harder to identify, investigate, and disrupt."*
- 5.20 There are several other vulnerabilities in the retail banking sector that stand out as potentially exploitable for terrorist financing. Funds can be easily transferred between UK accounts and third-party accounts overseas. The third-party accounts may have reduced terrorist financing mitigations in place and be used to store and move funds before transferring to a UK account, helping to mask what could be terrorist funds.
- 5.21 The ease of international transfers also applies to transfers to / from high-risk jurisdictions (although the higher the risk, the more mitigations the bank is likely to have in place). For example, UK account holders may regularly send money to a high-risk jurisdiction. While this is often for legitimate reasons, there is a higher risk that such funds may end up financing – directly or indirectly - terrorist organisations which operate in those jurisdictions. Business account overdrafts and loans can be significantly larger than personal loans and offer both higher repayments over shorter periods and opaqueness about a company's ownership and structure. Funds might be transferred overseas for 'usual' international business activity, but instead be used for terrorism purposes.

## Scale

- 5.22 There continues to be a high likelihood that domestic terrorist financing will involve retail banking because of the client base, wide range of products and services provided and speed and volume of transactions. As an example, since 2020 around £1.9 million has been forfeited from bank accounts through the disruptive powers under the Anti-terrorism, Crime and Security Act 2001 and the Proceeds of Crime Act 2002, by Counter Terrorism Policing (CTP).

## Strength of Mitigations

- 5.23 The retail banking sector is continuing to work collaboratively with HMG, law enforcement agencies and supervisors through the Joint Money Laundering Intelligence Taskforce's "Terrorist Finance Public-Private Threat Group" (TFPPTG). The TFPPTG provides financial institutions with a forum to both share and receive information to help support and develop their understanding of existing and emerging terrorist finance risks.
- 5.24 The sector's capability has improved through the implementation of a number of mitigations since 2020, which has included the setting up of specific "Responsible Officer" roles. This role will own different aspects of the terrorist financing response, including oversight of business and compliance and being reactive to changes in relevant legislation, rules and regulations, and industry guidance.
- 5.25 Law enforcement agencies play a key frontline role in terrorist financing investigations. The use of financial data within investigations plays a significant role in securing terrorism convictions, which may not always be for terrorist finance offences.

## Wholesale Banking and Markets

| Wholesale Banking and Markets | NRA 2017 | NRA 2020 | NRA 2025 |
|-------------------------------|----------|----------|----------|
| Money Laundering              | High     | High     | High     |
| Terrorist Financing           | Low      | Low      | Low      |

### Introduction

5.26 Wholesale markets are a major contributor to the UK's role as one of the world's leading international financial centres with trillions of pounds worth of global funds [transacted daily](#). [Wholesale financial markets](#) enable companies, public sector organisations, governments and financial institutions to raise short-term finance and long-term capital to fund growth, undertake domestic and international trade, manage financial and other risks, and pursue investment opportunities.

5.27 The wholesale markets include trading venues and bilateral dealing arrangements that facilitate the trading of wholesale investment products, and hedging instruments including financial instruments in all asset classes: equity, fixed income, currencies, and commodities. These instruments include shares, bonds, futures, swaps, and other more complex structures which can be tailored to a market participants' specific needs. Wholesale markets also include corporate finance firms that raise funds from a range of investors in the UK and overseas for issuers of securities (such as shares and bonds) that may be either publicly traded or unlisted.

5.28 There are approximately 280 wholesale brokers with combined 2023 revenues of over £24 billion. In 2024, there were also around 260 authorised corporate finance firms that raise funds from investors. There is a large variance in the size of the wholesale brokers market: 50% of firms' revenue is below £10 million and 10% of firms' revenue is above £10 billion. Three firms make up approximately 45% of the total revenues. While voice-broking (i.e. contacting clients by phone) remains the dominant feature of brokers in the sector, electronic trading is becoming more popular e.g. in the gilt market. Many firms are encouraging a shift to electronic trading because margins are higher and there is increased efficiency, especially in speed of execution, settlement and reporting.

### Money Laundering Risk

5.29 Whilst the breadth of activity in this sector means risks vary, the overall money laundering risk in the wholesale sector remains **high**, with the vulnerabilities and scale fairly static since 2020. Money laundering through wholesale banking and markets is typically associated with high value offences including [serious fraud](#), [international corruption](#) or market abuse.

## Vulnerabilities

- 5.30 UK foreign exchange turnover averaged \$3,351 billion daily in April 2024. Whilst there are fewer transactions than in the retail banking sectors, transactions typically have a higher value – often hundreds of thousands or millions of pounds
- 5.31 Wholesale markets are complex. This complexity creates high barriers to entry with most services requiring market expertise, limiting the use of this sector to criminals with access to market expertise. However, complex and fragmented trading chains make it unlikely that any one entity will have full visibility over the end-to-end transaction cycle. This can make it difficult for firms to identify suspicious activity.
- 5.32 Wholesale markets operate globally and are frequently exposed to jurisdictions with significant corruption, [sanctions](#) evasion risks and secrecy laws which make end client identification difficult. Wholesale brokers, however, primarily trade with major financial centres, including London, Singapore, Switzerland, China, including Hong Kong and the UAE or European markets – France, Germany, Spain.
- 5.33 The speed with which funds can move between organisations and across borders varies across the wholesale sector, depending on the instruments used. Swaps and securities move rapidly, and investment funds can be rapidly liquidated to cash or reinvested into other holdings. Other services, including long-term private equity investments, are slower, and may be attractive to different types of criminals, wishing to consolidate the proceeds of crime over time.

## Scale

- 5.34 Cases of money laundering remain low but often exceed millions or billions of GBP. The NCA considers it a realistic possibility that billions in GBP are laundered through wholesale markets annually. SARs containing the Money Laundering Through the Markets ('MLTM') glossary code have increased year-on-year. However, it is not possible to link increased reporting of MLTM SARs with increased money laundering – and the increase may simply be attributable to better awareness and use of the MLTM glossary code.

## Strength of Mitigations

- 5.35 After the 2020 NRA the FCA took action to support firms to mitigate their risks. Following the MLTM thematic review of wholesale brokers in [2019](#), which found key gaps in brokers' money laundering systems and controls, the FCA wrote to industry flagging key areas of concerns as a call to action to address compliance gaps. As a result of this exercise the FCA imposed a business

restriction on one high risk firm and commissioned two [S166](#) Skilled Person reviews.

5.36 In the 2025 follow up [review](#) the FCA identified good practice and progress in processes and controls, including customer due diligence and governance. Areas for improvement included underestimated risks in business wide risk assessments, transaction monitoring, information sharing between firms and training not being sufficiently tailored to firms' business models.

### Correspondent Banking

5.37 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, international wire transfers, cheque clearing, payable-through accounts and foreign exchange services. Consistent with the 2020 NRA correspondent banks have a high level of exposure to high risk jurisdictions and lack of oversight of all parties in the chain.

5.38 Where banks hold only nostro accounts (where the UK bank holds an account in a foreign currency with the overseas correspondent bank), the UK bank's visibility of transactions and financial movement allows easier identification of money laundering risks. For nostro trade finance accounts the TBML risks remain high. Vostro accounts (where the overseas correspondent bank holds an account in the UK bank) allow UK banks less overall visibility over the source of funds, and they are more reliant on counterparty controls to manage risks associated with the underlying clients. There is some evidence to suggest a minor increase in anonymity since 2020, with a reported rise of nesting (correspondent banks holding accounts for other correspondent banks, so the chain is longer and more opaque), partially driven in response to derisking behaviour. In these cases, the respondent bank is unable to see or assess the risk of the original customer. Since the 2020 NRA, there has been an increase in the use of [EMIs/PSPs](#) to move funds cross-border that historically would have been processed directly via correspondent banks.

### Mirror Trading

5.39 In mirror trading, investment decisions are based on algorithms developed from trading patterns of a number of successful traders. The large volumes associated with capital markets provide opportunities for money laundering not viable in other sectors. Our understanding of capital market risks has continued to grow since the 2016 Deutsche Bank 'mirror trading' case. Other attempts to launder between £100,000 and over £10 million via mirror trading schemes have been identified by law enforcement agencies, however, the use of mirror trading in money laundering does appear to be decreasing. This may be driven by the relative prominence of identified cases leading to improved oversight and controls in firms.

### Out of the money (OTM) options

5.40 Out of the money (OTM option; a contract between two entities that gives the buyer the right to trade a security at a given price with the seller) options are the most commonly seen tool for money laundering through the markets as they allow for the creation and buying of worthless securities, whilst appearing to be part of standard market activity. They can then be resold for a higher amount to another participant. Because the option has no worth, everyone involved in the transaction is almost certainly complicit and using it as a means to launder money. The two laundering methods seen using OTM options are far OTM options in markets that have a legitimate use for OTM options, and OTM options on markets that are little traded and where it would be unusual for such a security to be available.

### Wider trading activities

5.41 Some less frequently observed typologies have also been identified since 2020. In secondary equity markets, trading illiquid assets or highly liquid assets can allow layering activity to be easily hidden without much risk of loss through slippage. There is also scope for criminal money to be transferred by varying the profit margins and creating large trades to buy or trade spreads in multiple times, or for clean money to be raised from investors by rogue issuers (usually via mini bonds) directing the funds raised to overseas-based recipients of the funds who then engage in money laundering.

### Asset Management and Alternatives

5.42 There are a number of factors that could increase risk in the Asset Management space, including a trend of money moving towards private assets within mainstream Asset Managers, reducing transparency and sight into ultimate beneficial owners. Within Alternative Asset Managers, there is limited evidence of money laundering through UK established and/or managed private funds and hedge funds. Business models, investment structures, service providers and clients present potential vulnerabilities. The commonly cross-jurisdictional nature of firms' group and fund structures adds to complexity and opaqueness and limits the ability of UK authorities to act.

5.43 Criminals could make substantial business investments via alternative investment funds such as private equity, private credit, venture capital, or property funds and then use any resulting gains as a "legitimate" source of income. Private funds with hard to value assets, opaque investments, and more complex investment structures present additional risks. Increased investment in cryptoassets by Alternative Investment Funds potentially increases risks. Perceived lack of risk, historic underinvestment in controls by firms, and a general overreliance on third-party outsourcing may contribute to illicit actors viewing the Asset Management space as favourable.

## **Terrorist Financing Risk**

5.44 The risk of the Wholesale Market sector being used to finance terrorism remains **low**. The international offer of correspondent banking continues to be one of the sector's main vulnerabilities, due to the need to maintain international relationships with overseas banks that may be located in or bordering high risk jurisdictions.

5.45 Since the 2020 NRA, there has been no evidence of wholesale markets being directly used to finance terrorism. While the ability to obscure large financial flows through big corporations would be attractive for terrorist financing, we assess that the entry requirements for using the sector's products and services are likely to discourage terrorist actors.

### Vulnerabilities

5.46 Despite the sector's risk rating remaining low, there is a residual risk of inadequate AML/CTF and KYC processes and controls, including transaction and sanctions monitoring, and the identification and management of high-risk customers. These risks are more likely to occur in smaller firms.

### Strength of Mitigations

5.47 While resourcing is competitive across investigations, excellent operational relationships exist between law enforcement agencies and specialist supervisors giving confidence in tackling terrorist financing wherever it is identified.

## Wealth Management

| Wealth Management   | NRA 2017 | NRA 2020 | NRA 2025 |
|---------------------|----------|----------|----------|
| Money Laundering    | High     | High     | High     |
| Terrorist Financing | Low      | Low      | Medium   |

### Introduction

5.48 The UK's wealth management sector covers a diverse range of providers offering investment services to customers from a range of income levels. The MLRs apply to persons "whose regular occupation or business is the provision to other persons of an investment service or the performance of an investment activity on a professional basis". The sector is supervised by the FCA, who as of 2025 supervise approximately 400 firms that provide wealth management services as their primary activity. These firms employ approximately 43,000 individuals and have total revenues of approximately nine billion pounds. This total does not include firms where wealth management is not the primary activity, such as banks, which may have divisions that offer wealth management services.

5.49 Wealth management can be divided into portfolio management and non-advised execution-only activity (stockbroking). Portfolio managers provide discretionary and advisory investment management services to retail and professional clients. Stockbrokers facilitate the purchase or sale of traded listed securities or assets.

### Money Laundering Risk

5.50 The money laundering risk for the sector is judged to have remained **high** with little change to the sector's vulnerabilities or to the scale of money laundering since 2020.

5.51 The high value of assets managed or traded by firms in the sector increases its vulnerability to ML and TF risks. Portfolio management risks are driven by the high value of funds managed without direct involvement of the end customer. ML risks in execution-only businesses arise mainly due to the businesses being entirely customer directed, as well as the high volume of trading at high frequency. The sector's overall exposure to high risk domestic and international customers and jurisdictions remains high. Firms' understanding of their ML risk and the measures they take to mitigate these vary across the sector, but is assessed to have remained at a similar level to the previous NRA. Supervisory capacity and capability have increased, with more FCA focus on ML in this sector.

## High Net Worth clients

5.52 The sector can be abused to invest proceeds of crime in legitimate products, with the legitimate investment return concealing the illicit source. High net worth clients are more likely to use complex structures and may have multiple accounts across different jurisdictions. This can make it more difficult for firms to understand the nature of individual transactions and to identify suspicious behaviour. The high concentration of high net worth individuals and PEPs and the global client base of UK-based firms could increase the sector's exposure to the proceeds of political [corruption](#) and [tax evasion](#).

## Family Offices

5.53 The sectoral risk score is based on the regulated sector and does not cover activity that falls outside of the definition of investment firms. As noted in the 2020 NRA, many "family offices" (firms that limit their services to a single family or other connected customers), that operate in the UK are not required to be regulated but can support the management of the family's wealth. There are likely to be at least 1,000 family offices in the UK managing more than £700 billion. These firms may 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.

## Forward look

5.54 The 2020 NRA noted a rise in the accessibility and advertisement of retail investments through exchanges, platforms or advisors. This trend has continued and there has been a move towards online apps in the execution-only space and away from traditional stockbroking. The volume of customers on these platforms and the potential for lower understanding of the purpose or nature of individual transactions may make ML activity more difficult to identify.

## **Terrorist Financing Risk**

5.55 The terrorist financing risk for the wealth management sector is assessed to have risen to **medium**. The risks in this area are similar to those noted for the [TCSP](#) sector, and increased understanding of how these sectors are exposed to terrorist financing risks has driven this change in score. Wealth managers in the UK may be at risk of indirectly funding terrorist organisations through investments in firms who operate in high risk jurisdictions, where centralised terrorist groups are active. Poor licencing and registration processes (market entry controls) do not properly mitigate risks of terrorist actors being the beneficial owners of high-yield businesses such as [extraction mining and industrial scale fishing](#) in these high risk locations. Extortion and related criminal activity in these areas can also lead to indirect funding of terrorist organisations.

## Insurance

| Insurance           | NRA 2017 | NRA 2020 | NRA 2025 |
|---------------------|----------|----------|----------|
| Money Laundering    | Low      | N/A      | Low      |
| Terrorist Financing | Low      | N/A      | Low      |

### Introduction

5.56 The UK's insurance sector covers a diverse range of products and providers. The MLRs only apply to insurers and intermediaries offering long-term insurance contracts (including life insurance policies). As of 2025 there are approximately 1,200 insurers in the scope of the MLRs that are supervised by the FCA. General insurance providers are generally considered low risk and are not covered by the MLRs. However, general insurers do have obligations in the FCA handbook (SYSC 3.2.6) to counter economic crime, the Proceeds of Crime Act and the Terrorism Act. As a result, Joint Money Laundering Steering Group ([JMLSG](#)) guidance recommends that general insurers also adopt a risk-based approach. The ML and TF risks discussed below relate primarily to the MLR regulated sector offering life insurance products and long-term protection products and the wholesale general insurance sector offering products and services that price and underwrite risks from around the world.

### Money Laundering Risk

5.57 The risk of money laundering through the insurance sector is **low**. The UK's 2020 National Risk Assessment did not include a rating for the insurance sector but suggested that the sector was unattractive for money laundering, and we have identified no new evidence to change this assessment. General and life insurance products are widely available, but they are often accessed via advisors or require customers to qualify for them. Insurance products are generally not a good vehicle for moving criminal funds at speed. The anonymity provided by the insurance sector is also generally low as customers have to provide significant personal information to inform an insurer's risk-based assessment during onboarding. The vulnerabilities vary between the life insurance sector and the wholesale sector. The wholesale market generally offers more complex products and as it is highly leveraged towards commercial risk it is more complex to establish beneficial owners than its retail counterpart. The international nature of the London insurance market also increases the sector's exposure to providing cover in high risk jurisdictions, trades or industries.

### Investment Products

5.58 We assess ML risk to be higher in investment products such as unit linked or with-profits savings, endowments, bonds and whole of life policies, which have the potential to be used in a chain to 'clean' money. Use of cash to pay premiums can be considered as a risk factor, though cash is used very

infrequently. Within the life insurance portfolio, the ML risk to policies that only pay on death or illness (for example term assurance, critical illness and income protection) is considered to be limited.

### **Terrorist Financing Risk**

5.59 The terrorist financing risk through the insurance sector is **low**. Insurance was not scored individually for terrorist financing in the last NRA in 2020, but we have not identified changes in the level of risk in the sector. There is no evidence of insurance products being exploited for raising funds and we do not consider these products to provide attractive opportunities for terrorist finance activity. The size of the insurance market in the UK, particularly the London market, and the sector's exposure to high risk jurisdictions do amount to a residual risk that the insurance sector could be vulnerable to exploitation for terrorist financing purposes in future.

5.60 Heightened terrorist finance risks in the wholesale insurance sector generally arise from the international nature of the business, increased complexity of the products offered, relative complexity in establishing beneficial ownership and increased exposure to politically exposed persons. Intermediaries with poor anti-bribery and corruption controls and insurers with poor sanction controls may also increase this risk.

## Electronic Money Institutions and Payment Service Providers

| Electronic Money Institutions & Payment Services | NRA 2017 | NRA 2020 | NRA 2025 |
|--|----------|----------|----------|
| Money Laundering                                 | Medium   | Medium   | High     |
| Terrorist Financing                              | Medium   | Medium   | High     |

### Introduction

5.61 In the UK, Electronic Money Institutions (“EMIs”) and Payments Service Providers (PSPs) firms provide customers with an alternative to traditional banking models by offering non-bank payment services. EMIs and PSPs can be used to: exchange currency for overseas payments; provide prepaid cards, fuel, and gift cards; remittance services; merchant acquiring; open banking services; and provide both international and virtual international bank account numbers. The sector is gaining popularity from the public because of its convenience and accessibility, with relatively simplified digital account set-up procedures offering greater ease of use for customers, faster transaction processing times, and efficiency.

5.62 There has been a decrease in the number of FCA registered and authorised EMIs and PSP firms, with those registered or authorised under the E-Money Regulations 2011 decreasing by 14% from 308 in 2020, to 266 in 2024 and a 15% decrease from 469 in 2020 to 401 in 2024 of those registered or authorised under the Payment Services Regulations 2017 (PSRs). These numbers do not include FCA registered or authorised firms with sole money remittance permission, which are considered MSBs, and supervised by HMRC under the MLRs.

5.63 Despite the recent decrease in the number of firms, the sector has grown significantly in scale in the UK since 2020, with more people turning to non-bank payment mechanisms online. The following annual payments value table shows the growth and scale of the sector since the last NRA in 2020.

### Box 5.C - Electronic Money Institutions & Payment Services Annual Payments Value Table (as reported by firms)

| Calendar year <sup>1</sup> | FCA-registered/authorised EMIs total payments value | FCA-registered/authorised Payments firms total payments value (excluding money remitter only permissions) | Total (£)      |
|----------------------------|---|---|----------------|
| 2020                       | £477 billion  | £444 billion  | £921 billion   |
| 2021                       | £869 billion  | £553 billion  | £1.42 trillion |
| 2022                       | £984 billion  | £675 billion  | £1.66 trillion |
| 2023                       | £1.1 trillion                                       | £963 billion  | £2.06 trillion |

#### Money Laundering Risk

5.64 The money laundering risk in the regulated EMI and PSP sector has increased from **medium** to **high**. The rapid scaling of the sector since 2020, increased complexity and diversification of services, has contributed to the sector's attractiveness for criminals, with increased options to manage and launder funds cross border. There has also been increasing exposure to high risk jurisdictions. There is also a greater understanding of the risk now relative to the last NRA. Whilst risk mitigation has improved, increased exposure and use has driven the increase in risk score.

5.65 Although the risk from PSPs is assessed as high. There are two notable exceptions in HMRC's supervised sectors of Bill Payment Service Providers and Telecommunications and Digital IT Service Providers. Due to a range of factors, including low transaction values, the business models that they operate, as well as their comparatively low numbers, HMRC has assessed the risk from these sectors as Low.

#### Vulnerabilities

5.66 From a customer perspective, EMIs and PSPs may have simpler onboarding processes in comparison to high street banks, with no physical presence required to set up accounts and a simpler process than for most banks. The number of EMIs and PSPs available relative to banks is also an attractive feature of the sector for customers. By extension, this is attractive for money launderers seeking vulnerabilities to exploit.

5.67 Although EMIs and PSPs are required to conduct checks on personal and business customers or agents, where an agent brings a customer, the agent often conducts the relevant checks, instead of the regulated or registered EMIs and PSPs. This may not be as robust, increasing the risk of abuse by criminals. The regulated EMI or PSP retains responsibility for its AML compliance with the regulations, including when using third parties, such as agents.

5.68 The FCA has noted that the outsourcing of anti-money laundering compliance functions to third-party providers can create vulnerabilities in EMIs' and PSPs' controls. EMIs and PSPs can and do use third-party providers to outsource operational functions. When third-party providers are not familiar with the products at the EMIs and PSPs, they may fail to adequately address the specific risks the firms face, creating vulnerabilities in the EMI's and PSPs' control frameworks. It is important that when third-party providers are used, they understand the vulnerabilities the EMI or PSP is exposed to, and controls are appropriately calibrated to prevent abuse by criminals. It is also important that the principal EMI or PSP understands that while it may outsource a function, the EMI or PSP remains responsible for its AML controls' compliance with the regulations, and this responsibility cannot be delegated.

#### Scale

5.69 EMIs and PSPs are being increasingly targeted to launder criminal funds. Over the last 2-3 years, law enforcement agencies and supervisors have worked together to identify and act against firms that are owned or controlled by organised crime groups and who are complicit in facilitating criminal activities. The NCA, HMRC, FCA and others actively share intelligence on live investigations into money laundering through EMIs and PSPs.

#### Strength of mitigations

5.70 The MLRs apply to both EMIs/PSPs and retail banks, but banks are subject to more stringent regulatory requirements in non-MLR regulations, such as the Financial Services and Markets Act 2000. As a result, criminals may have more opportunity to find an MLR regulated firm in the EMIs/PSPs sector with weaker onboarding controls. The FCA has significantly increased its focus on the prevention of financial crime in this sector in recent years and has recorded a 231% increase in EMI and PSP MLR-related supervisory activity between 2020 and 2024. Improved mechanisms have also been established for routinely exchanging information with partner agencies in law enforcement on suspected criminality in the sector. As a result, the FCA, NCA, NECC and HMRC have developed a better understanding of the threat in 2025 than was held in 2020. Remediation tools used by the FCA include:

- feedback to firms with an expectation of remediation.

- requirements applied to firms with their voluntary agreement to limit risks until controls are improved, such as restrictions on high risk customer activity.
- The appointment of an independent skilled person, answerable to the FCA, to review a firm's systems and controls, make recommendations, and assure the remediation.

5.71 In serious cases, including where criminality may be suspected, the FCA may choose to use its powers to prevent a firm conducting any regulated activity. The FCA may refer such cases to internal or external enforcement teams for further investigation, prosecution or other sanction.

5.72 A Transparency International [report](#) noted professionals, who specialise in helping clients obtain EMI and PSP licences, could make it easier for criminals to gain access to the sector. While professional advice can be of value to legitimate firms, they could still be exploited by criminals seeking to enable money laundering. This demonstrates the need for financial crime supervision to keep pace with new and emerging risks as the sector continues to evolve rapidly.

#### Pre-paid cards

5.73 Since 2020, the risk posed by pre-paid cards remains high. These cards can store and move value through cash withdrawals, card purchases, and bank transfers. Some pre-paid card products allow conversion into cash and provide for ATM cash withdrawals. Due to the ease in which these cards can be used cross-border, the service is particularly vulnerable to the placement of criminal funds, with criminals layering transactions to conceal their origin. This allows for the integration of these funds into the legitimate financial system with little trace as to their origin.

#### Virtual IBANS

5.74 Virtual IBANs provide an address and account reference number within a central master account and are issued in the name of a business or individual. A 2024 [McKinsey report](#) found 23% of UK SMEs regularly use fintechs or other nonbank providers for their cross-border payments, possibly due to lower costs and greater accessibility. Multiple virtual IBANs can be issued and linked to a single payment account with customers able to move funds between them. This reduces the visibility of transactions to the authorised banking and custodial partners as the money moves between virtual ledger positions without moving into or from a bank account. EMIs and PSPs providing virtual IBANS can have higher rates of exploitation by criminals as there can be a lack of visibility for the payments provider issuing the underlying IBAN about the identity of end users. This arrangement relies on a reduced application of AML controls by or through Intermediary PSPs on end users of the virtual IBAN.

## Cryptoasset services

5.75 As of March 2025, there were five EMI and Payments firms registered with the FCA to provide cryptoasset services either itself or through a related-group company. However, since 2020 there has been a significant increase in the number of firms with e-money agents who are principally cryptoasset firms. In addition, an increasing number of EMI and Payments firms and their agents, are servicing customers who are directly or indirectly involved with cryptoasset services. Many of these cryptoasset service-providing customers will be based outside the UK, and some in jurisdictions of risk which do not have the same high regulatory standards as the UK. There is a high money laundering and terrorist financing risk associated with this, where the UK-incorporated EMI and Payments firms may provide the 'on ramps' and 'off ramps' (the exchange of fiat currencies for cryptoassets and vice versa), for a cryptoasset service provider.

### **Box 5.D - Case study: use of vIBANs**

HMRC has several civil and criminal investigations into an OCG who operated an alternative banking platform (ABP) to engage in money laundering predicated by cheating the revenue using a mini umbrella company (MUC) fraud, which is a type of organised labour fraud. The ABP was as an unregulated Electronic Money Distributor incorporated in a high risk jurisdiction. The ABP enabled MUC fraud in the UK by providing virtual bank accounts (vIBANs) to about 60,000 companies, (mainly MUCs) through a partnership with a UK authorised EMI. No customer due diligence was conducted when the customers were onboarded. The ABP operated for around seven years, and within the last year of operation about £2.5 billion was being laundered per annum with more than £500 million of this being estimated revenue loss. At the time of the demise of the platform there were around 35,000 live vIBANs of which over 14,000 were known to HMRC as entities of concern. The OCG deceived the EMI and their three UK safeguarding banks using vIBANs to engage in money laundering, which also occurred through the loading of pre-paid cards with funds originating from criminal activity. The EMD and EMI ceased trading in the UK. More than 20,000 MUCs deregistered by HMRC, tax assessments issued and more than £40 million was frozen in bank accounts. The case is ongoing.

## **Terrorist Financing risk**

5.76 The terrorist financing risk of EMIs and PSPs has increased from **medium to high**. The risk rating has been informed by a range of factors including those set out in the money laundering section, the cross-border nature of EMIs and PSPs, and the growth in firms exposed to high risk jurisdictions.

## Vulnerabilities

5.77 Many of the vulnerabilities that expose the sector to money laundering risk, also apply to the sector's attractiveness to terrorist actors. In particular, there is

an inherent vulnerability in the ubiquity and accessibility of EMIs and PSPs' products and services that make them attractive to legitimate users and supports the sector's growing popularity, but they also make it susceptible to terrorist financing. EMIs and PSPs also provide greater financial inclusion for the underbanked, but with this comes exposure to risk. The willingness of some EMIs and PSPs to provide bank-like services to high risk customers, and the vulnerabilities in some firms' systems and controls, have made the sector a target for terrorist actors. As with retail banks, regulated EMIs and PSPs can become exposed to illicit actors through partnerships or customer relationships with unregulated or less-regulated EMIs and PSPs.

### Strength of Mitigations

5.78 Since 2020, a small number of EMIs and PSPs have joined the Joint Money Laundering Intelligence Taskforce's "Terrorist Financing Public-Private Threat Group". This provides a forum to both share and receive information to help support and develop an understanding of terrorist finance risks. More EMIs and PSPs are due to join the Group in 2025 and shows a positive step from the sector in both its understanding and compliance of the AML/CTF regulations, and the obligations this places on the sector. However, while some firms have matured their systems and controls since 2020, the sector has increased in size in terms of its transaction value. Any weak links present in firms' systems and controls will provide bad actors with opportunities to use these for terrorist financing purposes. The FCA has prioritised tackling financial crime in the sector, including making prevention a supervisory priority and recruiting more specialist staff. In response, the FCA has seen some firms significantly improve their systems and controls, but there is more for firms to do.

## Cryptoasset Service Providers

| Cryptoasset exchange providers and custodian wallet providers | NRA 2017 | NRA 2020 | NRA 2025 |
|---|----------|----------|----------|
| Money Laundering  | Low      | Medium   | High     |
| Terrorist Financing   | Low      | Medium   | Medium   |

### Introduction

5.79 Since January 2020, cryptoasset exchange providers and custodian wallet providers (CASPs), as defined in the MLRs, have needed to register with the FCA for MLRs supervision. Registered firms facilitate their customers' exchange and transfer of various types of cryptoassets, by providing services such as exchanging cryptoassets for other cryptoassets or money and vice versa. They can also provide services for the safeguarding and/or administration of cryptoassets or private cryptographic keys on behalf of customers. This chapter sets out the risks of firms required to register under the MLRs. Broader [cryptocurrency risks are covered in the 'typologies' chapter](#) of the NRA.

5.80 The UK remains Central, Northern and Western Europe's largest cryptoasset economy, receiving \$217 billion (around £169.9 billion) in on-chain value in virtual assets, and ranking 12<sup>th</sup> (of 151 countries) in one blockchain analytics firm's global cryptoasset adoption index. The consumer base for cryptoassets has grown since 2020 with 2024 FCA research finding that 12% (extrapolated to around 7 million) of UK adults owned cryptoassets, compared to 4.4% (2.2 million) they calculated in 2021.

5.81 The number of FCA registered cryptoasset firms has increased from four at the end of 2020, to 48 as of April 2025. 368 applications for registration were submitted, 86% of firms who applied for registration did not meet the standard for registration, meaning that only a small amount of cryptoasset firms that applied for registration met the UK's AML standard. Since 2020, the nature of businesses offering cryptoasset services has also evolved, with some mainstream financial providers now offering cryptoasset services. As of April 2025, the [FCA listed](#) 32 UK businesses that appear to be carrying on cryptoasset activity without the requisite registration with the FCA. However, this is not a complete list of all entities engaging in unregistered or illicit cryptoasset activities in the UK, so the true number may be higher.

### Money Laundering Risk

5.82 The risk of money laundering through cryptoassets has increased since 2020 and is now assessed to be **high**. This score is driven by the increase criminal use of cryptoassets accompanying an increase in their licit use by the

general public, alongside the speed with which money can be moved. Despite an increase in mitigatory activity across law enforcement agencies, supervisors and firms, a growth in exposure to high risk jurisdictions, higher volumes moved and a general increase in illicit usage have increased the risk. This risk assessment also reflects an improved intelligence picture and understanding about how criminals launder illicit finance with cryptoassets relative to 2020.

## Vulnerabilities

5.83 Cryptoasset service providers have a high level of risk exposure due to the volume and value of activities they conduct in the ecosystem, the speed of transactions, their intermediary role within the global cryptoasset sector, as well as their connection with the traditional financial system. Criminals have made use of these services to convert fiat currency to cryptoassets and vice versa and they are a key means of extracting tangible assets from proceeds of crime laundered via cryptoassets (often referred to as an 'off-ramp' from crypto to fiat). According to private blockchain analytics firms, significant amounts of identifiable laundered funds end up at a small number of centralised exchanges.

5.84 Similar to traditional finance, a commonly used method of laundering cryptoassets is the use of money mules and mule accounts; laundering networks make use of numerous third-party accounts (either paid for, fraudulently accessed or stolen) to convert and move relatively small volumes (typically less than £10,000) of criminal funds at a time. In addition, cryptoasset firms report that even with customer due diligence measures and effective cryptoasset tracing technology, it can sometimes be difficult to identify the ultimate source of some funds because of the transnational nature of cryptoassets.

5.85 Unregistered exchanges and/or those outside of the FCA perimeter who are instead registered in jurisdictions with more limited oversight represent the greatest threat in terms of cryptoasset money laundering. They often have less stringent identity checks and, as such, appeal to those looking to launder and move cryptoassets. Where there is limited UK nexus to this threat activity, powers for UK authorities including the FCA to directly intervene can be limited.

## Scale

5.86 Intelligence indicates the scale of cryptoassets being used for money laundering has increased since 2020. This is based on an increase in the estimated amount of illicit crypto transactions linked to the UK, and an increase in crypto appearing in money laundering intelligence. This assessment may in part be due to greater focus and visibility by regulators

and law enforcement agencies since the MLRs came into force for relevant cryptoasset firms in 2020.

5.87 The scale of money laundering from cryptoassets is difficult to measure. The NCA estimate that \$1.7-5.1 billion in illicit cryptoassets transactions are linked to the UK annually (through regulated and unregulated businesses). [Chainalysis](#) found that \$22.2 billion was sent from illicit addresses globally in 2023 – this figure is a lower bound estimate of the total amount laundered as it is only based on illicit addresses that have already been identified by Chainalysis.

5.88 Cryptoassets have been increasingly seen in money laundering intelligence over the last five to six years. Alongside large increases in intelligence reporting by the regulated financial sector on potential illicit use of crypto, mentions of cryptoassets in NCA intelligence have increased. This ranges from smaller street level cases involving drugs or fraud up to large scale laundering involving transnational crime groups and international controller networks. Some of this growth can be accounted for by the increase in reporting requirements for newly regulated businesses and growing consumer interest in cryptoassets. However, the overall growth in legitimate transactions involving cryptoassets makes it almost certain that their use in money laundering has also grown.

5.89 As the use of cryptoassets continues to grow, the corresponding illicit use has also increased. As we introduce a more comprehensive regulatory framework on a wider range of cryptoasset activities, covering issues ranging from governance and conduct to operational resilience rules, we envisage that the increased robust regulation should help with mitigating the risks of illicit use of cryptoassets, thereby reducing the residual money laundering risks.

#### Strength of Mitigations

5.90 The FCA's capacity to address money laundering and terrorist financing risks has been supported by an increase in available resources and its capability to address money laundering and terrorist financing risks has also increased from 2020. This is reflected in relevant mitigating activity taken, including targeted interventions to stop unregulated crypto ATMs. The number registered cryptoasset firms has increased from four at the end of 2020 to 48 as of 10 April 2025. The FCA maintains a robust gateway and supervises registered firms to ensure they remain compliant with the MLRs.

5.91 The FCA has seen improvements in some firms' conduct following FCA engagement. The FCA has also taken intervention action to impose business restrictions on cryptoasset businesses, required a skilled person review on economic crime systems and controls issues, issued feedback letters, and referrals for enforcement action where appropriate.

#### **Box 5.E – Case Study: Crypto ATMs**

In 2023, the FCA visited 38 locations across the UK suspected of hosting crypto ATMs. This resulted in the FCA disrupting 30 machines operating unlawfully across the country. In September 2024, an individual was charged for unlawfully running multiple crypto ATMs without FCA registration. In February 2025 (after pleading guilty), the relevant individual was sentenced to four years in prison for illegal crypto activity worth over £2.5 million and associated offences. The number of crypto ATMs advertised on CoinATMRadar in the UK has fallen from more than 80 in 2022 to nil in 2024. Where suspecting criminality, law enforcement and supervisors continue to work together to take appropriate action.

5.92 In September 2023, the UK also introduced the 'travel rule' to the MLRs to further mitigate financial crime risks, as per FATF requirements. This means that cryptoasset businesses in the UK are required to collect, verify and share information about the sender and receiver of cryptoasset transfers. In October 2023 financial promotions rules were introduced to address concerns with misleading advertising and a lack of suitable information in cryptoasset markets. The FCA issues alerts about unregistered firms and firms illegally promoting cryptoassets, issuing over 1,700 in the first year of the regime. Crypto ATMs offering cryptoasset exchange services in the UK must be registered with the FCA and comply with the MLRs. No crypto ATMs have been approved to operate in the UK, and the FCA has taken a robust approach to countering the threat posed by crypto ATMs operating unlawfully.

5.93 In April 2024, the Proceeds of Crime Act 2002 (POCA) was amended to ensure that law enforcement agencies have the right legislative framework in place to recover criminals' cryptoassets. These amendments enable law enforcement agencies to investigate, seize, and recover the proceeds of crime within the cryptoasset ecosystem more effectively.

5.94 Directed by the Economic Crime Plan 2 (and supported by Economic Crime (AML) Levy funding) law enforcement agencies have invested in improving both their capacity and capability in relation to the investigation of the criminal use of cryptoassets. The impact of these initiatives is reflected in successful operations such as the recent Operation Destabilise. Funding has been used by law enforcement to gain access to specialist crypto services such as blockchain analysis and storage solutions. Law enforcement agencies

have also responded to the growth in crypto-enabled crime by employing specialist officers and embedding them in investigative teams.

5.95 However, challenges remain. The process of investigating criminal use of cryptoassets is made more complicated by the constantly shifting and developing nature of the crypto environment and the significantly increased size of the market. The seizure of cryptoassets by law enforcement agencies is also complicated by the need to isolate and access seized funds, often from CASPs based outside of the UK's jurisdiction<sup>[4]</sup>.

#### Forward look

5.96 HM Treasury and the FCA intend to bring certain cryptoasset activities within the regulatory framework of FSMA. This will ensure that appropriate systems and controls, including governance and conduct-related requirements apply to in scope firms to better protect consumers.

5.97 The new activities being brought into the FSMA regime include issuing stablecoins in the United Kingdom, dealing in cryptoassets as a principal or agent, arranging deals in cryptoassets and some staking services (i.e. firms offering services to their customers in connection with earning rewards from the validation of transactions on a blockchain network). These activities are increasingly popular among consumers, and potentially to criminals. Introducing these activities into the FSMA framework also seeks to reduce the ML risk, as the firms become subject to various requirements in the FCA Handbook, complementing the obligations already supervised under the MLRs. This regime will be in line with the proposals published by HM Treasury in October 2023, with the exception that stablecoins will not be brought into regulated payments.

#### **Terrorist financing risk**

5.98 The risk of registered cryptoasset firms being used to finance terrorism has grown but remains **medium**. This rating has been based on a range of factors including the ability to send both large and small sums rapidly and frequently across borders using cryptoassets. Changes to terrorist financing vulnerabilities and mitigations largely mirror those applicable for the money laundering risk, but there is a smaller notable increase in the scale of cryptoasset use which explains why the risk remains medium for terrorist financing. As the use of, and access to, cryptoassets increases for legitimate purposes, so does the range of cryptoassets and supporting services available. The fast evolution of cryptoassets means new sector risks emerge, often faster than the pace of global regulations.

## Vulnerabilities

5.99 The same characteristics of the registered cryptoasset firms that are driving their use by legitimate users also expose the sector to terrorist financing. As in all other financial services, the products and services offered by cryptoasset firms heavily rely on remote onboarding, especially non-face-to-face customer identification / verification and updating of information. Additionally, [anonymity-enhancing technology](#), such as mixers, tumblers, and privacy wallets, continues to evolve and allow users to hide transactions and the cryptoassets' end destination. These anonymity-enhancing techniques make it more difficult for law enforcement agencies to track and trace illicit funds in a timely manner. Decentralised finance is another type of cryptoasset service that is vulnerable to terrorist financing. The absence of traditional financial intermediaries, the high degree of automaton of the transfers, and the highly fragmented nature of the services all amplify the vulnerabilities for terrorist finance. More importantly, as the smart contract code underpinning the majority of the DeFi protocols is available and visible in the public domain, while these inherent technical features make DeFi vulnerable to hacking by nefarious actors, including terrorists, in raising funds, there are opportunities for law enforcement agencies through the transparent and public nature of the blockchain.

5.100 There are other vulnerabilities that are potentially exploitable for terrorist financing. While these vulnerabilities are partially mitigated by the sector, supervisors, and law enforcement agencies, they all contribute to the overall risk rating. For example, the limit set by CASPs on the total value of virtual assets that can be purchased, moved, or traded in a set period is typically high (e.g. \$25,000 daily limit). Generally, there are rarely limits on the number of transactions an individual can make per day. Both these characteristics are attractive to terrorists looking to move a large amount of funds.

5.101 Similarly, there has been an increase in the use of privacy enhancing techniques, through both privacy coins and mixers. Privacy coins can facilitate a more sophisticated and complicated layering process, making it harder (though not impossible) for both cryptoasset firms and law enforcement agencies to identify suspicious activity in the first instance, and then identify the right evidence for terrorist financing investigations. The borderless nature of cryptoassets, means they can be sent to, or received from, overseas jurisdictions, including those with high terrorist financing risks or jurisdictions that have not introduced any regulatory framework for cryptoassets (including travel rule requirements). While some overseas cryptoasset firms will decline clients who are high risk or on sanctions lists, the range in quality of CDD processes in overseas exchanges means that cryptoasset firms may not necessarily have formed a complete view or understanding of which specific clients or transfers facilitate terrorist financing. Some cryptoasset firms may

inadvertently or intentionally have fewer restrictions in place and be targeted by illicit actors either based overseas or looking to move funds overseas.

5.102 The relatively new state of the cryptoasset sector has resulted in differing regulatory standards across the globe, as countries implement the FATF, IOSCO and FSB standards at a different pace or in different ways. Like in many financial sectors, the UK's regulations for the cryptoasset sector are robust, but many countries have lower, or no regulatory requirements for cryptoasset firms. For example, centralised exchanges where countries may not have implemented appropriate regulations, but which have higher flows, volumes and values than decentralised exchanges. Overseas decentralised exchanges are, however, less regulated (no central answerable authority to impose regulations) and can conceal the origin and destination of funds to facilitate trades without reliance on a traditional intermediary or a custodian, those with which law enforcement agencies can usually direct requests to. This can also act as a catalyst for the vulnerability caused by the cross-border nature of the sector.

#### Scale

5.103 The prevalence of cryptoassets in terrorist financing cases has also grown. For example, Hisham Chaudhary sent cryptoassets to a terrorist organisation. In 2021, Chaudhary was convicted of seven terrorism offences, including two for terrorist financing and was jailed for 12 years. He converted around £55,000 from various sources, including his salary, into Bitcoin to send to contacts in Türkiye to extract Islamic State supporters from internally displaced people camps in Syria. The use of legitimate sources of funds (salary payments) to purchase the cryptoassets, is a common source of terrorist financing, as is the ability to transfer the cryptoassets overseas for terrorist use, highlighting two inherent vulnerabilities of the cryptoasset sector.

#### Strength of Mitigations

5.104 The government has responded to the growing prevalence of cryptoassets and the terrorist financing risk that brings. Since the last NRA, the Economic Crime and Corporate Transparency Act (ECCTA) 2023 has come into force on 26 April 2024. This Act amended Schedule 1 of the Anti-terrorism, Crime and Security Act 2001, which provides law enforcement agencies with the powers to seize and detain cryptoassets and cryptoasset-related items; apply to freeze crypto wallets held with a cryptoasset service provider or custodian wallet provider; and, ultimately, to forfeit cryptoassets related to terrorism. Since the ECCTA came into effect, law enforcement agencies have already detained around £28,146 terrorist cryptoassets.

5.105 The "Public-Private Crypto Forum" provides cryptoasset firms, alongside law enforcement agencies, HMG and supervisors, a means to share knowledge and gain a better understanding of cryptoassets existing and emerging

terrorist finance risks. In a positive step, the sector has slightly increased its capacity and capability to manage its terrorist financing risks. For example, some cryptoasset firms exposed to other asset flows use a unique tool to analyse blockchain activity to identify the source of cryptoassets and any associations with illicit activity.

5.106 The FCA's capacity and capability to manage the terrorist financing risks in the cryptoasset sector has maintained a high level. Law enforcement play a pivotal role in terrorist financing investigations. However, since 2020, law enforcement agencies' capacity and capability to manage the terrorist financing risk from the cryptoasset firm sector have both decreased. This is due to staff resourcing and retention issues in the police service, the lack of cryptoasset training for non-specialists and the technology available to law enforcement in order to keep up with changing technologies and methodologies.

## Forward look

5.107 The top three emerging terrorist financing risks for the cryptoasset sector are:

- **Crypto hacking:** This has already been seen in the cryptoasset industry in 2024 by illicit and state threat actors. These hacks exploit vulnerabilities or loopholes in the system to steal cryptoassets.
- **Crowdfunding donation-based platforms:** Digitally enabled donation-based crowdfunding through dedicated online platforms and social media, is increasingly being exploited for terrorist financing purposes. The FATF [have highlighted](#) that the crowdfunding donation-based industry has started to incorporate funding options tied to virtual assets, and that countries should closely monitor whether and how terrorists adopt virtual assets for crowdfunding donation-based campaigns.
- **Utilisation of privacy protocols:** There could be sanctions risks when mixers and other privacy-enhancing services are used, and compliance teams within cryptoasset firms need to be alert to transactions involving sanctioned services or unusual or unexpected volume transactions involving masking services that bad actors might attempt to use. This could be crystalised further with the implementation of further advanced privacy technology that coins like Monero are seeking to implement.

## Money Service Businesses

| Money Services Businesses | NRA 2017 | NRA 2020 | NRA 2025 |
|---------------------------|----------|----------|----------|
| Money Laundering          | High     | High     | High     |
| Terrorist Financing       | High     | High     | High     |

### Introduction

5.108 Money Service Businesses ([MSBs](#)) provide services for currency exchange services, money transmission and cheque cashing. The sector is diverse and largely retail facing, with providers ranging from local convenience stores to large multinational and UK-wide businesses. Most operated under a principal-agent model, where a corporate centre, the 'principal' enters into relationships with one or more 'agents' who are authorised to act on behalf of the principal. The majority of agents are based on the high street.

5.109 MSBs play an important role in providing financial services to those communities and people who are unable to or choose [not to access mainstream services](#). Remittance services are popular with diaspora communities as a cheaper and accessible alternative to traditional banks, foreign tourists often use MSBs for currency exchange, and those on a low income use MSBs for cheque cashing. Whilst the vast majority of MSBs are supervised by HMRC, those that provide money transmission are also required to register with the FCA under the Payment Services Regulations. The Gambling Commission supervises casinos for any MSB activity they offer under the MLRs 2017.

5.110 At the end of 2023/24, 983 MSB principals were registered with HMRC and operated out of 29,845 premises either as branches or agents. In the same period, the agent population stood at 28,862 with these agents being overseen by their principals. The sector has and continues to reduce in size, as principals, agents and premises have all fallen significantly (51%) between 2017 and December 2024. This fall is assessed as potentially being due to both commercial factors and a heightened compliance approach by HMRC.

### Money Laundering Risk

5.111 The money laundering risks associated with MSBs have not changed since the 2020 NRA and the overall risk within the sector remains **high**. However, MSBs should be viewed in the context of a wide range of money laundering typologies and a constantly evolving threat picture.

### Vulnerabilities

5.112 [Cash](#) remains widely used by criminals who continue to exploit features of the MSB sector to move or convert criminal funds. The global reach of money remitters, including to high risk jurisdictions, the ease of making cash transactions, including the anonymous nature of the origins of cash, the one-

off nature of many transactions and the speed of transactions are key features that make the sector particularly attractive to criminals.

5.113 Consistent with the 2020 NRA, the money laundering risk remains high where MSBs offer certain services such as money remittance and currency exchange. These services allow money to be moved quickly and cheaply to foreign jurisdictions. This can involve converting cash into small volumes of higher denomination notes in various currencies, which can be more easily moved across borders and banked in or outside of the UK, or being placed with a money transmitter who can make the equivalent value appear and paid to a recipient anywhere in the world, including the transmission of 'monetary value' by [Informal Values Transfer Systems](#) (IVTS).

5.114 In addition, those MSBs that offer forex services also remain high risk. This is due to the vast amount of money that can be transferred by forex MSBs in a single transaction via banks, the fees for which are often cheaper than those incurred by retail banks. In 2023/24, HMRC seized large amounts of unreconciled cash from registered MSBs highlighting the risk of cash based money laundering within the sector.

#### Strength of mitigations

5.115 Following the last NRA, HMRC has led a step change in its approach to mitigating against the high risk present in the MSB sector. This included establishing a specialist MSB compliance team and hosting a cross-government MSB intelligence taskforce. This MSB Taskforce has increased the flow of intelligence and led to increased penalties and sanctions.

5.116 Compliance levels vary across the sector; however, the highest risk of non-compliance sits with the small and medium enterprises with less than five premises, who make up 15% of the sector.<sup>4</sup> These MSBs make losses or very minimal profits, which increases the risk firms seek to cut compliance costs or rely on off the shelf compliance products. Some agents may also be susceptible to exploitation by criminals to provide them with supplementary income.

5.117 The largest MSB principals invest significantly in their compliance. However, given the large and fluid agent networks they operate, there is an increased risk of inappropriate agents not being identified. There is limited information sharing between MSBs, which means an agent removed by one principal is free to move to another.

#### Unregistered Activity

5.118 Remittance MSBs, including those operating as IVTS are required to register with both HMRC and the FCA as money remitters. However, not all businesses are registered, either out of choice or ignorance of the requirements to do so. Some unregistered MSBs have been found to use personal accounts to transfer value. The true scale of the number of unregistered MSBs is not known, but HMRC has a long running project monitoring un-registered activity.

5.119 This risk is further exacerbated by the low risk appetite amongst the traditional financial sector to provide banking services for MSBs. Many MSBs have moved into complex relationships with other MSBs including with intermediary EMI and PSPs. This business model enables audit trails to be disguised and can provide plausible deniability about the integration of suspected proceeds of crime for businesses when confronted, which makes it challenging for supervisory and law enforcement agency investigations.

#### Exporting of physical cash

5.120 The exporting of physical cash can be an effective way of moving bulk amounts of cash – in specific currencies – to certain jurisdictions. However, given the volume and value of cash exports, it can also be exploited to move the proceeds of crime, by disguising audit trails and allowing for the co-mingling of legitimate and illegitimately derived cash. HMRC is continuing to work to understand why some MSBs are exporting significant volumes of GBP sterling to jurisdictions where there is no obvious economic or market requirement, including through collaborative dialogue with other MSB supervisors in the jurisdictions in receipt of the cash.

### **Terrorist Financing Risks**

5.121 The terrorist financing risk associated with MSBs remains **high**. As highlighted in the 2020 NRA, the low cost of transferring funds and the ability to reach a range of high risk jurisdictions continue to render MSBs an attractive and accessible method for terrorists to move small amounts of funds quickly into and out of the UK.

#### Vulnerabilities

5.122 MSBs are cash-intensive and have significant exposure to high risk services. The small amounts that are typically transacted are unlikely to be deemed suspicious by MSBs, and funds can be sent via third countries to reduce suspicion further. This is particularly relevant for terrorist financing, where the amounts involved are typically low and come from legitimate sources. An example of this is the July 7, 2005, London bombings, where reports stated that the groups involved were self-financed. Knowledge and experience gaps on terrorist financing across MSBs and individual agents are also a contributing risk factor for the sector – given the large number of MSBs, it is likely that these gaps could be exploited by terrorist actors.

5.123 As with the money laundering risk the principal agent business model of MSBs, increases the risk of terrorist financing in the sector. Many MSBs are high street based, and the lack of formal business relationships with customers accessing currency exchange services presents challenges to detecting unusual suspicious transactions or patterns. Similarly, by using a complicated chain of MSBs and other payment service providers, criminally complicit MSBs can distance themselves from suspicious transactions, confuse audit trails and provide plausible deniability.

## Strength of mitigations

5.124 As outlined above, overall compliance by the small and medium sized firms in the sector continues to be poor, especially in relation to remittances to high risk jurisdictions. Following a HMRC small and mid-sized businesses campaign, warning letters were issued to nearly half of the businesses visited. Since the 2020 NRA, HMRC have issued sanctions for poor compliance to MSBs remitting to other high terrorist financing risk countries without sufficient controls. HMRC issued a £1 million penalty in July 2024 to a business remitting to a high terrorist financing risk jurisdiction, alongside other sanctions in other cases.

5.125 Onboarding and monitoring of agents also continues to be an issue for the sector. As outlined above, whilst HMRC has made positive changes to its risk mitigations since 2020, challenges remain regarding oversight of the agent population, low levels of terrorist financing SAR reporting, owing to poor risk understanding, and terrorist exploitation of the CDD threshold. Data and intelligence sharing between MSBs remains an issue that hinders the sector's ability to identify and address terrorist finance risks.

### **Box 5.F - Case study: Unregistered MSB**

An MSB was trading for a year and a half without being registered under the MLRs for supervision. During this period, the MSB transmitted funds to the value of £543,680, using Informal Value Transfer Systems. Such transactions occurred without oversight or compliance checks by a supervisory authority, thereby undermining efforts to prevent, detect and combat ML/TF and creating opportunity for illicit remittances to occur undetected.

At the time of the criminal investigation, the defendant was listed as the sole director of two companies.

The defendant pleaded guilty to running an unregistered MSB, contrary to the MLRs, and received a 12 month custodial sentence (suspended for 18 months), 150 hours unpaid work, was ordered to pay £1,000 in costs and received a five year directorship disqualification.

## High Value Dealers

| High Value Dealers  | NRA 2017 | NRA 2020 | NRA 2025 |
|---------------------|----------|----------|----------|
| Money Laundering    | Low      | Medium   | Medium   |
| Terrorist Financing | Low      | Low      | Low      |

### Introduction

5.126 High value dealers (HVDs) are firms or sole traders who make or receive payments of over €10,000 in cash for the purchase of goods. In the year ending March 2024, 257 HVDs were registered with HMRC, a significant decline from 448 firms registered in the year ending March 2020. This decline is likely due to a reduction in the number of firms accepting cash payments, either entirely or above a certain value. HMRC categorises HVDs under 12 sub-sectors with the highest risk areas for criminal abuse assessed as being jewellery, motor vehicles and cash and carry/alcohol. This chapter should be read alongside the cash and [trade based money laundering](#) and [IVTS](#) chapters.

### Money Laundering Risk

5.127 High value goods are appealing to criminals partly due to their versatility. Goods purchased with criminal cash can be re-sold, either for profit or loss in exchange for clean funds. They can also be kept as a store of value, or, depending on the goods in question used as status symbols. High value payments for multiple lower value goods can also be used to launder criminal funds. In [tax evasion](#), the use of undeclared cash income to buy undeclared stock for sale in the business (with sales under or not declared) is a long-established technique.

5.128 The risk is heightened in cases where remote cash payments are involved, either through couriers stated to be delivering cash for clients or depositing cash directly into the bank account of the HVD. High value goods, such as watches, precious stones and jewellery can also be moved across international borders via passenger routes without attracting the same attention as large cash movements. UK law enforcement agencies continue to seize [listed assets](#) (which includes precious stones and watches) both at the border and in wider policing operations, some of which are likely to have been purchased with cash.

### Scale

5.129 In the financial year 2023/24 £7 million worth of listed assets were seized in England, Wales and Northern Ireland. Bulk goods, including gold, scrap metal and vehicles may also be used to facilitate trade based money laundering and may be purchased with cash. Given the range of goods that can be used to facilitate ML the risk is naturally heightened in firms who either rarely transact

in cash or are unaware of the requirements of the MLRs. In both cases a firm is unlikely to know what checks need to be carried out or the characteristics of an unusual or suspicious transaction.

### Strength of mitigations

5.130 As the sector's supervisor, HMRC run a pre-registration process for firms seeking to make and receive cash payments above the threshold, with approximately 25% of applicants being successful and the remainder refused permission. Since 2020, HMRC has led several HVD campaigns, resulting in numerous warning letters and penalties. The majority of MLR compliance issues arise out of inadvertent non-compliance where a firm did not understand their responsibilities and risks, although this can be difficult to distinguish from wilful non-compliance.

### **Terrorist Financing risk**

5.131 The risk of the high value dealer sector being used to finance terrorism remains **low**. For the customer to be able to purchase items above the HVDs threshold, requires high levels of liquidity, which will sometimes involve providing a sum upfront to 'hold' the items. Nevertheless, the sector provides opportunities to obtain small objects of high value, which can be moved across borders without the need for individual export licences and might not be checked by customs officials. Since 2020, there have been no cases of HVDs being used to move or store terrorist funds through the sales and purchases of luxury goods.

### **Activities not regulated under the MLRs**

5.132 The retail sector is increasingly shifting away from cash transactions, embracing electronic payment methods such as smartphone-based payments and gift cards. This transition has the potential to alter the regulatory landscape, as the UK's MLRs primarily focus on cash transactions. The economic scale of the HVD sector is significant, encompassing industries such as luxury retail and high-end automotive sales. As electronic payments become more prevalent in HVDs, there is greater intersection with regulated sectors, including payments.

5.133 This increases opportunities to prevent economic crime but also brings challenges and presents several money laundering vulnerabilities. The reduced use of cash to purchase high value goods does not necessarily reduce the risk of illicit financial activity; rather, it changes its nature. Electronic payments, particularly those made through smartphone apps registered outside domestic regulatory jurisdictions, can obscure transaction trails and complicate enforcement efforts. Similarly, gift cards purchased with cash and resold through unofficial channels create an alternative method for money laundering, allowing individuals to make anonymous purchases without

triggering traditional AML safeguards. Under the UK's MLRs these methods do not meet the definition of cash payments. Without regulatory adaptation, such loopholes could be exploited to integrate illicit funds into the legitimate economy.

5.134 The scale of money laundering activity involving high value goods remains difficult to quantify, but there are indications that electronic payment methods are being used for this purpose with increasing frequency. The complexity of tracking such transactions makes it challenging to estimate the full extent of illicit financial flows.

## Art Market Participants

| Art Market Participants | NRA 2017 | NRA 2020 | NRA 2025 |
|-------------------------|----------|----------|----------|
| Money Laundering        | N/A      | High     | Medium   |
| Terrorist Financing     | N/A      | Low      | Low      |

### Introduction

5.135 Art market participants (AMPs) include any firm or individual who trades in or acts as an intermediary in the sale or purchase of works of art over €10,000 or is involved in the storage of art worth over €10,000 in a freeport. As of March 2025, 1,337 art market participants were registered with HMRC, rising significantly from the 208 registered in 2020. These were principally made up of galleries, auction houses, private dealers and intermediaries. This is a result of the deadline for AMP registration with HMRC being in June 2021, rather than a fundamental change in the size of the sector.

5.136 According to the 2025 [Art Basel report](#), the UK has the second largest art market in the world (after the US) and remains the largest in Europe. The UK art market attracts diverse artists and collectors and sees a large annual flow of funds both in to and out of the UK.

### Money Laundering Risk

5.137 The risk rating for money laundering in the sector has decreased from **high** to **medium** since the last NRA. The sector was added to the MLRs in 2020 and first scored as part of the 2020 NRA; as such it was a newly regulated sector which had not previously needed to have a full range of ML and TF measures in place. HMRC's improved understanding of the risk in the sector, and therefore our ability to respond to it has driven the decrease in the score. However, there remains a risk of the sector being used for money laundering.

#### Vulnerabilities

5.138 The high volume of funds moveable in a single transaction, the ability of artworks to appreciate in value over time, alongside the enjoyment or status gained by owners makes art appealing to both legitimate and criminal investors. It can be more easily stored and transported than other assets of commensurate value, such as real estate. The art market is diverse; whilst some firms mostly buy or sell to longstanding clients they know well, some operators frequently buy or sell in private or through intermediaries, decreasing visibility of the true buyer or seller of the artwork. Whilst there are legitimate reasons for operating in such a way, this trading environment is advantageous to those seeking to launder money and hide their true identity. Even where firms have long standing relationships with clients, they should

monitor changes of circumstance or behaviour. Any transactions carried out using [cryptoassets](#) is potentially higher risk due to the ease in obscuring the source and ownership of funds. Art market participants do not normally handle cash for sales over the registration threshold.

5.139 The value of art can vary significantly, making it attractive to varying levels of criminality and a useful mechanism to store value over a period of time. Price fluctuations in the value of art allow both for profits to be made by sale of the art and to conceal the movement of value where the price of artwork is manipulated by criminals. Over or under valuing artwork in order to transfer value is similar to some [trade-based money laundering](#) schemes. Whilst expert teams, such as those working in anti-corruption, are likely to recognise the use of art in money laundering it is also likely to be less suspicious to law enforcement agencies, as opposed to gold or cash, with which they are more familiar.

5.140 Reputation plays an important role in the art market, and the risk of negative publicity is an incentive for firms to avoid engaging with identifiable criminals or illicit activity and ensure appropriate procedures are in place. However, active complicity is not necessary for a firm to be abused by criminals and the Metropolitan Police's Arts and Antiquities Unit continues to see evidence of criminal activity in the sector; ongoing and effective compliance with MLR requirements is therefore an important preventative measure to mitigate the risk.

#### Strength of mitigations

5.141 Art market participants have been included in scope of the MLRs since 2020. Whilst progress has been made towards these requirements, significant compliance challenges remain across much of the AMP population. Since June 2021, HMRC has taken regulatory action against over 90 AMPs, due to trading while unregistered as an AMP with penalties totalling over £535,000 issued in response. Initial compliance activity was focused on intelligence received by HMRC and around galleries and auction houses where risk was deemed to be higher. Common compliance issues identified included insufficient risk assessments and policies, controls and procedures. SAR reporting and registration with the UKFIU's SARs portal by the sector is low compared to the risk. Work is ongoing to raise awareness of the SARs process and the importance of registering with the portal and submitting SARs for both compliance and in building our collective understanding of the sector's risks.

5.142 There is established expertise in the Metropolitan Police Service's Arts and Antiques Unit, however, wider law enforcement has less awareness of the sector's risks that impacts our ability to assess the scale of ML and means of

addressing it. Work is ongoing to further improve understanding of risk in the sector.

### Cross-Border risks

5.143 The international nature of the art market is a significant part of both its success and its money laundering risk. Other leading markets in the world (the USA and China) do not have money laundering supervision for the art market raising the risk of criminal activity. Given the relative ease with which art can be used to move value across borders, firms should exercise the appropriate customer due diligence when dealing with potentially high risk individuals and individuals from high risk jurisdictions.

### Art Fairs

5.144 Art fairs are a key part of the UK art market. UK art fairs have global attendance which can create challenges where other jurisdictions do not exercise similar controls as the UK, such as obtaining information about the source and ownership of funds, particularly where anonymous and layered corporate structures are involved.

#### **Box 5.G - Case study: Bansky artwork**

In 2024, Mr Christopher Scrivens was convicted for drugs offences. He had laundered criminal money through another person's account with the judge stating that he had invested in expensive art in an effort to distance himself from his crimes. As part of the investigation Gwent police seized three pieces of Banksy artwork collectively valued at over £190,000.

### **Terrorist Financing Risk**

5.145 The terrorist financing risk of the art market participant sector remains **low**. As with the 2020 NRA, we continue to assess that the sector remains generally unattractive to terrorists. Buying and selling of artwork involves time consuming processes and requires high levels of liquidity. While the sector can facilitate the movement of large amounts of money in a single transaction, high-value purchases typically require knowledge of art and a trusting relationship within the sector. Moreover, a large collection of valuable artworks could warrant unwanted attention in a way that terrorists seek to avoid; whereas money launderers would want to either launder their illicit money quickly through the sector, or purchase artwork with a range of value that could appreciate over time.

### Vulnerabilities

5.146 Owning valuable works of art does not hold the same merit as a "status symbol" for terrorists as it does for other criminals. Terrorists would be more likely to use the sector as a mechanism to store funds in the artwork, while

generating further finance for use on, e.g. travel, cost-of-living expenses, operations. Firms may be unsighted on the full transactional chain, which may mask the source of funds of the purchaser. There is a risk that an individual or business could, including inadvertently, purchase artwork on behalf of a person who is a terrorism risk. This risk increases through the use of third-party intermediaries. Intermediaries are sometimes used to buy or sell on behalf of an unknown customer, which can both hide the source of wealth and the true beneficial owner of the item or artwork and could be of terrorism concern.

### Scale

5.147 The scale of abuse in the sector for terrorist financing purposes remains low. However, it is possible that the level of risk that the sector may be seeing may be underreported. Since 2020, there have been two linked cases of terrorist financing in the sector. Both cases have received substantial media coverage due to the extent of one individual's art collection, the other because of his UK TV presence. In April 2023, Nazem Ahmad was sanctioned and subject to an asset freeze in the UK due to suspected Hizballah financing. Despite Ahmad being sanctioned in the U.S. in 2019, he was able to conduct business with UK art galleries and auction houses to evade these prohibitions. In June 2025, Oghenochuko Ojiri, an art dealer and TV personality, was convicted of eight counts of failing to make a disclosure contrary to Section 21A of the Terrorism Act 2000, This was during the course of business within the AMP sector, between October 2020 and December 2021, where Ojiri sold artwork worth c. £140,000 to Nazem Ahmad. He was sentenced to two years and six months' imprisonment, with an extended 12 months on licence.

### Strength of mitigations

5.148 Consistent with assessment of AMP sector controls for money laundering, AMPs should be thorough and consistent in their CDD to mitigate the risk of terrorist actors exploiting the sector's vulnerabilities.

5.149 As the AMP sector's supervisor, HMRC's capacity and capability to manage the terrorist financing risks to the sector have been maintained since 2020. Law enforcement agencies have also maintained their capacity and capability to deal with the terrorist financing risks from the AMP sector. However, they have seen a reduction in resource available to work on this issue since 2020. The AMP sector is seen as a niche field, which requires specialist knowledge to investigate terrorist financing related cases.

### **Activity not regulated for AML/CTF purposes - Antiques, Antiquities, Digital Art and Jewellery**

5.150 The Antiques, Antiquities, Digital Art and Jewellery (AADJ) sectors involve the buying and selling of unique, historical and collectible items, that may be

of significance and value. The UK dominates the global trade of objects over 100 years old, ranking as the [world's top exporter](#).

5.151 Unless paid for in cash above the €10,000 threshold, the AADJ sectors are not currently in scope of the MLRs. The inherent similarities between the AADJ sectors and the AMP and HVD sectors make it likely that the ML/TF vulnerabilities in the AMP and HVD sectors are shared by the AADJ sectors. They are also vulnerable to actors storing and moving large sums of money in a single transaction, and using small, easily transportable objects to do so – this may even include cultural items scavenged from areas of conflict, which are transported across borders for sale. Digital art, which is completely transferrable online, removes the need for physical transportation, or insurance and customs costs. The [2023 FATF report on the Antique, Antiquities and Cultural Objects market](#) included discussion of vulnerabilities which are relevant to the UK, such as sales of smaller high value items which may be concealed into or out of the UK using criminal networks, laundering the proceeds through the sector, or sales of cultural objects, which have been [looted from countries](#) and sold on with documents that fake its provenance, and the funds used for terrorism.

5.152 As the AADJ sectors are unregulated, it's unclear how much ML/TF is occurring and likely that limited controls are in place to mitigate against these. As unregulated businesses sit outside of the MLRs, there is no obligation for dealers to submit suspicious activity reports under POCA or TACT to the NCA. Law enforcement agencies will, in turn, have limited visibility of suspicious ML/TF behaviour arising in these sectors, lacking opportunities to identify and investigate any ML/TF.

## Casinos

| Casinos             | NRA 2017 | NRA 2020 | NRA 2025 |
|---------------------|----------|----------|----------|
| Money Laundering    | Low      | Low      | Medium   |
| Terrorist Financing | Low      | Low      | Low      |

### Introduction

5.153 The Gambling Act 2005 defines casinos in legislation as an arrangement (whether on premises or via remote communication such as the internet) where people can participate in casino games. Non-remote casinos (NRC) and remote casinos (RC) are also permitted to offer non-casino games in accordance with the conditions of their operating licence issued by the Gambling Commission. The number of casino licensees has increased since the last assessment, from 210 in 2020 to 247 in 2024. Of these, 97 (39%) have been identified by the Gambling Commission as posing a higher risk. The volumes of funds moving through the sector has also increased. There has been a shift in consumer habits towards remote casino gambling since the 2020 assessment, in part due to the impact of the Covid-19 pandemic when all land-based casinos were closed.

### Money Laundering Risk

5.154 The money laundering risk in the casino sector has **increased** from **low** to **medium**. This is mainly driven by changes in customer, geographical and transaction risks, particularly the increase in funds moving through remote casinos (as above, some of which can be attributed to altered customer behaviour during the Covid-19 pandemic lockdown), new ways to play casino games, and the updated assessment of MSB activities offered by some casinos. From the data assessed, the most common occurrences of ML through licensed casinos are in the form of recreational spending of criminal property, however there are also instances of attempts by criminals to 'clean' funds through casinos.

5.155 There is also an increase in illegal casinos targeting the UK. Criminals could use illegal casinos to launder money, or they could be run by criminals and be used to launder their criminal funds. In addition, illegal gambling is a predicate offence and any funds associated with it could be criminal funds.

### Vulnerabilities

5.156 The casino sector continues to be exposed to financial flows from higher risk payment methods, including those linked to MSB facilities. Whilst the number of casinos offering MSB services since 2020 has declined, offering MSB services attracts higher risk customers using higher risk transactional methods, such as foreign currency exchange, third-party transfers and third-party cheque cashing facilities, including those from and to higher risk geographical locations. The use of money mules to gamble and money mule accounts established to transfer criminal funds into the [retail banking](#) system also remains a risk.

5.157 Casinos continue to attract both domestic and international customers. High-end non remote casinos continue to have a higher proportion of international PEPs, including those from higher risk jurisdictions. This increases the risk of exposure to funds generated from corruption.

5.158 The use of [white-label partnerships](#) by remote casinos also present ML vulnerabilities. This business model involves remote casinos entering into relationships with third parties for the purpose of promoting gambling activities (often relating to marketing agreements and sports sponsorship arrangements), and there have been cases where insufficient due diligence has been carried out on these third parties. Historically, some white-label arrangements included gambling operators relying on unlicensed third parties for elements of their compliance approach. In these cases, the licensee would remain responsible for compliance, although they did not always have sufficient oversight. These arrangements are now less common, but risks remain where white-label providers offer large numbers of websites, as failure by a single remote casino to control the ML risks relating to their white-label partnerships can impact a significant number of websites.

5.159 Permitting [peer-to-peer poker](#) through remote casino platforms also carries higher ML and TF risk as it can facilitate the exchange of criminal funds between customers. The use of VPNs also exposes remote casinos to increased risks, as they can be used to allow customers based in potentially higher-risk jurisdictions to appear based in the UK whilst masking their true location. Many remote casinos have controls in place to detect geographical risk factors, including VPN use by customers and links to high risk jurisdictions, so criminals may target those with less stringent controls, and the stringent rules within British gambling are thought to act as a deterrent. Other methods to achieve anonymity continue to grow, with an increase in the reported use of false identities in an attempt to gain access to casinos.

### Scale

5.160 Reported incidents of suspected predicate offences and illegal activity related to casinos, have increased since 2020. The total number of SARs reported by the sector has continued to rise year on year; particularly between 2022/23 (c.6000) and 2023/24 (c.7500) where it increased by 26%. This increase in reporting may be due to several factors, including: the industry improving resources to detect suspicion, improved reporting practices and training, and a greater understanding and subsequent reporting of SARs.

### Strength of Mitigations

5.161 Compliance levels for casinos have shown some improvement since 2020. In the 2023-24 reporting period, 25% of casinos assessed by the Gambling Commission were found to be non-compliant and 25% were found to be generally compliant (50% were found to be compliant).

5.162 With gaming and electronic machine activity in non-remote casinos, there remain potential gaps in relation to sufficient monitoring of customers in

cases where their transactions remain below the €2000 CDD threshold for transactions and a business relationship is not deemed to have started. However, the scale of this issue is mitigated to a degree by the statutory limits on stakes and prizes.

5.163 Compliance with CDD and EDD requirements declined between 2023 and 2024. Assessments in 2024 identified that 12.5% (compared to 7% in 2023) of casinos inspected were not compliant with all CDD requirements. 41% of casinos inspected (compared to 11% in 2023) were not applying EDD requirements on a risk-sensitive basis. Compliance in other areas has improved, with 100% of casinos assessed in 2024 found to have effective policies in place for cash (and cash equivalent) usage by customers (compared to 90% in 2023).

### **Anonymity**

5.164 Some high-end non-remote casinos customers use personal assistants and third-party employees when interacting with casinos, which may add an extra layer of complexity when verifying identity and source of funds or wealth as part of due diligence checks. Similarly, prepaid cards can be used to deposit criminal funds into casino accounts which are subsequently gambled and withdrawn to another, different payment method, potentially keeping the source of funds anonymous. Prepaid cards have been identified in the Gambling Commission supervisory assessment as higher risk, so firms are required to implement appropriate controls in response. Poker Stable contracts, where a collection of players are backed by an individual or a staking syndicate, may also create issues relating to anonymity, as the source of funds or the identity of those backing players may not be verified.

### **Money Service Business**

5.165 [MSB](#) services are offered by some casinos in the UK, which creates potentially higher risks of ML and TF occurring in casinos which offer this facility. In 2023, 13% of casinos offered MSB services to their customers with approximately two thirds of MSB transactions within casinos being foreign currency exchange. Non-remote casinos handle a significant number of high-value transactions in multiple currencies. More third-party transfers and third-party cheques were transferred 'to' casino accounts than 'from' them, which increases the risk of criminal funds moving into the UK financial system. Euros are the most frequently exchanged currency and US Dollars are the highest volume transaction currency. UAE Dirham is a popular currency for transactions into foreign exchange facilities and onwards into casino accounts, however it is not a popular currency when transferring out of casino accounts. As part of their activity to address these risks, the Gambling Commission participates in HMRC's MSB taskforce.

### **Remote slot gaming**

5.166 [Since 2020](#) income from remote casino slot games has increased by 52% from £2.3 billion to £3.6 billion, with more customers reportedly gambling for longer periods. The increased scale and volume of slot gaming, when

combined with risks of non-face-to-face business relationships and the non-compliance with CDD requirements by some casinos (as discussed above), increases the risk of ML and TF. The UK government has recently implemented new slot stake limits (£5 limit for all adults from 9 April 2025, and £2 limit for adults aged 18 to 24 from 21 May 2025). With limited data currently available for these changes, no conclusions can be inferred in this assessment as to their likely impact in mitigating ML and TF risks in the UK.

## Illegal casinos

5.167 Illegal casinos continue to attract new customers, heavily targeting online advertising with offers that entice new customers to gamble with them. As they operate illegally, they will not be supervised by the Gambling Commission, nor have a requirement to implement MLR controls. The use of cryptoassets in illegal casinos is also increasing. The Gambling Commission has continued to take significant enforcement action in 2024/25 to address the risks of illegal casino gambling. This includes joint action with the police to identify and close illegal non-remote casinos and disrupt the activities of illegal remote casinos. Suspected ML and other serious predicate offences have been identified during these joint operations, resulting in arrests being made. Between April 2024 and March 2025, the Gambling Commission issued 1,158 stage one cease and desist notices in relation to illegal casinos, referred 118,181 URLs to Google and Bing, and had 81,292 URLs which promoted illegal casinos removed from search engine results.

## Emerging Risks

5.168 As with other sectors, casinos are experiencing increasingly sophisticated attempts to bypass CDD checks using false documentation, which in some cases have been generated using Artificial Intelligence (AI).

5.169 In-game currencies present a risk of both [fraud](#) and money laundering and offer an opportunity to gamble both the proceeds of crime and to generate them. Crash games, in which customers have a multiplier applied to their stake which increases over time and they must attempt to cash out before the game 'crashes' and the funds are lost, have been offered in crypto casinos (which are illegal if accessible via the UK). However, they are also offered by some licensed casino operators. The increased interest from the regulated casino market in crash games may pose an opportunity to launder criminal funds through GB- regulated operators. As there is an incentive for legitimate customers to use these games in a similar way as may be useful to criminals, criminals could conceal the high risk behaviour of cashing out quickly with limited gameplay within the context of the crash game (where these behaviours are inherently more common).

## Terrorist Financing risks

5.170 The risk of terrorist financing remains **low** in this assessment, which is the same as the 2020 NRA rating. Typologies and risk indicators of terrorist financing are shared with the casino sector and the Gambling Commission by

relevant LEAs. As explained in this assessment, inherent risks are present in the casino sector which can be exploited by terrorist financiers, therefore full implementation by the sector of required mitigations are imperative, and vigilance should be maintained, as sources of funding for terrorist financing can derive from both illicit and licit sources of finance.

### **Gambling Activities not regulated for ML/TF**

5.171 Currently remote and non-remote casinos are subject to the UK's MLRs, meaning that all other forms of gambling (including bingo, betting, lotteries, and adult gaming centres) are not captured by the MLRs. However, according to the Gambling Commission's 2023 Risk Assessment, there is also a high risk of money laundering associated with remote betting, remote bingo and non-remote off-course betting. Significant volumes of funds are moved through these three activities, accounting for 32.1% of the total GB gambling industry gross gambling yield. While these sectors are not subject to the UK's MLRs, they are subject to stringent licence requirements, including those related to AML. As with casinos, the Gambling Commission tests compliance with these requirements via a programme of compliance activity.

5.172 Off-course retail betting premises account for 71.2% of all gambling outlets in the UK. The complexity of transactions and their speed, increased anonymity and exposure to high risk customers, increases the vulnerabilities these premises are exposed to. Customers are able to deposit cash into betting accounts over the counter and make electronic transactions in retail betting premises which, with some operators, can then be credited to the customer's remote betting account and vice versa, which makes transaction chains more complex and more able to be moved cross border at speed. Whilst off-course retail betting premises are not subject to the MLRs, they are bound by strict licence conditions, meaning they must implement appropriate and effective AML and CTF controls, including risk sensitive identity verification and other 'know your customer' measures.

5.173 Remote gambling activities, e.g. betting and bingo, have an account-based approach similar to remote casinos. The use of e-wallets online gambling accounts can result in co-mingling of funds from both MLR-regulated (casino) and non-MLR regulated (betting, bingo etc.) activities (contained within the same gambling account), which could make investigation by law enforcement agencies more difficult. The Gambling Commission regularly assists law enforcement agencies in their investigations and is able to provide specialist support in interpreting gambling account data.

5.174 Wider Betting-related criminality, e.g. match fixing and the use of insider information, continues to be a risk for betting businesses in the UK, and this risk is addressed by the Gambling Commission's Sports Betting Intelligence Unit (SBIU). Since 2020, high volumes of reporting of suspicious betting activity have gradually decreased, however the manipulation of sporting events remains a concern, with the use of third-party remote (mule) accounts a popular option for some criminals, including OCGs. Common areas of ML risk include illegal betting groups manipulating or creating false markets, creation of illegal betting apps, customers defrauded using illegal websites, illegal

gambling premises knowingly allowing the use of criminal funds to gamble, and non-gambling premises allowing large scale cash gambling illegally. The widening availability of betting markets means that there are emerging threats, e.g. the emergence of political and novel betting markets.

## Non-Profit Organisations

| NPOs                | NRA 2017 | NRA 2020 | NRA 2025 |
|---------------------|----------|----------|----------|
| Money Laundering    | Low      | Low      | Low      |
| Terrorist Financing | Low      | Low      | Low      |

### Introduction

5.175 Non-profit organisations (NPOs) are organisations that primarily engage in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of “good works”. The UK’s NPO sector is large and diverse, spanning many different types, aims, activities, sizes and places. In the context of money laundering and terrorist financing, charities remain the most significant component of the NPO sector owing to their relative income, exposure to risk and profile. As of 25<sup>th</sup> June 2025, there were over 184,000 registered charities in the UK with a combined income of over £100 billion. Over 20,000 charities operate internationally, undertaking a range of charitable work.

5.176 Since the 2020 NRA, there have been greater domestic and international efforts to protect legitimate humanitarian activity of NPOs from any unintended consequences of terrorism financing and the MLRs. This includes the implementation of UN Security Council Resolution 2664, changes to the Financial Action Task Force’s standards where relevant to NPOs, and legal [guidance](#) published by the Crown Prosecution Service.

### Money Laundering risks

5.177 The money laundering risk in the NPO sector is **low**. However, the risk is judged to have risen within the “low” banding, due to a greater scale of ML activity in the sector than previously understood. This adjustment reflects a more informed understanding of the sector from supervisors, rather than an indication that the money laundering risks themselves have increased. This should be read alongside the [MSB](#) and [IVTS](#) sections.

### Vulnerabilities

5.178 Concerns remain where some charities are accepting interest free loans from their members or local community in cash and making repayments via bank transfer. This practice exposes the charities to potential money laundering risks by those facilitating the loan. Recent concerns have also been raised about close connections between charities, connected businesses and companies and that these structures may facilitate money laundering. Charities rely heavily on donations and anonymous donations continue to be a vulnerability in the sector. Online giving platforms are used extensively by charities and potentially provide a mechanism for donations to be made on a more detached basis.

5.179 A significant proportion of independent schools are registered charities, and these organisations remain vulnerable to receiving criminal funds through the payment of tuition fees.

#### **Box 5.H - Case Study: SYUK**

In January 2025, Rajbinder Kaur was given a custodial sentence of two years and eight months for money laundering and six counts of theft, totalling £50,000 in charitable donations to Sikh Youth UK ('SYUK'). Ms Kaur and her brother, Kaldip Singh Lehal, were also convicted of knowingly or recklessly providing false or misleading information to the Charity Commission England and Wales (CCEW) in an attempt to conceal Kaur's offending.

In 2016, an application to register SYUK as a charity was submitted to the regulator. However, when the CCEW requested further details due to a lack of sufficient information, the applicants chose not to continue, resulting in the application's closure. SYUK solicited funds from the public in support of carrying out charitable activities. However, Kaur diverted these donations into her own bank accounts, using them to pay off personal debts and to send funds to family members. She used over 50 personal bank accounts to obscure the stolen money's trail. In 2018, concerns raised by West Midlands Police prompted the CCEW to launch a statutory inquiry into funds held by and raised in connection with SYUK. Kaur and Lehal were arrested and charged in 2019. Evidence from the CCEW's statutory inquiry supported the police's investigation and was presented at trial, helping to secure their convictions.

#### Strength of mitigations

5.180 NPOs are expected to have in place suitable financial controls and the relevant regulators publish a range of guidance and toolkits for charities and their trustees. Guidance sets out the areas of greatest risk and offers guidance on mitigating them. However, the level of understanding of ML risks varies across the sector, given its diverse nature and various sub sectors (international, faith, education, amateur sport, environment etc).

### **Terrorist Financing Risks**

#### Vulnerabilities

5.181 Consistent with the findings of the 2020 NRA, the UK NPO sector continues to be assessed as **low risk** for terrorist financing. The type and level of risk varies within the sector owing to its diversity: charities operating in or near conflict zones and jurisdictions where terrorists control territory are exposed to a significantly greater risk than other parts of the sector, by virtue of their proximity to active terrorist threats.

5.182 Some charities operating internationally rely on downstream partners and financial institutions within the wider payment and delivery chains, and the risks faced by charities may therefore be impacted by the risk management and compliance capabilities of these other organisations. Correspondent banking poses another delivery chain vulnerability in this context, given international banks are subject to differing, and in some cases, weaker levels of regulation.

5.183 Similarly, incidences of de-risking by financial institutions and the absence of formalised banking systems in the areas where NPOs often operate can push NPOs towards higher risk, informal mechanisms to move funds, such as cash transactions and use of less well-regulated money service businesses (MSBs) or other internal value transfer systems (IVTSs).

#### Scale

5.184 Whilst charities working in or near conflict zones and jurisdictions where terrorist groups control territory have greater exposure to terrorist financing risks, no individual from a UK NPO has ever been prosecuted for terrorism offences relating to legitimate humanitarian, development or peacebuilding work.

#### Mitigations

5.185 Since the 2020 NRA, the CCEW's guidance has been updated where appropriate to reflect FATF's revisions to Recommendation 8 and the accompanying Best Practices Paper. The CCEW is also conducting an NPO Domestic Sector Review for the UK and has made amendments to its guidance on internal controls to provide more detail on the financial controls that a charity should have in place. The Charities Act 2023 has strengthened the regulatory regime for charities in Scotland by extending the rules for automatic disqualification. CCNI has not identified the need to introduce any additional mitigations to terrorist financing since the 2020 NRA.

5.186 There has continued to be close cooperation between the CCEW and Counter Terrorism Policing (CTP), including CTP's National Terrorist Financial Investigation Unit (NTFIU), on intelligence sharing, outreach to the sector, and engagement with government departments such as the Home Office. There also continue to be effective mechanisms for the OSCR and CCNI to share and receive information with Police Scotland and PSNI respectively.

5.187 In line with the findings of the 2020 NRA, the sector demonstrates the capacity to effectively identify and mitigate risks internally. Many of the charities delivering aid overseas have robust financial controls to identify the source of funds, extensive due diligence systems to identify beneficiaries and screen downstream partners, and many NPOs and their partners have sophisticated security systems in place.

5.188 There continue to be significant levels of charitable expenditure and activity in jurisdictions recognised as high risk by HMG since the 2020 NRA. NPOs are

required to submit applications for a defence or 'consent' under Section 21ZA of TACT 2000 where applicable. A range of humanitarian exceptions and general licences are now in use under SAML 2018 but there may be circumstances where individual licences are needed to permit activity that would otherwise be prohibited by sanctions. The Government continues to expect a high level of engagement with the relevant reporting mechanisms from organisations operating in these contexts. It is committed to working with the sector, including through the Tri-Sector Group (See Section 1 for more information on the TSG), to develop practical measures and guidance to manage risk and support compliance with the legislative framework, including increased use of reporting mechanisms where appropriate, without compromising other HMG priorities or unnecessarily impeding legitimate humanitarian activities overseas.

#### **Box 5.1 - Case Study: Tarek Namouz**

In 2023, Tarek Namouz was sentenced to 12 years in prison for terrorism offences, including financing Daesh in Syria.

During his trial, Mr Namouz claimed he was funding charitable projects, presenting plans for a farm and building in Syria intended to aid those in need. However, these plans were a cover for his true intent; the creation of a Daesh operational base for the manufacture and storage of weapons, from which terrorist attacks could be launched on neighbouring areas.

Mr Namouz was found guilty of eight counts of entering into a funding arrangement for terrorism. He was also convicted of two counts of possessing terrorist material after videos were found on his phone detailing how to make an improvised explosive device and using knives to carry out an attack.

### **Activities not regulated for ML/TF**

#### **Donation-based crowdfunding**

5.189 Crowdfunding is a method by which individuals, charities and businesses can raise money from the public to support a campaign through online means. The sector is likely to grow with the growth of new payment technologies such as cryptocurrencies and the use of social media and gaming platforms for crowdfunding activity.

5.190 There is intelligence to suggest that digitally enabled donation-based crowdfunding through dedicated online platforms and social media is increasingly being exploited for terrorist financing purposes. There has been an increase in police investigations involving online crowdfunding platforms as well as modest increases in Suspicious Activity Reports (SARs). Internationally, in its [report](#) in October 2023, the FATF concluded that

donation-based crowdfunding is vulnerable to exploitation for terrorist financing, including [TF crowdfunding](#) activity using cryptocurrencies.

5.191 Donation-based crowdfunding is an attractive method for terrorist financing due to the ability to rapidly transfer funds and easily reach a global audience without geographical restrictions and is open to exploitation by terrorist actors due to limited regulatory oversight in the UK. In contrast to loan and investment-based crowdfunding, donation-based crowdfunding is an activity that falls outside the MLRs, and crowdfunding and social media platforms are therefore not subject to the corresponding legal obligation under TACT 2000 to report suspicious activity to the NCA. The absence of reporting from the sector means that HMG does not have comprehensive data on the scale and typologies of abuse. This gap in financial intelligence is further exacerbated by the limited information provided through bank account transactions and platforms swiftly removing terrorist material in accordance with their obligations under the Online Safety Act. This limits opportunities for law enforcement agencies to identify and investigate possible terrorist financing suspects, and removes evidence that payment service providers (PSPs) could otherwise report when facilitating transactions.

## Legal Service Providers

| Legal Service Providers | NRA 2017 | NRA 2020 | NRA 2025 |
|-------------------------|----------|----------|----------|
| Money Laundering        | High     | High     | High     |
| Terrorist Financing     | Low      | Low      | Low      |

### Introduction

5.192 [Legal Service Providers](#) covers a wide variety of firms or individuals providing specific legal services, including firms or practitioners who provide legal or notarial services to other persons when participating in financial or real estate transactions; and those services offered by legal professionals from within larger businesses such as financial institutions and accountancy firms. The list of activities in scope is broad and practitioners must make a determination as to whether a matter is in scope of the regulations on a case-by-case basis. Around 170,000 solicitors practised in England and Wales in March 2025 and there are more than 17,000 barristers practising in England and Wales currently in 2025. In the UK overall 7,564 firms or individuals in the UK legal sector were registered for supervision under the MLRs in 2023-24, a slight decrease from 8,462 in 2021-22.

### Money Laundering Risk

5.193 The money laundering risk for the sector is assessed to have remained **high** with no significant change in vulnerabilities since 2020. Criminals are often drawn to legal service providers due to the veneer of legitimacy legal professionals can offer due to perceptions of the sector's integrity. The nature of the services offered, and the volumes of money that can be moved through them also contribute to the sector vulnerabilities, although the speed of transfer can often be slower than in some other regulated sectors. Non-compliance levels remain relatively low across the sector, but the vulnerabilities the sector is exposed to and the scale of money laundering involving the legal sector have also remained high since 2020.

### Vulnerabilities

5.194 The 2020 NRA judged that the services most at risk of abuse for money laundering purposes were conveyancing, trust or company services and misuse and exploitation client accounts. These continue to be assessed as the highest risk services and more details on these areas are below.

5.195 Legal Service Providers that offer a combination of legal services, such as solicitors, are at the greatest risk in the legal sector. The [OPBAS 5th report](#) found that there was a consistent view among the PBSs that barristers and advocates are exposed to a lower level of risk. However, the potential for AML non-compliance in these activities remains.

5.196 Criminals may use a combination of legal services to frustrate due diligence efforts and complicate transactions. Whilst criminals typically seek to use a single lawyer or firm, ultra-high-net worth criminals wishing to avoid scrutiny may employ the services of several firms. This can make it more difficult for a single LSP to identify illicit activity, particularly where inadequate source of funds checks are performed.

5.197 The 2020 NRA identified sham litigations as an emerging area of risks. Since then, there has been [one prosecution](#) related to this issue, indicating that while the risk persists and firms should remain aware, it is not currently assessed to be a widespread or common issue.

#### Scale

5.198 Whilst there has been a decrease in the volume of SARs submitted by the legal sector since 2020, the decrease in SARs is not judged to be indicative of a decrease in the scale of misuse of legal professionals. The volume of cases of suspected money laundering that involve lawyers has remained high, relative to the small number of regulated professionals. Many identified cases that involve legal sector professionals involve high sums of assets laundered.

#### Strength of Mitigations

5.199 The majority of firms invest in ensuring their services are not used for criminal purposes. In 2023/24 only 16% of firms reviewed were deemed non-compliant. However, where legal professionals are complacent, take a 'tick box' approach to compliance, or lack sector specific knowledge and/or training on the money laundering threat, the risk of the services provided being exploited increases.

5.200 Weaknesses in supervision can increase these vulnerabilities. Compliance levels at PBSs have improved since the creation of OPBAS. However, the 2024 OPBAS report found effectiveness to be inconsistent, with none of the selected nine PBSs across the legal and accountancy sectors assessed by OPBAS over 2023/24 effective in all OPBAS sourcebook areas. The [HM Treasury 2023/24](#) report showed an increase in the number and total value of fines issued by PBSs, with 240 fines issued in the 2023/24 reporting period compared to 33 fines issued in 2022/23.

5.201 Whilst much work has been done to improve supervision of LSPs by PBSs since the previous NRA, pockets of ineffectiveness remain in enforcement, the application of risk-based approach and information sharing. HM Treasury's consultation on reform of the AML/CTF supervisory regime acknowledges these issues and seeks to make improvements to the effectiveness of supervision in the UK.

## Conveyancing

5.202 **OPBAS** continues to consider conveyancing as an inherently high risk activity and the risk that conveyancing services are abused for money laundering purposes remains high. It often involves legal service professionals who are essential for most property purchase in the UK. The purchase of property in the UK is attractive to criminals who seek to launder large sums of illicit funds in a single transaction, both to disguise their wealth and to benefit from the use or ownership of the property.

5.203 Conveyancers who deal with prime or super-prime property purchases are more likely to be exposed to higher risk persons such as PEPs, and overseas buyers where it may be more difficult to assess source of wealth. However, there remains a risk that smaller scale criminals will look to purchase properties with more modest values. This risk can be increased if insufficient controls are put in place. There has been an increase in firms found non-compliant with the MLRs by the Council for Licensed Conveyancers, rising from 48% of firms reviewed in 2021/22 to 66% in 2023/34.

## TCSPs

5.204 The provision of trust or company services is rated as high risk in this NRA and is examined in further depth in the sector specific chapter, and the **typology** section. LSPs who offer those services should familiarise themselves with those sections and their supervisor's assessments as providing TCSP services alongside traditional legal services heightens risk exposure.

### **Box 5.J - Case Study: property purchase**

On 7<sup>th</sup> January 2019 a solicitor was found guilty of money laundering offences. The individual acted for two clients on over 80 property purchases, with total purchase prices amounting to more than £7.3 million. Deposit and purchase monies were found to come from fraudulently obtained mortgages, money raised from such fraudulently obtained properties and some unexplained cash deposits.

The judge commented that the solicitor's position as a solicitor meant that his culpability was high, and noted that he "must have been aware" that he was assisting in the acquisition of criminal property.

Separately, the individual worked as solicitor for a private company, of which he was also a shareholder. This company was found to have been used to disguise or convert some of the proceeds of drug dealing. The individual was struck off the Roll of Solicitors in England & Wales.

## Misuse of client accounts

5.205 LSPs use designated and pooled client accounts to hold and move money on behalf of their clients for related legal services. Money may move rapidly

and in large sums through these accounts. Client accounts continue to be assessed as high risk as they can be misused by criminals to both move illicit funds and to provide a veil of legitimacy to the proceeds of crime. Criminals can use client accounts as a way of moving money from one individual or entity to another through a trusted third party (the LSP) under the guise of a legitimate transaction. They are also attractive to criminals as their use can contribute to true transferee and beneficiary being shielded, reducing transparency and assisting with obfuscating the source of funds. A substantial proportion of client account transactions are in scope of the MLRs and there are strict rules on handling client money. These rules are formulated by PBSs and are intended to mitigate the risk of abuse. The emergence of Third Party Managed Accounts as an alternative to client accounts may, in time, reduce the client account risk. A larger evidence base is required before an assessment of any displacement of risk, and the longer term impact of the move towards third party managed accounts can be made.

#### **Box 5.K - Case Study: Tipping off**

Mr Osmond was co-founder and senior partner of London firm Osmond & Osmond, as well the MLRO. Mr Osmond's client was businessman James Redding Ramsay.

In 2018, SFO investigators made covert enquires about Mr Osmond's client who had recently paid £4 million toward the purchase of a property in Mayfair. Mr Osmond contacted his client to inform him of the investigation and met with him over the next five months to discuss, including by flying out to Mr Ramsay's home in Malta.

Furthermore, in response to an SFO request, Mr Osmond supplied a fake 'letter of engagement' that set out his role as solicitor for a British Virgin Islands company which was purchased by Mr Ramsay and used to move funds for the purchase of the London property. Consequently, in 2023, Mr Osmond was prosecuted for 'tipping off' and was sentenced to nine months in jail, suspended for 18 months.

The SRA carried out a forensic investigation into the firm and found that Mr Osmond had also breached the Solicitors Accounts Rules and MLR by allowing more than £28 million to pass through the firm's client account without any underlying legal transaction. The Solicitors Disciplinary Tribunal suspended Mr Osmond from practice for 12 months on 25 February 2025, and placed restrictions on his practice to take effect following the expiry of the period of suspension.

### **Terrorist Financing Risk**

5.206 Consistent with the findings of previous NRAs, we continue to assess the terrorist financing risk as **low**, with limited appetite for terrorist finance actors to use legal services such as conveyancing and client accounts to move funds.

## Accountancy Service Providers

| Accountancy service providers | NRA 2017 | NRA 2020 | NRA 2025 |
|-------------------------------|----------|----------|----------|
| Money Laundering              | High     | High     | High     |
| Terrorist Financing           | Low      | Low      | Low      |

### Introduction

5.207 The accountancy sector covers a wide variety of firms ranging from sole traders, medium-sized enterprises to large multi-national companies, and also includes people who hold no formal accounting accreditation. There are approximately 50,000 service providers supervised by one of 13 PBSs or by HMRC, with the majority being small firms. Accountancy services which can be used for money laundering purposes include payroll services, bookkeeping, insolvency services and tax advice services. ASPs may also offer trust and company related services, and services, such as auditing, which are an important defence against economic crime. This section does not cover in-house accountants who do not fall under the MLRs.

5.208 The money laundering risk for ASPs remains **high**. The prevalence and accessibility of accountancy service providers, with a wide range of services available online and in most towns, contributes to its attractiveness to criminals. Accountancy service providers can be used to provide the appearance of legitimacy to transactions that feature criminal funds, for example, through the use of accountant's certificates of confirmation to support the falsification of documents such as accounts and invoices. Criminals will seek to take advantage of weak or inadequate risk assessments, policies, controls and procedures and, although less likely, may seek to infiltrate or corrupt the employees of legitimate firms. The risk is particularly high for clients with [cash intensive businesses](#) as this can disguise the real source of funds and allow for the easier mixing between legitimate and criminal earnings.

### Vulnerabilities

5.209 Accounting services can, when properly carried out and in compliance with the MLRs, provide an important defence against economic crime. However, when these functions are not properly carried out, whether accidentally, negligently or complicitly, they risk legitimising criminal activity. The quality of audits delivered by qualified accountants – as assessed by the Financial Reporting Council – has improved since 2020, but a small number need significant improvement, potentially enabling criminal abuse.

5.210 The fragmentation of services also poses a potential risk. Criminals who require multiple services, may use different firms for each service, preventing a single firm from seeing the full picture. For example, tax advisers and payroll agents may be employed to do specific tasks and only see limited information

from their client. Bookkeepers may then also be used but only given incomplete records. Where a firm has access to, or interactions with, most or all the activities of their customer, they will be better placed to understand the full picture and identify risks.

5.211 Similarly, providing services in a supply chain can generate risk; a supply chain is created when a service is provided to an end user via an intermediary. Supply chains can compound the risks by placing distance between the service provider and the end user of the service making it easier for the end user to maintain anonymity. Where supply chains involve intermediaries or end users outside the UK, the risk is further increased; this combines the risk of the service being provided overseas or to high risk third countries.

5.212 Most UK accountants have a limited international exposure with firms predominantly having UK based and local community practices. However, where firms – typically larger firms – do have international clients, it is important that they understand the potential risk of abuse by firms and individuals with links to higher risk jurisdictions and individuals, such as overseas politically exposed persons.

#### Strength of mitigations

5.213 Firms are likely to be more vulnerable when they have a poor understanding of the money laundering risks and don't have appropriate policies, controls and procedures in place. This is of particular concern in smaller firms and sole practices – who collectively make up the majority of accountancy firms – where the company or individual may lack the knowledge, resources or time to put those practices in place and ensure they are kept up to date and relevant, both in broad terms and as they relate to particular clients. Poor customer due diligence both at onboarding and on an ongoing basis is amongst the most common compliance issues identified and risks leaving firms exposed to abuse. This issue is highlighted when larger firms remove clients they have identified as high risk with the client then successfully moving to another firm with less robust procedures.

5.214 Whilst a great deal has been done by supervisors and professional groups to provide training and raise understanding and awareness, significant gaps in knowledge of the risk remain. The number of SARs submitted by the sector also remain lower than the assessed risk would suggest is commensurate (and in comparison with a spike in 2020-2021, which may have reflected Covid-19 response related fraud risks being reported).

5.215 Accountancy service providers are supervised by 13 PBSs or by HMRC. As noted in OPBAS's September 2024 review of themes and progress in the PBS (which excludes HMRC), there remain grounds for improvement among the sector's supervisors – with none deemed fully effective – particularly around

the resourcing of AML supervision. The review notes that both onsite visits and desk-based reviews are yet to return to pre-2020 levels. However, a greater proportion of these visits are resulting in formal or informal action to address failings, which may suggest a better understanding of where problems may exist.

### Payroll services

5.216 The provision of these services involves the managing of client funds and may therefore include legitimising proceeds of crime to provide payment. Additionally, clients may seek to over or under report employee numbers or pay as a means of moving criminal funds into new accounts under the guise of payment to people who have not carried out any work or as a means to avoid taxes such as National Insurance contributions. This is particularly risky activity where payroll services are being provided as a standalone service and/or the accounting firm lacks familiarity with the company. Both situations mean that the service provider may lack a full picture of the company's activity, making it easier for false information to be provided.

### Tax advice services

5.217 The tax compliance services provided by accountants are important and valuable to companies of all sizes. However, accountants may knowingly or unknowingly facilitate tax evasion and fraudulent claims, and consequently the laundering of the proceeds of those offences, where clients deliberately provide inaccurate or incomplete information, for example, by undeclared income or payments.

### Trust or company services

5.218 The provision of trust or company services is rated as high risk in this NRA and is examined in further depth in the sector specific chapter and the [typology section](#). Accountants who provide those services should familiarise themselves with those sections and must take into account their supervisor's assessments. This is of particular relevance to ASPs as a large majority of registered TCSPs were supervised by accountancy PBSs, in the year ending March 2024. Where firms perform both broader accountancy and TCSP functions they must ensure they are correctly registered for both.

#### **Box 5.L - Case Study: Farooq**

In 2024 Bilal Farooq, an accountant, was convicted and sentenced to two years imprisonment for helping a drug dealer launder £190,000 over a 12 month period. Farooq allowed criminal funds to be transferred into his personal account and the accounts of companies he had set up. During the trial Mr Farooq's barrister conceded that Mr Farooq had 'turned a blind eye' to the source of funds.

## **Terrorist Financing Risk**

5.219 The terrorist financing risk of the accountancy service providers sector remains **low**. Since 2020, there has been no evidence of ASPs being abused for terrorist financing.

5.220 Accountancy service providers are inherently linked to company formation and [Trust or company service Providers](#) (TCSPs), which have their own terrorist financing risks. For this NRA, TCSPs terrorist financing risk score has been assessed to have increased from low to medium, with the risk of company and trust arrangements being created in the UK and receiving funds from organisations that are wittingly, or unwittingly, funding terrorist actors or organisation. Firms will need to be aware of this increase in risk score for TCSPs and, where they offer company or trust arrangements, consider their supervisors risk assessment, as well as apply the appropriate risk assessment, policies, controls and procedures for both the sector and their TCSP activities.

## Trust or Company Service Providers

| Trust or Company Service Providers | NRA 2017 | NRA 2020 | NRA 2025 |
|------------------------------------|----------|----------|----------|
| Money Laundering                   | Medium   | High     | High     |
| Terrorist Financing                | Low      | Low      | Medium   |

### Introduction

5.220 Trust or Company Service Providers (TCSPs) encompass a wide range of business models that provide one or more TCSP services. Common types of TCSP business model include: formation agents, virtual office providers, accountancy or legal service providers offering ancillary TCSP services, trustee service providers, company secretarial services and nominee services. Some businesses, referred to as multi-service providers, offer a combination of TCSP services and are therefore likely to face heightened risk. For most firms, TCSP activity is a secondary activity, usually alongside other accountancy or legal services.

5.221 A small proportion of firms operate as specialist formation agents and/or virtual office providers. Differing business models will be exposed to different levels and types of risk. There were just over 27,000 UK TCSPs operating at the start of 2025. It is likely an unregistered population continue to operate in the UK. In 2023/24 HMRC fined four businesses for failure to register as TCSPs.

5.222 The supervision of TCSPs is split between supervisors. The majority of TCSPs (approximately 90%) are supervised by legal or accountancy PBSs. HMRC supervises most TCSPs for whom TCSP services are their primary business, including nine of the top 10 firms responsible for approximately 80% of company registrations facilitated by TCSPs. A small number of TCSPs are supervised by the FCA, often provided alongside wider financial services in the wealth management sector. This chapter should be read alongside the company/trust typology chapter.

### Money Laundering Risk

5.223 The money laundering risk of TCSPs continues to be assessed as **High**. Despite some improvements in the capacity of supervisors and law enforcement agencies to address TCSP risks, the vulnerabilities TCSPs are exposed to has risen since the 2020 NRA. This rise is primarily a result of improved knowledge rather than significant changes in the perceived risks since 2020.

5.224 Whilst a TCSP is not necessary for the illicit use of corporate entities and legal arrangements, TCSP services can be used in mass company

incorporations and to assist layering and obscuring beneficial ownership which can be appealing to criminals.

### Vulnerabilities

5.225 The use of complex structures and legal arrangements, use of virtual office addresses not connected to beneficial owners, and the combination of services involving intermediaries and nominees, can facilitate anonymity. This anonymity is attractive to criminals looking to distance the criminal origin of funds. Reforms to Companies House under ECCTA, once fully implemented, may decrease this anonymity, but it is too early to assess this.

5.226 Some TCSPs have a significant level of exposure to overseas money laundering risks, but this is not sector wide. For example, in the accountancy sector larger firms tend to have more international focus, whereas smaller accountancy firms generally provide TCSP services primarily for UK customers. Other sub sectors, for example virtual office providers, have noted an increase in payments made with large volumes of cash by foreign nationals, many from China, where it can be difficult to trace the source of funds.

#### **Box 5.M - Case Study: TCSP and accountancy services**

An investigation has revealed UK subjects involved in large-scale frauds and scams since 2015, who own/have owned a multitude of frequently-established shell companies and are suspected of money laundering through company accounts. Many of these companies have been registered to a very small West Midlands accountancy firm, supervised by a PBS and licensed for TCSP services.

5.227 Companies formed by TCSPs do not directly move money themselves, requiring other services such as a bank account to do so. However, once a company or trust is formed, large volumes can be moved into and through it. Since 2020, there has been an increase in the partnering of TCSPs (including overseas based nominees) and EMIs to provide company/financial service packages, which further increases the speed in which money can be moved through newly created structures. In just one case £30 million was moved through multiple TCSP linked UK companies as part of a TBML scheme. In another scheme, tens of UK companies were used to launder proceeds of fraud from non-UK jurisdictions averaging \$800,000 and up to €3.6 million per transaction.

5.228 There is a large variance in the exposure of different sub sectors to these vulnerabilities. For example, for trust services the cost is relatively high and the speed of movement is low, given the long-term nature of trusts. In contrast, companies and company packages (including bank accounts, a registered office address and company directors) can be formed or

purchased for relatively small amounts, with many TCSPs offering 'same day' completion of formation services offered online.

5.229 Another vulnerability centres around the lack of an ongoing relationship with a customer in some sub-sectors. Some TCSPs referenced in investigations only interact with the criminal when creating the company that is later used for criminality. If an associate or nominee without an obvious criminal background is used to seek the formation, and appears credible, the TCSP may wittingly or unwittingly fail to suspect its future criminal use. When the TCSP acts as a nominee director or shareholder, the business relationship is ongoing, which means they should have full knowledge around how the firm is being used given the director duties under the [Companies Act](#). This is also the case where TCSP services are ancillary and provided to clients with which the business has a longer standing relationship. In these cases, firms should be alert to changes in longstanding customer risk profiles as well as the purpose and legitimate business need for new services requested.

#### Strength of Mitigations

5.230 Supervisors have increased efforts to support TCSPs to comply with the MLRs. Since 2020, HMRC has produced additional webinars, YouTube videos, and updated guidance on GOV.UK to support TCSP compliance. OPBAS also published a multi-PBS project on TCSP risks, supporting a system-wide approach to tackling the abuse and exploitation of TCSPs by criminals.

5.231 Following the 2020 NRA's rise to high risk, a TCSP action plan was launched between law enforcement, supervisors, OPBAS and Companies House. Key actions from the plan included the distribution of a TCSP manual to local and regional police, the creation of a public-private intelligence cell to produce an alert of TCSP red flags, TCSP thematic review exercises undertaken by PBSs, and TCSP intensification intervention run by HMRC on its supervised population.

5.232 Despite this, supervisors continue to identify compliance failings in the sector. Whilst the majority of UK TCSPs adequately assess and manage risks, TCSPs who do not have established hundreds of thousands of companies used for criminal activity. Since 2020, there has been an increase in sanctions by HMRC for non-compliance, from 75 warnings and sanctions (including five financial penalties totalling £38,397) in 2021/22 to 103 warnings and sanctions, including 27 financial penalties, totalling £272,430 in 2023/24. In 2024, HMRC proceeded with their first cancellation of a TCSP's registration. Disaggregated data on TCSP enforcement was not collected by PBSs in 2020, but PBSs fines almost doubled from £531,179.00 in 2022/23 to £971,764.90 in 2023/24. PBSs membership cancellations also rose, from seven in 2022/23 to 50 in 2023/24.

5.233 The TCSP market, particularly those acting primarily as formation agents, is highly competitive with very low margins and businesses often competing to onboard and finalise services as quickly as possible. This can lead to inadequate or under-resourced compliance activity, which increases the risk of their services being exploited by criminals.

#### Nominee Services

5.234 The provision of a “nominee” service, where TCSPs provide a nominated director or shareholder to act for a company, can be legitimate but can also be a method of increasing the anonymity of the true controllers of a company. In [UK law](#) nominee directors must meet the same legal obligations as all directors. However, this does not entirely negate the money laundering risks linked to the use of nominee directors. In the 2020 NRA, the risk of nominees was assessed to be relatively lower than other types of TCSP service. Subsequent improvements in information sharing between law enforcement and supervisors now suggest the risk may be higher. Further information is needed to understand and assess the scale of abuse of nominee services.

5.235 As per the 2020 NRA, directors associated with an implausibly large number of companies continue to be considered higher risk. The relative level of risk can differ depending on the size and complexity of the companies. Further high risk factors identified since the 2020 NRA include nominee directors associated with multiple companies in disparate industries, fabricated directors who aren’t actually performing the role at all but have had their IDs stolen, or nominee directors who cannot demonstrate they have the appropriate knowledge, skill or experience to act in the company’s best interests.

#### Supply Chain risk

5.236 Until recently, overseas TCSPs were able to directly form companies with Companies House without registering for UK supervision unless they used a virtual office in the UK. There is evidence of actors abroad forming thousands of companies often linked to one address – e.g., 13,000 businesses using one premise. New measures in ECCTA limit overseas TCSPs from forming UK firms with Companies House. From 2025, alongside certain individuals, only those designated as Authorised Corporate Service Providers (ACSPs) can form firms with Companies House. To be eligible to become an ACSP, firms must be supervised under the MLRs. In response, overseas TCSPs are likely to seek relationships with UK TCSPs to facilitate the creation of UK companies, adding to the risks that the UK TCSPs face.

5.237 The MLRs permit a UK TCSP to rely on a counterparty’s CDD where that counterparty is subject to equivalent regulation. However, the UK TCSP must understand the business of the counterparty, including the rationale for the structures or services created. The UK TCSP also needs to be able to obtain,

immediately on request, copies of CDD information from the counterparty. The UK TCSP remains responsible for any failures in the proper application of due diligence measures, and should consider whether it is appropriate to rely on a third party for CDD checks.

5.238 Higher risk factors in supply chains have changed little since 2020, and include intermediaries who market facilitating anonymity; requests to provide services that can be used as part of a scheme to disguise income and assets; a high number of intermediaries in the supply chain; excessive frequency of requests, and a lack of clear rationale not to use a UK TCSP directly.

#### **Box 5.N – Case Study: TCSP fined for failing to identify beneficial owners**

A TCSP provided multiple services (nominee shareholder, nominee director, registered office address, formation) including in packages. The anonymity this combination of services provides is attractive to criminals seeking to obscure their beneficial ownership or channel illicit funds through layers of corporate structure to obscure their criminal origin. The TCSP failed to identify and verify the beneficial owners of corporate entity customers it provided services to, the majority of which were acting as intermediaries in a supply chain of TCSP services further increasing the risk presented. This put the TCSP at risk of providing services to those seeking to use its services to facilitate money laundering or terrorist financing. The TCSP was required to address these failings and received a fine from its supervisor for its MLR breaches.

#### Off the shelf companies

5.239 As part of their suite of services, some TCSPs will set up and administer onward sale of 'off the shelf' companies. Acquiring a shelf company can be simple, involving a transfer of shares and responsibilities at Companies House, as opposed to completion of the company incorporation process. Shelf companies can appeal to criminals, offering a veneer of legitimacy and in some cases the appearance of a reputable trading history under which to conduct criminal financial and trade activity (such as fraud, smuggling illicit commodities, and TBML). The onward sale of shelf companies is not currently an MLRs regulated activity. HM Treasury consulted on addressing this risk in 2024 and has confirmed an intention to legislate to add this activity to the MLRs.

#### **Terrorist Financing risks**

5.240 The terrorist financing risks of TCSPs increased from low to medium. While there is no information to show a change in scale of terrorist financing through the TCSP sector since 2020, an increased understanding of how the TCSP sector is exposed to organisational terrorist financing risks has caused this change in score. The terrorist finance risks relate to trusts, partnerships and companies which are formed in the UK for legitimate reasons, but are at risk of benefiting from proceeds generated from businesses who operate in

locations where there are higher terrorist activity risks, or areas under the control of terrorist groups. They may be by wittingly or unwittingly paying terrorist groups to continue to be able to operate in the area.

### Vulnerabilities

5.241 Different services provided by TCSPs will attract different levels of risk. This means that for some services - such as one-off company formation, ongoing company services, trust creation and administration, and the provision of e-banking services to trusts and companies - the true nature of business and source of funds may not be properly identified and understood. The terrorist financing risks may be increased when additional vulnerabilities, such as complex corporate structures, are present. These add difficulty in identifying the ultimate source of funds. Vulnerabilities may also be increased when firms fail to fully understand the source of funds or verify the customer's identity; when funds are held in or contribute towards trusts; or where companies are being created and/ or being managed through company service providers. Negligent or complicit providers are an added risk. We do not, at this time, have an adequate understanding of the scale of this risk.

### Mitigations

5.242 Since their low risk score in the 2020 NRA, it is unlikely that TCSPs will have developed a comprehensive understanding of their exposure to the risks of organisational terrorist financing in high risk locations. Whilst there have been some improvements since 2020, supervisors continue to report that inadequate due diligence and risk assessments remain the most common compliance failings. The low risk score in the 2020 NRA has also meant that supervisors, in line with their risk-based approach, have not conducted any terrorist finance specific supervision campaigns since 2020. TCSP terrorist financing risks have instead been assessed as part of wider supervisory activity. Similarly, guidance by supervisors does not yet reflect the improved understanding of these organisational terrorist financing risks, which means that guidance is not yet playing a substantial role in supporting firms to mitigate these risks.

## Estate Agency Businesses

| Estate Agency Businesses | NRA 2017 | NRA 2020 | NRA 2025 |
|--------------------------|----------|----------|----------|
| Money Laundering         | Low      | Medium   | Medium   |
| Terrorist Financing      | Low      | Low      | Low      |

### Introduction

5.243 Estate Agency Businesses (EAB) cover a number of different activities associated with the purchase and sale of property. Activities in scope include offering advice and handling enquiries from sellers and buyers, property sourcing, sending out property details and arranging viewings, and dealing with buyers or sellers of properties.

5.244 EABs in scope of the [MLRs](#) include those based in the UK who deal with overseas property, either exclusively or alongside other property services. It can also cover EABs based abroad if they are doing business with UK customers. Whilst a large proportion of property transactions involve estate agents, estate agents are not essential for all property/land transactions. Private sellers, "off-market" transactions and direct sale by developers can all be used as alternative mechanisms. These are currently out of scope of the regulations and there is an intelligence gap in the proportion of purchases/sale which do not involve estate agents and are out of scope of the regulatory requirements.

5.245 The number of EABs has increased slowly over the last four years, with over 17,300 EABs operating from over 23,800 UK premises registered with HMRC as of March 2025. The vast majority are small businesses with 90% of registered EABs having a single premise. Only 17 businesses have over 50 premises, the largest having 600 premises.

### Money Laundering Risks

5.246 The money laundering risk for EABs remains **medium** rated but has **slightly risen** since 2020, particularly in regard to the vulnerabilities the sector is exposed to.

5.247 As covered in the [property](#) typology chapter, property purchase is attractive to criminals at all scales and locations in the UK, with suspicious purchases identified by law enforcement ranging from super prime London properties worth tens of millions to £50,000 flats in Scotland. 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.

### Vulnerabilities

5.248 Since the 2020 NRA, certain vulnerabilities that expose EABs to money laundering risk have increased. Similar to TCSPs, EABs do not directly deal

with the large volumes of funds associated with the property market but have a large indirect risk.

5.249 Several factors have increased the levels of complexity in the industry. The use of complex structures and arrangements to purchase property remain common, especially in the high end and commercial property market. Representatives from the EAB sector have reported increasing and extensive use of Private Investment Vehicles (PIV) / Special Purpose Vehicles (SPV) to purchase property since 2020.

5.250 There have also been changes in the demographics of persons purchasing property since 2020 including a drop of Russian ultra-high net worth clients since the Russian invasion of Ukraine. One [report](#) flagged that whilst Chinese investment remains high, it has decreased slightly from a 2020 high. It is not, however, possible to identify how much UK property is controlled by Chinese nationals, as Land Registry records only capture a correspondence address and not a nationality. The purchase of property with overseas funds can add complexity for EABs in identifying source of funds and how those funds enter the UK banking system, especially if funds originate from countries with currency export restrictions or are moved via MSBs or IVTS, e.g. Chinese underground banking.

5.251 Property transactions are relatively slow compared to other forms of financial transactions given the number of steps and regulated firms involved in property purchase, so may not be useful for some forms of money laundering that require immediate movement of funds. Auctions can be quicker which in conjunction with other risk factors, such as the use of intermediary agents, can be attractive to criminals. Estate agents are available in most towns in the UK and online availability has increased.

#### Scale

5.252 The NCA assess as much as £10 billion is estimated to be laundered through UK property annually, however this does not mean EABs are exposed to all property risks. In a study of 24 cases associated with Russian illicit finance, 6 involved property, one of which involved EABs. SARs submitted by the sector have steadily grown since 2020, but it is not possible to determine if this indicates a rise in the scale of risk or increased knowledge in the sector.

#### Strength of Mitigations

5.253 Supervisor and law enforcement knowledge of the money laundering risks associated with property has continued to improve since the last NRA, with several assessments published and shared across the law enforcement community. Some gaps remain on the risks associated with commercial property. Data from the newly introduced register of overseas entities will support further improvements in understanding of property risks, but gaps still remain with a number of entities non-compliant with the registration requirement.

5.254 HMRC has run several EAB compliance campaigns since 2020, including a campaign on EABs selling super prime residential properties and campaigns

on social housing and asset, land, and relocation management agents. In the super prime campaign, HMRC identified compliance breaches of varying severity in just over 50% of firms, resulting in three financial penalties. Of the breaches, nearly 60% related to issues with risk assessments, policies, controls and procedures and 21% related to CDD. EABs are often involved in chains with other regulated sectors with purchases involving conveyancing and the financial sector. This should mean that CDD checks are done several times. Nevertheless, compliance activity indicates that some EABs do not carry out sufficient risk assessment and CDD checks, assuming that others in the deal chain will do the checks.

5.255 It is assessed that a number of EABs continue to operate without being registered with HMRC for supervision under the MLRs. Between 2020 and 2025, HMRC issued over 720 penalties totalling £4.9 million to EABs for trading while unregistered. In July 2022 HMRC secured the first criminal conviction of a person operating an EAB that was trading while unregistered. In addition to the criminal sentence, the convicted person was unable to engage in MLR activity until their conviction is spent.

#### Online EABs

5.256 The shift towards remote processes during the COVID 19 pandemic may have introduced new vulnerabilities and challenges in verifying the legitimacy of transactions, potentially facilitating money laundering. This trend of property transactions increasingly being carried out online has continued post COVID 19. Face-to-face contact with a customer offers an opportunity to interact with the customer which is not available when business is conducted fully online. Due diligence processes in online only interactions should take this into account.

#### Super-prime property

5.257 The most significant UK property money laundering risk is through the purchase of super-prime property. The number of PEPs involved in super-prime property purchases is significantly higher than in other property transactions. With super-prime property, even a one or two percent fee will mean a large sum of money coming into the EAB. There is a risk that EAB may face a conflict between taking the large fee or stopping the transactions because of a suspicion of money laundering. UKFIU report instances where high-end EABs request a defence against money laundering to carry on a business relationship despite identifying a significant money laundering risk, including where clients are PEPs subject to adverse media reporting. Supply and demand for London super-prime reportedly increased in 2023. Scotland reportedly also saw a continued increase in property sales totalling more than £1 million in between 2020-23.

### **Terrorist Financing Risk**

5.258 The real estate sector continues to pose a **low** risk from terrorism financing. No new terrorist financing trends have emerged in the estate agency sector

since the last NRA and we do not have any evidence to suggest that the sector has been exploited for terrorist financing purposes. We therefore assess that the sector provides very limited opportunities for terrorists to raise funds through it. However, the sector remains more attractive for other forms of economic crime which could translate to vulnerability to terrorist financing in the future. It is subsequently important for actors in the estate agency sector to continue to put in place strong controls for preventing terrorist financing and other forms of economic crime.

## **Activities not subject to the MLRs**

### Developers

- 5.259. Property developers buy land, obtain planning permission, build property, and sell it to realise a profit. Many developers' business models are complex, particularly in larger developments that may involve joint ventures with landowners who may include public bodies, construction groups, investment partners and others.
- 5.260. Under the MLRs, EABs are currently defined at [Reg 13\(2\)](#) and in accordance with the Estate Agency Act (EAA) 1979 which means to act as an EAB a firm need to sell via a third party. If developers are structured so their sales are via a separate legal entity, the sales entity will fall in scope of the MLRs, but where properties developers sell their own properties within the same legal entity they fall out of scope. The ML risk is the same, but the business structure determines whether their sales are caught by the MLRs or not.
- 5.261. Approximately 600 of the EABs registered with HMRC have stated they are development companies, estimated to represent approximately 26% of developers operating the UK. Other developers may fall in scope of the MLRs via financial services and products they arrange, so are supervised by the FCA.
- 5.262. One particular vulnerability is the high proportion of overseas buyers, that may make it more difficult to assess the source of funds. 'Off-plan' properties (sale of houses or apartments before they have been built or completed) are more frequently sold to overseas buyers. These off-plan purchases are made directly with developers. Developers require pre-sales to reduce the risks associated with market volatility reducing the incentive to understand the source of funds.
- 5.263. Finally, new UK developments are sold off-plan in China by representatives of developers and likely concluded through BVI companies. In this scenario, the marketer in China, the salesperson for the UK company and the person receiving the deposit/funds in China including Hong Kong, may be unclear as to which party is responsible for KYC checks.

## Letting Agency Businesses

| Letting Agency Businesses | NRA 2017 | NRA 2020 | NRA 2025 |
|---------------------------|----------|----------|----------|
| Money Laundering          | N/A      | Medium   | Low      |
| Terrorist Financing       | N/A      | Low      | Low      |

### Introduction

5.264 Letting Agency Businesses (LABs) respond to instructions from landlords seeking to find tenants or from tenants seeking land/property to rent. To fall within the scope of the [MLRs](#), the rent must be equivalent to a monthly rent of €10,000 or more. Unlike the majority of EABs, LABs handle client funds. The number of LABs regulated under the MLRs continue to be a small proportion of the overall lettings market, with around 500 firms conducting LAB activity.

### Money Laundering Risk

5.265 The risk associated with LABs is assessed to have **decreased** to **low**. The 2020 NRA covered LABs for the first time. Whilst inherent vulnerabilities remain that the sector should continue to be aware of, the change in score has largely been driven by the improved knowledge of both the supervisor and sector who have now embedded requirements under the MLRs. The primary means by which rental properties could be used to launder funds has not changed since the 2020 NRA. Tenants paying rent with illicit funds (as a realisation of their proceeds), the landlord and tenant bring part of the same criminal group, laundering their funds under the guise of rent payments, sub letting, and refunds of upfront rental payments remain the primary means through which letting agency businesses could be exploited for money laundering. There is also the possibility of the process being repeated regularly.

### Vulnerabilities

5.266 The high rental threshold for inclusion in MLRs means that regulated LABs are more exposed to specific vulnerabilities than the wider rental market. Regulated LABs are likely to be exposed to high risk persons and products, including ultra-high net worth individuals and PEPs, and often involve the use of complex legal arrangements. In the commercial lettings sector complex structures are commonly used by legitimate businesses so their use is less likely to raise suspicion than in the residential market. The accessibility and speed with which transactions can occur also continues to expose LABs to money laundering risks. Compared to the purchase and sale of property, payments in the lettings markets move quickly, especially in securing properties with deposits etc.

5.267 Changes in the lettings market since the 2020 NRA indicate some vulnerabilities have increased whilst others have decreased. Some LABs have reported an increase in the rise of rent-to-rent (guaranteed rent)

activities where a landlord consents to rent their property to a third party for a specified time and for a guaranteed monthly income. In these cases, the landlord may not have oversight on who the third party allows to occupy the property, increasing anonymity in the lettings sector. However, since 2020 majority of regulated LABs report that they have 'phased out' the use of cash (though cash is still present in lets below the threshold).

### Scale

5.268 The exact scale of money laundering through the regulated lettings market is unknown, and SARs reported are not disaggregated between lettings and real estate businesses. Very few suspected cases have been identified by law enforcement since the introduction of the regulations in 2020. Looking ahead, with the introduction of the Register of Overseas Entities, there is a risk that certain PEPs and ultra high net worth individuals may increase use of rental agreements for super prime property to avoid scrutiny on public registers associated with property purchase which could increase the favourability of the rental sector for money laundering.

### Strength of Mitigations

5.269 2020 HMRC LAB compliance campaigns have improved the supervisors' knowledge of the sector, facilitating improved risk-based supervision. Compliance levels in the sector remain mixed. In one of HMRC's compliance campaigns, nearly half of firms visited had a breach of the MLRs, mainly relating to their risk assessment and/or policies control and procedures, with some instances of customer due diligence failings.

### Use of rental payments for non-rental purposes

5.270 Letting agents can often handle money for fees, deposits and rent, but equally, transactions can happen directly between the parties or with third parties. There is a risk that LABs could be exploited by criminals, channelling non rental funds to the LAB to use it as an intermediary for purchases, that if conducted in the name of the criminal may raise suspicions. Examples reported include two cases, where rents accruing to over £250,000 were being held in the letting agents' bank account and agents were also paying out from those funds on behalf of the landlord, bills such as school fees, service charges on other properties not being rented out, store card bills and settlement of other personal bills.

## **Terrorist Financing**

5.271 The terrorism financing risk through the lettings sector is **low**. This aligns with the risk score from the 2020 NRA and we have not found any emerging trends in relation to terrorist financing and the lettings sector since 2020. We therefore continue to assess that lettings services and agencies provide limited opportunities for raising funds for terrorist activity and have no evidence to suggest the sector has been abused for terrorist financing purposes. However, a residual risk of terrorist financing– while low – applies given the attractiveness of the UK property sector to international investors,

demonstrating the need for lettings agents to maintain stringent controls in place for countering terrorist finance, in line with regulatory requirements.

### **Activities not subject to the MLRs**

#### LABs under the €10k threshold

5.272 The MLRs currently impose a €10,000 threshold on the lettings market. This means the letting of any property for less than €10,000 a month is exempt from the MLRs. Properties for rent under the €10,000 threshold tend to make up the larger part of the market. Since 2020 law enforcement agencies have improved their understanding of LABs under the MLRs threshold but there remains an intelligence gap in the scale of the abuse.

5.273 Law enforcement have identified the misuse of rental properties under the MLRs threshold where criminals appear to be paying rent with criminal funds to facilitate other criminal activities. Renting instead of buying is quicker, with low entry costs and ability to quickly and cheaply relocate if at risk of law enforcement detection, and if under the MLRs threshold, no MLRs controls are put in place. This criminality has a wide geographic focus occurring in both urban and rural locations.

5.274 In particular, MSHT offenders use rental properties as locations for exploitation of victims. Where a property is rented from a complicit property provider, it is highly likely that rent will be paid in cash, sometimes at an inflated price to that advertised. Letting agents have also been identified arranging rentals where cannabis farms run by Western Balkan OCG's are subsequently found. Between 2015 and 2024, the Met recorded 8,000 offences related to cannabis farming or cannabis production, but this is estimated to be a fraction of the industry.

# Section 6 - Cross Cutting Risks

## Artificial Intelligence (AI)

6.1 As set out in the AI Opportunities Action Plan the capabilities of AI are developing at an extraordinary pace and offer remarkable opportunities across both the public and private sector for the UK. This applies to the prevention of money laundering and terrorist financing. Unfortunately, as with many other useful forms of technology, AI can also be abused for criminal purposes. Whilst criminals will continue to use proven methods they also seek to adapt to new opportunities. Current use of AI for money laundering is not fully understood but is not currently believed to be widespread; however, engagement between the private sector and law enforcement suggests that there has been use of AI for synthetic bank account creation, fraud and impersonation, phishing and on-boarding of money mules. Looking to the future, there are a number of ways in which AI could potentially be used to facilitate money laundering on a larger scale. These are focused around the use of AI in the money muling process, AI enhanced identity theft and synthetic account generation, and the use of AI to evade money laundering defences.

### Money muling

6.2 Money muling is a common money laundering technique which AI could be used in. Recruitment of money mules often takes place via social media. AI could support this process, for example by automating the search for potential targets for recruitment by rapidly filtering groups for targets by age or employment status. Once targets have been identified an AI system could potentially be used to further filter and recruit individuals by using automated chat bots that simulate human conversation to better understand a target or actively recruit them. A chain of AI models happening in this way could potentially provide a steady stream of mule recruits to professional money launderers, significantly easing the recruitment burden on them and potentially increasing the volume of illicit transactions they can manage.

### Identity theft and synthetic accounts

6.3 Alongside money mule accounts criminals continue to use stolen, hijacked or synthetic (fraudulent accounts set up by cybercriminals) accounts to facilitate money laundering. The UK [National Cyber Security Council](#) has cited the potential of AI to lower the barrier for novice cyber criminals. Generative AI could potentially help criminals to pass banks and other firms' onboarding checks by creating synthetic identities or generating images to match stolen documents that is required to pass those tests. It could also potentially be

used to automate the process of applying for credit checks, which in turn could facilitate the creation of synthetic bank accounts.

#### Evading and defeating AML systems

6.4 Related to the above, AI could also be used to evade and defeat wider AML defences. Sufficiently advanced trained AI could be used to manage illicit financial transactions in line with normal legitimate account activity such that they do not raise the suspicion of typical transaction monitoring processes. AI managed money mule or synthetic accounts could also be used to undermine behavioural analytics by flooding institutions with low level accounts and transactions that could then disguise illicit activity.

#### AI use in combatting money laundering

6.5 AI also offers opportunities to better combat money laundering in both financial institutions and law enforcement agencies; there are a number of ways in which this could be done, or which are already being explored. For example, if AI can be used to reduce administrative tasks this could free up law enforcement time to be spent on investigations. One of the principal challenges to existing rule-based and algorithmic AML systems is the number of false positives they generate (as well as genuine instances that are missed). These false positives then need to be manually reviewed, resulting in unnecessary work and expense. AI enhanced behavioural analytics may be able to better identify suspicious behaviour by extracting insights from large, complex financial datasets alongside wider sources such as social media datasets and open source information.

6.6 These more open networks can be examined by AI for AML purposes in a number of ways. This can include mapping of connections between individuals to better identify groups, characterising relationships and identifying risks of criminality, particularly in complex cases such as trade-based money laundering where networks, and information about them, are often dispersed. These functions can also support customer due diligence processes.

6.7 Whilst AI may help to improve the development of deepfakes it can also potentially help counter both deepfakes and more traditionally made fraudulent documentation, potentially reinforcing the effectiveness of KYC protections. A number of techniques can be used to carry out this function with various approaches being examined by a range of actors.

## Schools and Universities

6.8 The UK is home to some of the world's leading universities, higher education institutes and private schools. These institutions are an important part of our society and economy that help educate our children, young people and life-long learners, drive research and scientific discovery and attract global talent. Their strong international reputations make them attractive around the world, including to political and business elites and their families. This also applies to criminals and kleptocrats who may seek to use these institutions to launder their criminal funds and reap the reputational and professional benefits on offer for their children.

6.9 A number of reports have highlighted the risks associated with the abuse of the education sector by criminals. For example, one study found six recent instances where a UK school or university had admitted the child of a West African PEP that had been convicted of corruption related crimes or had their assets seized. Other [reporting](#) showed that at least fourteen leading universities had accepted funding from Russian sources. Given the rise in sanctions against Russian PEPs and nationals since the invasion of Ukraine (as well as other, unrelated sanctions) educational institutes should be careful to ensure they are not breaching UK sanctions. The NCA's first successful prosecution for [breaching of the UK's Russia sanctions](#) included the payment of school fees in breach of sanctions. Further information can be found in the [sanctions evasion](#) and [corruption](#) money laundering threats section.

6.10 As set out in the [cash typology](#) section, due to its anonymity and the difficulty in confidently establishing its origin, payment in cash continues to represent a money laundering risk and this is also true for the education sector. The acceptance of cash payments for tuition fees, grants, donations, and other financial transactions means that the education sector is exposed to the risk of criminals seeking to use and integrate criminal funds via their services.

6.11 Receiving third-party payments also creates risk, particularly if educational institutions fail to conduct additional checks on the payment. Third-party payments include any persons other than the student, or the student's parent or legal guardian, and companies that are not registered sponsors. Funds may be passed through several companies before being used to pay fees, which obfuscates the source of funds and makes it difficult for institutions to recognise suspicious activity, making proper due diligence checks particularly important. This difficulty can be exacerbated by a lack of understanding of payment sources and unfamiliarity with parent's/customer's business and financial affairs.

6.12 Students can also be victims of abuse by criminals. Students – international students, particularly Chinese students – are increasingly being used as

[money mules](#) and cash couriers by organised criminal groups. This activity involves students allowing a criminal third party, either willingly or not, to use their student bank account to transfer criminal funds into and out of their account, in return for a proportion of funds laundered. This is often done to add an additional layer of obfuscation and legitimacy to transaction chains. Students can be enticed to do this to earn quick money via a small fee, to facilitate remittances to their home country or by entering a financial arrangement with a third party to settle tuition fees at a reduced rate, with the third party potentially using criminal funds to do so.

6.13 [An online poll](#) by Nationwide found of 1500 students, 91% worry about their financial situation. Collectively, 61% of students believe they are vulnerable to money mule scams, with one of the main reasons provided being increased financial worries (59%). Nearly a third (29%) of students would risk someone else using their account or to transfer money for someone, though there was no indication from reporting that this had occurred.

6.14 Whilst some students are actively complicit in this criminal activity, others may be completely unaware, or may have more limited understanding of the illegality and potential consequences of the activity. If this activity is discovered by banks or law enforcement, it can cause the student significant harm, including closure of bank accounts or loans or criminal prosecution. Educational institutions should ensure that students understand the risks involved and that this activity potentially constitutes a criminal offence.

## Football Clubs and Football Agents

- 6.15 Football is the UK's national game and the most watched sport in the world. Football is an economic powerhouse, with [Deloitte's Annual Review of Football Finance](#) estimating Premier League clubs had a turnover exceeding £6 billion in the 2023/24 season. These factors make football and football clubs an enticing opportunity for legitimate owners and investors at all levels of the football pyramid. However, they could also make football an [attractive target for criminals](#), kleptocrats and other malign actors seeking to [launder their criminal funds or generate further illicit gains](#).
- 6.16 Despite the commercial success at the very top of the game, there are a significant number of clubs that are financially distressed, in part due to the high level of financing needed to run a competitive football club. Such clubs are vulnerable to exploitation by criminals who may offer easy money in exchange for ongoing access that facilitates future criminal exploitation. Alongside money laundering, football has the potential to be abused for a range of other crimes including [illegal betting, match fixing, fraud and bribery](#); these are all proceeds-generating crimes and clubs may also be used to launder money, to invest illicit funds or to grow the enterprise value of the club for a financial return and profits generated from them.
- 6.17 The diverse operating models of football clubs means there is no standard methodology should someone or a group of people wish to funnel criminal funds through the sector. Many clubs have complex offshore corporate structures involving overseas-based enablers and financial products, often in jurisdictions with limited regulatory oversight. Larger clubs with bigger revenues are at a greater risk of receiving the proceeds of corruption for example via investment from overseas PEPs and transnational serious OCGs. Ownership structures using layered front and shell companies, often based overseas or in jurisdictions with low transparency, could obscure the ultimate beneficiaries of clubs and other major stakeholders, such as sponsorship arrangements.
- 6.18 Further down the football pyramid, domestic and local OCGs may be able to launder criminal funds using a variety of methods. As with larger clubs, corrupt actors could use front companies to buy or invest in clubs. Additionally, lower down the pyramid OCGs could provide loans to clubs using criminal funds, which is a particular risk when lower-league clubs are in financial distress and unable to access loans from traditional lenders. Although not specific to football, carrying debt is a normal financial practice for football clubs, presenting a vulnerability that could be exploited by bad actors to invest and move criminal funds through clubs. This could be enabled by poor application of due diligence on investors, especially where a club is already in financial distress.

- 6.19 Clubs could be used as a vehicle both to launder funds, as well as a final destination for criminal money to be invested. The laundering of suspected proceeds of crime could occur through different routes including [player transfers, falsification of ticket sales](#), falsification of services provided or received by high risk commercial sectors, merchandise sales and club or player [sponsorship](#) deals and image rights. Player values in particular are difficult to objectively determine which increases the risk of manipulation for money laundering. There may also be other routes to launder proceeds of crime.
- 6.20 Professional service providers including accountants, lawyers, trust or company service providers and wealth managers are common features in football related transactions so could be exposed to a risk of facilitating money laundering. In many cases these services are employed in-house by clubs, potentially presenting conflict of interests in detecting and reporting suspicious financial activity.
- 6.21 As they are employed in house rather than 'by way of business', many agents and 'fixers' in the sector operate without regulatory supervision, compounding the opportunities and risks of money laundering. [Fees paid to agents, intermediaries and others involved in transactions could be a convenient route by which to launder money or pay bribes](#). This risk is raised when agents represent both player and club during a transaction. Lawyers, accountants, financial service firms and others associated with processing these fees and payments should take all necessary steps to understand their purpose and source to ensure they are legitimate. Due to its hidden nature the scale of criminality in football remains an intelligence gap and difficult to accurately estimate.

# Annexes

## Annex A – Glossary

|         |   |
|---------|---|
| AADJ    | Antiques, Antiquities, Digital Art and Jewellery              |
| ABP     | Alternative Banking Platform                                  |
| ACE     | Asset Confiscation Enforcement                                |
| ACSP    | Authorised Corporate Service Provider                         |
| AML     | Anti- Money Laundering  |
| AMP     | Art Market Participants                                       |
| ASP     | Accountancy Service Provider                                  |
| BVI     | The British Virgin Islands                                    |
| CASP    | Cryptoasset exchange providers and custodian wallet providers |
| CCEW    | The Charity Commission for England and Wales                  |
| CSEW    | Crime Survey for England and Wales                            |
| CD      | Crown Dependency  |
| CDD     | Customer Due Diligence  |
| CFA     | Criminal Finances Act   |
| CH      | Companies House   |
| CIFAS   | Credit Industry Fraud Avoidance System                        |
| CONTEST | Counter-Terrorism Strategy 2023                               |
| COPFS   | Crown Office and Procurator Fiscal Service                    |
| CPS     | Crown Prosecution Service                                     |
| CT      | Counter-Terrorism   |
| CTF     | Counter-Terrorist Financing                                   |

|         |   |
|---------|---|
| CUB     | Chinese Underground Banking                         |
| DeFi    | Decentralised Finance                               |
| DEX     | Decentralised Exchanges                             |
| DR      | Dissident Republican                                |
| EAB     | Estate Agency Business                              |
| ECCT(A) | Economic Crime and Corporate Transparency Act 2023  |
| EDD     | Enhanced Due Diligence                              |
| EMI     | Electronic Money Institution                        |
| ERWT    | Extreme Right-Wing Terrorism                        |
| FATF    | Financial Action Task Force                         |
| FCA     | Financial Conduct Authority                         |
| FCDO    | Foreign, Commonwealth and Development Office        |
| FIS     | HMRC Fraud Investigation Service                    |
| FSMA    | Financial Services and Markets Act 2000             |
| GC      | Gambling Commission                                 |
| GGY     | Gross Gambling Yield                                |
| HMG     | His Majesty's Government                            |
| HMRC    | His Majesty's Revenue and Customs                   |
| HMT     | His Majesty's Treasury                              |
| HVD     | High-Value Dealer                                   |
| IBAN    | International Bank Account Number                   |
| ICN     | International Controller Network                    |
| IOSCO   | International Organisation of Securities Commission |
| IVTS    | Informal Value Transfer System                      |
| JMLIT   | Joint Money Laundering Intelligence Taskforce       |

|        |   |
|--------|---|
| JMLSG  | Joint Money-Laundering Steering Group   |
| KYC    | Know Your Customer  |
| LEA    | Law Enforcement Agency  |
| LSP    | Legal Service Provider  |
| ML     | Money Laundering  |
| MLR    | Money Laundering Regulations  |
| MLTM   | Money Laundering Through Markets  |
| MoRILE | Management of Risk in Law Enforcement   |
| MSB    | Money Service Business  |
| MSHT   | Modern Slavery and Human Trafficking  |
| NCA    | National Crime Agency   |
| NCSC   | National Cyber Security Centre  |
| NDEC   | National Digital Exploitation Centre  |
| NECC   | National Economic Crime Centre  |
| NIRT   | Northern-Ireland Related Terrorism  |
| NOSTRO | The UK bank holds an account in a foreign currency with the overseas correspondent bank |
| NPO    | Non-Profit Organisation   |
| NRA    | National Risk Assessment  |
| NRC    | Non-Remote Casinos  |
| NTFIU  | National Terrorist Financial Investigation Unit   |
| OAC    | Organised Acquisitive Crime   |
| OCG    | Organised Crime Group   |
| OEIC   | Open-Ended Investment Companies   |
| OFSI   | Office of Financial Sanctions Implementation  |

|       |  |
|-------|--|
| OIC   | Organised Immigration Crime                                    |
| OPBAS | Office for Professional Body Anti-Money Laundering Supervision |
| OPR   | Outward Processing Relief                                      |
| OT    | Overseas Territory   |
| OTC   | Over the Counter   |
| OTM   | Out of the Money   |
| PBS   | Professional Body Supervisor                                   |
| PEP   | Politically Exposed Person                                     |
| PIF   | Private Investment Funds                                       |
| PIV   | Private Investment Vehicle                                     |
| PKK   | Kurdistan Workers' Party                                       |
| POCA  | Proceeds of Crime Act 2002                                     |
| PSNI  | Police Service of Northern Ireland                             |
| PSP   | Payment Service Provider                                       |
| PTC   | Private Trust Company  |
| PTF   | Private Trust Foundation                                       |
| P2P   | Peer-to-Peer crypto asset exchanges                            |
| RC    | Remote Casinos   |
| RECU  | Regional Economic Crime Unit                                   |
| ROCU  | Regional Organised Crime Unit                                  |
| ROE   | Register of Overseas Entities                                  |
| SAMLA | Sanctions and Anti-Money Laundering Act 2018                   |
| SAR   | Suspicious Activity Report                                     |
| SIC   | Standard Industrial Classification                             |

|        |   |
|--------|---|
| SME    | Small and Medium-sized Enterprises                              |
| SOC    | Serious Organised Crime   |
| SoF    | Source of Funds   |
| SoW    | Source of Wealth  |
| SPV    | Special Purpose Vehicle   |
| TACT   | Terrorism Act 2000 / 2010                                       |
| TBAMF  | The British Art Market Federation                               |
| TBML   | Trade-Based Money Laundering                                    |
| TCSP   | Trust or Company Service Provider                               |
| TF     | Terrorist Financing   |
| TFPPTG | Terrorist Finance Public-Private Threat Group                   |
| TRS    | Trust Registration Service                                      |
| TSG    | Tri-Sector Group  |
| UHNW   | Ultra High Net Worth  |
| UKFIU  | UK Financial Intelligence Unit                                  |
| UNCTAD | UN Trade and Development  |
| VIBAN  | Virtual International Bank Account Number                       |
| VOSTRO | The overseas correspondent bank holds an account in the UK bank |
| WB     | Western Balkans   |

## Annex B – Legislation, Law Enforcement Agencies, and Supervisors

| Legislation  | Aim   | Changes since the last NRA  |
|--|---|---|
| Proceeds of Crime Act 2002 [Home Office]   | Contains the single set of money laundering offences and civil and criminal confiscation regimes applicable throughout the UK.  | <p>Amendments have been made through the Economic Crime (Transparency and Enforcement) Act 2022 and Economic Crime and Corporate Transparency Act 2023.</p> <ul style="list-style-type: none"> <li>• Reforms to the unexplained wealth order regime</li> <li>• Search, seize and recover criminal or terrorist cryptoassets</li> <li>• Introduction of a failure to prevent fraud offence</li> <li>• Reform of corporate liability law</li> <li>• Introduction of register of overseas entities</li> <li>• Reform of Companies House</li> </ul> <p>Laid a Statutory Instrument to raise the DAML reporting threshold to £3,000.</p> |
| <p>Sanctions and Anti-Money laundering Act 2018 (SAMLA) [FCDO]</p> <p>ii) Counter Terrorism (Sanctions) (EU Exit) Regulations 2019 [HM Treasury]</p> | <p>Provides powers for the UK to impose sanctions for a range of purposes, including compliance with United Nations obligations or other international obligations.</p> <p>Creates a power for the UK to make, amend and appeal regulations relating to AML and CTF activity.</p> <p>ii) Provides the UK with ability to apply sanctions for counter-terrorism purposes to those with a domestic nexus.</p> | <p>SAMLA has been amended by the Economic Crime (Transparency and Enforcement Act) 2022 and Economic Crime and Corporate Transparency Act 2023. Amendments made by the 2022 Act were aimed at streamlining some of its processes, including the processes for making sanctions regulations, designation, reporting, and review. Amendments made by the 2023 Act primarily related to enforcement and director disqualification sanctions.</p> <p>ii) The secondary legislation has been amended to include a travel ban measure and director disqualification.</p>  |

|   |   |   |
|---|---|---|
| <p>Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs) [HM Treasury]</p> | <p>Sets out the high-level requirements on regulated firms to combat money laundering and terrorist financing and ensure that key professionals identify their customers and understand the purpose behind transactions, including the source of funds where necessary.</p>   | <p><b>·2022 Treasury Post Implementation Review:</b> Examined how to make the UK’s future regime more effective, setting updated objectives for the Money Laundering Regulations (MLRs) that focus on partnership between public and private sectors, prioritising real-world effectiveness and the protection of the UK’s financial system, in line with Economic Crime Plan 2.</p> <p><b>·MLRs Statutory Instruments:</b> HM Treasury made several updates to the MLRs in 2022 and 2023, including introducing the FATF Travel Rule for greater transparency in cryptoasset transfers, removing the EU Bank Account Portal requirement, and amending regulations to ensure a proportionate approach to domestic Politically Exposed Persons (PEPs), ensuring the regime remains dynamic and responsive to technological and international developments. HM Treasury is bringing forward a further package of changes aimed at improving the effectiveness of the MLRs following a consultation in 2024.</p> |
| <p>Terrorism Act 2000 (TACT) [Home Office]</p>  | <p>Sets out the primary offences relating to terrorist financing. Contains the definition of ‘terrorist property’ at section 14; the terrorist financing offences at sections 15-18; and includes powers for law enforcement to request disclosure orders, financial information and account monitoring orders.</p> | <p>Amendments have been made to TACT through the Economic Crime and Transparency Act 2023, which amended Section 22B Terrorist Financing: information Orders, and Schedule 6: Financial Information.</p>  |
| <p>Anti-terrorism, Crime and Security Act 2001 [Home Office]</p>  | <p>Schedule 1 contains the powers for law enforcement to be able to seize and detain, or apply to freeze, and forfeit terrorist property. This includes cash, listed assets, funds in accounts, and cryptoassets.</p>   | <p>Amendments to Schedule 1 of ATCSA have been made to allow law enforcement to be able to seize or detain, apply to freeze and forfeit terrorist cryptoassets.</p>   |

| <b>Enforcement agencies</b>                               | <b>Role</b>  |
|---|--|
| National Economic Crime Centre                            | Established in 2018 in the NCA the NECC is a multi agency centre responsible for coordinating and improving the UK's operational response to economic crime. It collaborates with the public and private sectors to understand the threat, direct the response and enhance the system response. It also promotes the use of innovative powers and provides expert evidence on money laundering to UK courts.   |
| National Crime Agency                                     | <p>The NCA is the lead national agency for tackling serious and organised crime. It includes the UKFIU and houses the NECC which are described below.</p> <p>Powers include: intelligence and evidence gathering; cash seizure and forfeiture; restraint and confiscation; and civil recovery and taxation.</p>  |
| UK Financial Intelligence Unit (UKFIU)                    | The UKFIU has national responsibility for receiving, analysing and disseminating intelligence submitted through the Suspicious Activity Reports (SARs) regime, including sharing information with law enforcement agencies at home and internationally. The UKFIU's Terrorist Finance Team receives, identifies, assesses, and exploits information from SARs submitted under both the Terrorism Act and the Proceeds of Crime Act, where a terrorist financing link is identified. These types of SARs include additional sensitivities and are only made available to a restricted group of end users  |
| Intelligence Agencies and Joint Terrorism Analysis Centre | UK intelligence agencies and the Joint Terrorism Analysis Centre are responsible for monitoring and assessing the terrorist threat to the UK and its interests overseas. These agencies are supported by law enforcement.  |
| Crown Prosecution Service (CPS)                           | <p>The principal public agency responsible for prosecuting criminal cases, including money laundering, in England and Wales.</p> <p>The CPS Proceeds of Crime Division has specialist prosecutors dedicated to asset recovery cases (civil and criminal) from restraint/freezing of assets early in an investigation to confiscation and the enforcement of orders, where they can use their prosecutorial powers to ensure orders are paid.</p> <p>The Crown Office and Procurator Fiscal Service (COPFS) is the equivalent authority in Scotland whilst the Public Prosecution Service (PPS) is the principal prosecuting authority in Northern Ireland.</p> |
| Border Force  | Border Force has a unique role in law enforcement anti-money laundering efforts, deterring and preventing the smuggling of illicit cash and listed assets across the UK border. It collaborates closely with various UK and international law enforcement agencies in intelligence development and investigative work.   |

|   |   |
|---|---|
| <p>Serious Fraud Office (SFO)</p>                   | <p>The SFO is an independent government agency responsible for investigating and prosecuting serious or complex fraud, bribery, corruption and associated money laundering in England, Wales, and Northern Ireland. It has a dedicated proceeds of crime division with lawyers and financial investigators handling confiscation investigations, restraint proceedings, money laundering investigations, and civil recovery work.</p>   |
| <p>Office of Financial Sanctions implementation</p> | <p>The Office of Financial Sanctions Implementation (OFSI) is a part of HM Treasury in the UK. Its core mission is to ensure that financial sanctions are properly understood, implemented, and enforced across the UK.</p> <p>In relation to terrorist asset-freezing, proposals for designation under the Sanctions and Anti-Money Laundering Act are made to OFSI by the police, Security Service, or by other government departments or international governments. The investigation of breaches is conducted by the relevant CTIU, with engagement from others including OFSI and the Crown Prosecution Service.</p> |
| <p>His Majesty's Revenue &amp; Customs (HMRC)</p>   | <p>HMRC is the UK's tax, payments and customs authority. HMRC works with independent prosecuting authorities to secure convictions and acts as an MLR supervisor.</p> <p>HMRC's risk and intelligence service collects and develops intelligence on tax-related money laundering risks, sharing insights with domestic and international tax, customs, and law enforcement partners.</p>  |
| <p>Regional organised crime units (ROCUs)</p>       | <p>ROCUs operate across nine policing regions, providing specialist investigative and intelligence capabilities within their respective areas. ROCUs also support the CPS in their civil recovery casework</p> <p>ROCUs act as the primary interface between the NCA and police forces and are accountable to their respective police and crime commissioners.</p> <p>Each ROCU contains a Regional Economic Crime Unit (RECU), which focuses on recovering criminal assets through confiscation and civil powers on behalf of local forces, as well as other agencies like HMRC and the NCA.</p>                         |
| <p>Local police forces</p>                          | <p>All police forces in the UK have a wide mandate to investigate local crime and criminal gangs. Cases investigated by local forces will involve money laundering as a parallel investigation when targeting predicate crimes, as well as standalone ML investigations. There are 43 police forces in England and Wales, each subject to oversight from police and crime commissioners.</p>  |

|   |   |
|---|---|
|   | The City of London Police are the national lead force for economic crime and fraud. The Metropolitan Police Service has the national remit for terrorism and associated financing and has strong economic crime investigation capabilities.   |
| National Terrorist Financial Investigation Unit (NTFIU) | <p>The National Terrorist Financial Investigation Unit is part of the Metropolitan Police Service's Counter Terrorism Command and is the strategic policing lead for Countering Terrorist Financing in the UK. NTFIU primarily investigates the financing of terrorism, whether this is an individual or organisation, and supports other CT investigations which require both financial intelligence and financial disruption activity.</p> <p>Across the UK, there are 10 Counter-Terrorism Financial Investigation Units responsible for investigating terrorist financing activity within their geographical regions, and for supporting other CT investigations which require financial intelligence</p> |
| Police Scotland   | Scotland is served by a single national police service, police Scotland, which is funded by and accountable to the Scottish police authority.   |
| Police Service of Northern Ireland (PSNI)               | Northern Ireland's police force is Police Service of Northern Ireland which is primarily funded by the Northern Ireland Department of Justice and is accountable to the Northern Ireland Policing Board. In addition, the UK Government provides PSNI with additional security funding in recognition of the unique security situation.   |
| Companies House   | Companies House is an executive agency of the <a href="#">Department for Business and Trade</a> . It holds the UK's registers of companies and the Register of Overseas Entities, driving confidence in the economy by creating a transparent and accountable business environment. Companies House data informs business and consumer decisions, supports growth and helps disrupt economic crime. The Economic Crime and Corporate Transparency Act, which came into force in March 2024, represents a fundamental shift in the role of Companies House, from being a collector of information to becoming an active gatekeeper of the accuracy and integrity of information on the registers.              |
| Insolvency Service                                      | The Insolvency Service is a UK government agency and an executive agency of the Department for Business and Trade. Its primary role is to support economic confidence by helping individuals and businesses in financial distress, tackling financial wrongdoing, and ensuring fair outcomes for creditors.   |

| <b>Statutory supervisors</b> |   |
|------------------------------|---|
| Financial Conduct Authority  | <p>Supervises financial services firms and virtual asset service providers in the UK. The sectors which the FCA regulates include:</p> <ul style="list-style-type: none"> <li>• Retail banking</li> <li>• Wholesale financial market</li> </ul> |

|   |  |
|---|--|
|   | <ul style="list-style-type: none"> <li>• Investment management</li> <li>• General insurance and protection</li> <li>• Retail lending</li> <li>• Retail investments</li> <li>• Pensions and retirement income</li> </ul> <p>Powers: supervisory and enforcement under the MLRs and wider financial services regulations.</p>  |
| HMRC  | <p>Supervises estate agency businesses, letting agency businesses, art market participants, high value dealers, money service businesses, bill payment service providers, telecommunications, digital and IT payment services, trust and company service providers who are not supervised by the FCA or PBSs, and accountancy service providers who are not supervised by one of the accountancy PBSs.</p> <p>Powers: Civil and criminal enforcement under MLRs and other HMRC powers.</p>               |
| Gambling Commission   | <p>Supervises for all online (remote) and land-based (non-remote) casinos operating in Great Britain or providing casino facilities to British customers. The Gambling Commission is also the regulator for other gambling businesses operating in Great Britain or providing gambling services to British customers, including betting, lotteries, bingo, and arcades.</p> <p>Powers: Licence revocation, fines, AML/CTF oversight.</p>   |
| <b>Approved professional bodies</b>   |  |
| <p>Overseen by the office for Professional Body Anti-Money Laundering Supervision (OPBAS). Consists of 22 regulated bodies responsible for the supervision of the legal and accountancy sectors</p> |  |
| Legal sector  | <ul style="list-style-type: none"> <li>• BSB (Bar Standards Board - General Council of the Bar)</li> <li>• CILEx (Chartered Institute of Legal Executives)</li> <li>• CLC (Council for Licensed Conveyancers)</li> <li>• Faculty of Advocates</li> <li>• Faculty Office of the Archbishop of Canterbury</li> <li>• General Council of the Bar Northern Ireland</li> <li>• Law Society of Northern Ireland</li> <li>• Law Society of Scotland</li> <li>• SRA (Solicitors Regulation Authority)</li> </ul> |
| Accountancy   | <ul style="list-style-type: none"> <li>• AAT (Association of Accounting Technicians)</li> <li>• ACCA (Association of Chartered Certified Accountants)</li> <li>• AIA (Association of International Accountants)</li> <li>• ATT (Association of Taxation Technicians)</li> <li>• CIMA (Chartered Institute of Management Accountants)</li> <li>• CIOT (Chartered Institute Of Taxation)</li> <li>• IAB (Institute of Accountants and Bookkeepers)</li> </ul>  |

|  |  |
|--|--|
|  | <ul style="list-style-type: none"> <li>• ICAEW (Institute of Chartered Accountants in England and Wales)</li> <li>• ICAI (Institute of Chartered Accountants in Ireland)</li> <li>• ICAS (Institute of Chartered Accountants of Scotland)</li> <li>• ICB (Institute of Certified Bookkeepers)</li> <li>• IFA (Institute of Financial Accountants)</li> <li>• IPA (Insolvency Practitioners Association)</li> </ul> |
| <b>Additional supervisory bodies</b>         |  |
| The Charity Commission for England and Wales | A non-ministerial government department that registers and regulates charities in England and Wales. It has specific powers to protect and redirect charitable funds, remove or disqualify trustees and direct dissolution of charities if abused.   |
| Office of the Scottish Charity Regulator     | A non-ministerial office responsible for the registration and regulation of charities in Scotland. Its role is to identify and investigate apparent misconduct in the administration of charities.   |
| Charity Commission for Northern Ireland      | 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.  |

## Annex C – Diagrams

### Money Laundering: Visualising ML Flows

Not all funds will be spent immediately so funds will often be stored. This can involve use of bank accounts, safety deposit boxes, crypto cold storage and financial investments that mature over several years. High value goods also associated with criminal lifestyle purchases can also be used as a long term store of value.

**Re-vestment into criminality**

This involves goods or services purchased with criminal funds to support further criminal activity. For example: renting property to grow cannabis, conceal modern slavery, purchasing of boats to smuggle illicit commodities or traffic people, or transferring funds to a supply chain to pay for illicit commodities.

**Storing Funds**

Involves purchase of high value goods for purpose of enjoying criminal a luxury lifestyle. Where the value of the asset is maintained goods could be used as a long term store of value or liquidated in order to release funds or relauder. Includes gold, jewellery, watches, property, art, furniture, cars, yachts.

**Generating Funds**

**Moving and concealing funds**

**Criminal Lifestyle**

**Spending Funds**

**Reputation Laundering**

**Criminal Lifestyle services**

Money Laundering starts after funds are generated from crime, within or outside the UK. Different volumes, frequency, asset types, legitimate market trends and goals of the criminal may impact the laundering of funds. Whilst some forms of money laundering are often associated with specific crimes, it is not the sole determining factor for how money is subsequently laundered. Key predicate offences that impact the UK include:

- fraud, and cybercrime
- drug and acquisitive offending
- OIC, MSHT, and CSEA
- tax crimes, corruption and sanctions evasion
- environmental crime

The process by which the value of funds is either moved, or transformed in order to conceal its criminal origin. At its simplest it involves a single step complex schemes are split, mixed and layered. Key typologies include:

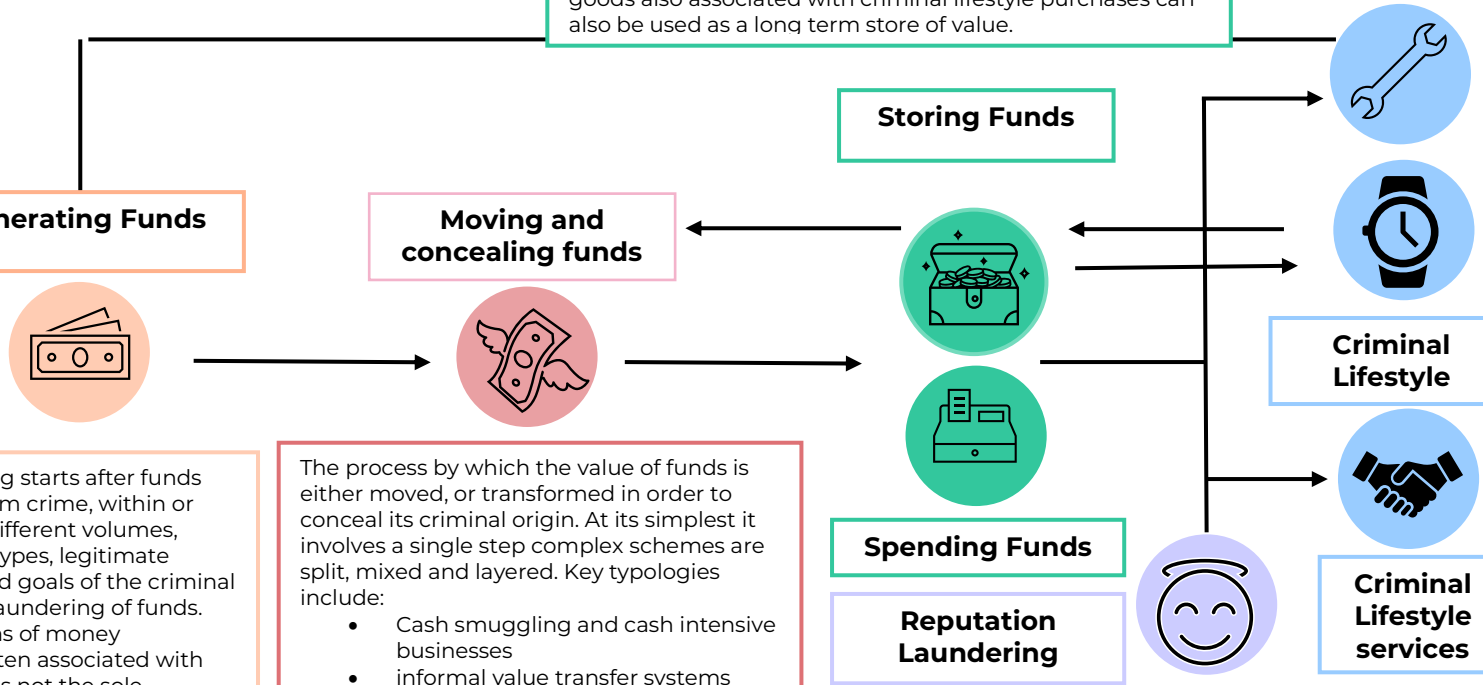
- Cash smuggling and cash intensive businesses
- informal value transfer systems
- trade based money laundering
- use company or trust structures
- Use of commercial and residential property
- movement of funds into different crypto currencies
- use of professional enablers.

Various sectors, including those that are regulated, play a critical role as gatekeepers

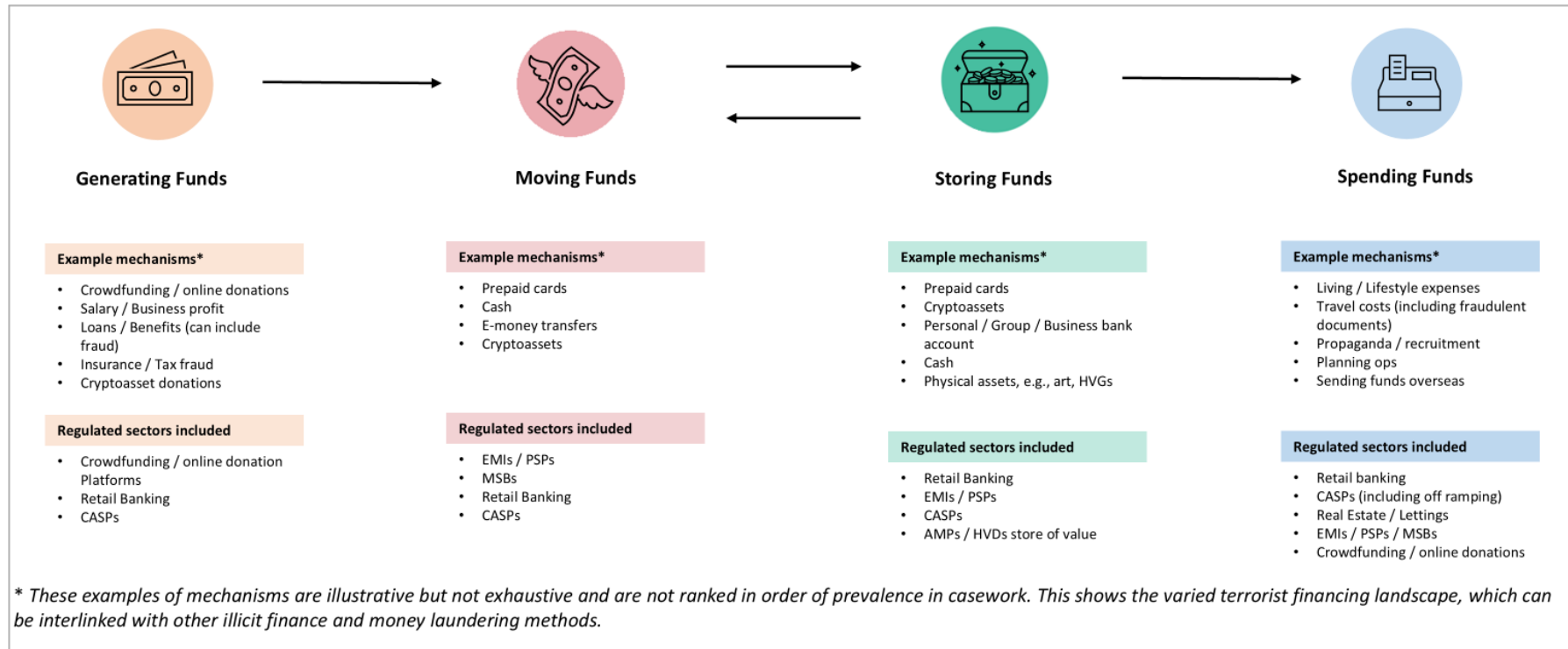
**Communities:** donations (foodbanks) and investment in local infrastructure (e.g. local sports clubs). Wins hearts and minds of communities. Benefits criminal as communities may refuse to cooperate with police or used as a recruitment tool

**Elite:** donations to cultural institutions (museums), civic institutions (universities), private schools enrolments, political donations.. Result is to legitimise the criminal and allow access to the both political and cultural elites of chosen domiciles

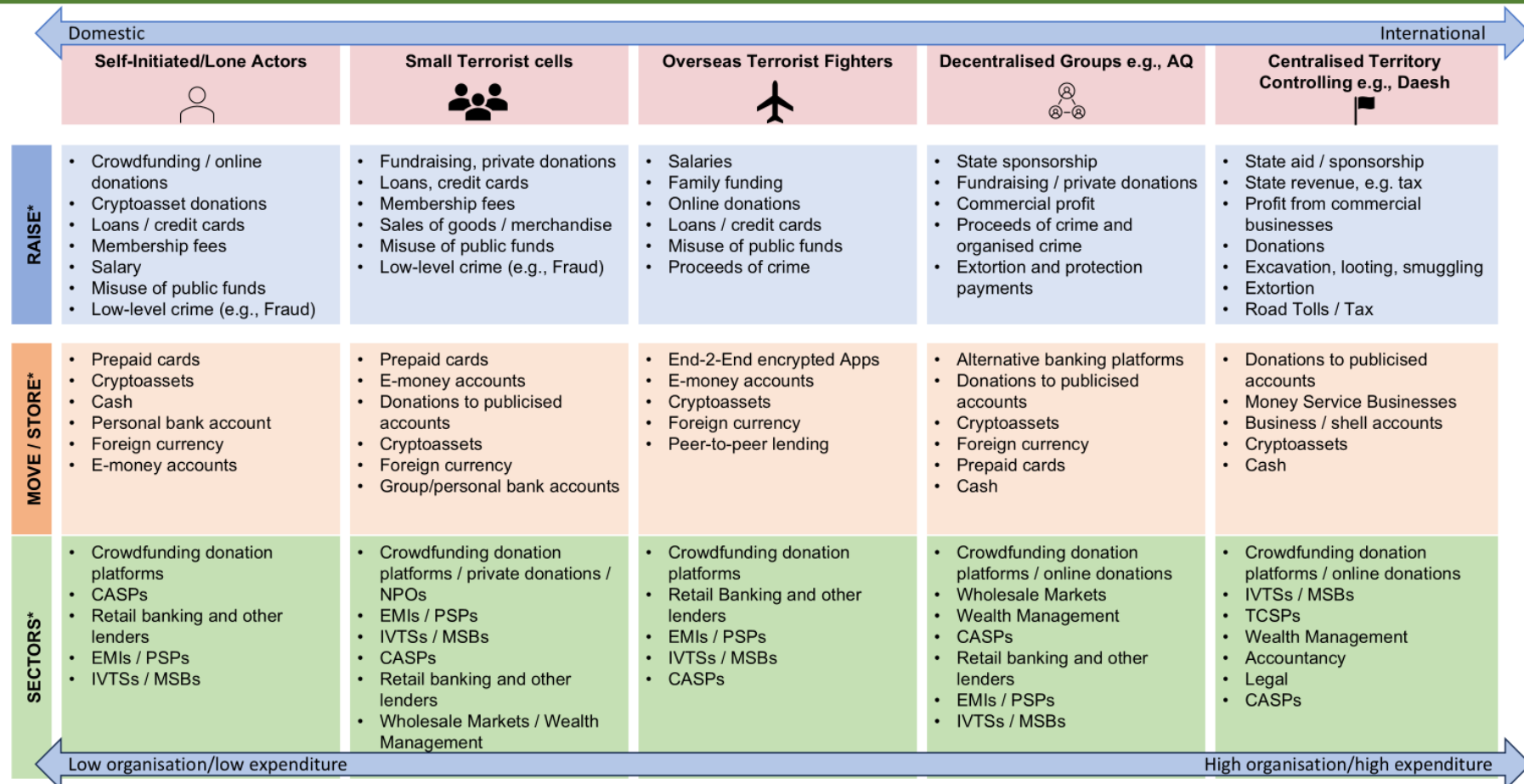
**Information:** PR agencies, Private security firms, litigation/SLAPP lawsuits, or citizenship by investment schemes. Benefits in controlling information (negative and positive) and can make it difficult for regulated sectors (via adverse media CDD) and law enforcement (through whistleblowers to investigative journalists) to identify criminality.



## Terrorist Financing: Visualising TF flows



# Terrorist Financing: Visualising the threat from TF in the UK



\* These examples of mechanisms are illustrative but not exhaustive and are not ranked in order of prevalence in casework. This shows the varied terrorist financing landscape, which can be interlinked with other illicit finance and money laundering methods.

## **Annex D - Boxes**

### Section 1

Box 1.A System Prioritisation

### Section 2

Box 2.A – UK AML/CFT System

Box 2.B – Economic Crime Plan 2

### Section 3

Box 3.A – UK Money Laundering Flows

Box 3.B – Politically Exposed Persons (PEPs)

Box 3.C - System Prioritisation

Box 3.D - Case study: Operation Machinize

Box 3.E - Case study: Post Office Money laundering conviction

Box 3.F - International controller networks

Box 3.G - Case study: safe custody services

Box 3.H - Notable forms of IVTS

Box 3.I- IVTS flows

Box 3.J - Case Study: Trade Based Money Laundering scheme

Box 3.K - Case study: PEPs

Box 3.L - Case study: Use of property to launder funds

Box 3.M – Case Study: Operation Hammerhead

### Section 4

Box 4.A – Examples of terrorist financing mechanisms.

Box 4.B - Case Study: COVID bounce back loans

Box 4.C - Case Study: Payments via an MSB

Box 4.D – Terrorist financing mechanisms by type of terrorist.

Box 4.E - Case study: Demonstrating terrorist financing through different ideologies/groups

### Section 5

Box 5.A – MoRiLE methodology

Box 5.B - Risk Scores

Box 5.C - Electronic Money Institutions & Payment Services Annual Payments Value Table (as reported by firms)

Box 5.D - Case study: use of ViBANs

Box 5.E – Case Study: Crypto ATMs

Box 5.F - Case study: Unregistered MSB

Box 5.G - Case study: Bansky artwork

Box 5.H - Case Study: SYUK

Box 5.I - Case Study: Tarek Namouz

Box 5.J - Case Study: property purchase

Box 5.K - Case Study: Tipping off

Box 5.L - Case Study: Farooq

Box 5.M - Case Study: TCSP and accountancy services

Box 5.N – Case Study: TCSP fined for failing to identify beneficial owners

### **HM Treasury contacts**

This document can be downloaded from [www.gov.uk](http://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](mailto:public.enquiries@hmtreasury.gov.uk)

