System Priorities - 2025

The UK's response to economic crime is a collaborative effort and partnership with the private sector is essential to prevent, identify and disrupt the financing of organised crime. To support public private collaboration, and under a commitment made in the Economic Crime Plan 2, the National Crime Agency (NCA) and the Financial Conduct Authority (FCA), Home Office and Treasury have worked in partnership to agree the following system priorities and make them available to the regulated sector. This work has been conducted with the close support of representatives of the financial sector through UK Finance.

These Priorities are aligned to the both the National Risk Assessment (NRA) and NCA National Strategic Assessment (NSA) and are intended, with the full endorsement of the FCA, to support the regulated sector in allocating resources to where they can have the most impact on the threat, on a cost-neutral basis while maintaining their regulatory responsibilities.

UK Law Enforcement has a well-developed model for understanding the scale of Serious & Organised Crime threats and setting threat Priorities. Public Private Partnership structures (such as the JMLIT) have aided the application of these for the private sector, but they have not been communicated as a list of priorities directly before. All Priorities are considered to be equal and are not ranked. Each Priority is provided with a definition, set of suggested actions and links to further information.

The only predicate offences listed in these priorities are those which fall within the definition of economic crime, such as; Fraud, Sanctions Evasion or Terrorist Financing. The priorities focused on money laundering typologies will apply to all possible predicate offences including, but not limited to; Organised Immigration Crime, Drugs and Firearms offences, and Human Trafficking.

The governance of these priorities will be the responsibility of a newly created public-private System Prioritisation Governance Group (SPGG). For further detail on the priorities or the concept of System Prioritisation the project team can be contacted at SystemPrioritisation@nca.gov.uk. Otherwise please continue to look to guidance from UKFIU and the FCA, or your relevant regulator, for any changes resulting from this process.

01.	Economic Crime & Sanctions Evasion facilitated by UK-based or UK-registered **Professional Enablers**, particularly evasion of sanctions linked to the Russian invasion of Ukraine
02.	Transaction flows and corporate structures associated with the abuse of power by overseas **Politically Exposed Persons** (PEPs)
03.	Protecting the public by creating a **cryptoasset** ecosystem that is increasingly resilient to criminal abuse
04.	**Criminal cash** consolidation, cross-border movement and deposit into the UK banking system (including via the Post Office)
05.	**Money laundering** in the UK or through UK corporate structures on behalf of the OCGs with links to **priority Jurisdictions** including, Albania, China, Russia, and the UAE. This includes the activity of International Controller Networks and Underground Banking
06.	**Fraud perpetrated by international offenders** against victims in the UK, including OCGs with links to criminality in **priority Jurisdictions** including, Ghana, Nigeria, India and Southeast Asia (with a focus on Cambodia, Laos and Myanmar)
07.	The exploitation of **money mules** by mule herders running networks to obfuscate the origin, movement and cashing out of the proceeds of crime, often Fraud, as well as for other purposes, including the financing of terrorism
08.	Tackling the significant percentage of the value of frauds in the UK which originate from a **telecommunications service or online platforms**
09.	The financing of **terrorist** attacks or plots in the UK, or individuals or groups engaged in attack planning or propagating terrorist ideology.

Economic Crime & Sanctions Evasion facilitated by UK-based or UK-registered Professional Enablers, particularly evasion of sanctions linked to the Russian invasion of Ukraine

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 play a fundamental role in the ability of serious, organised criminals to disguise criminal assets and launder the proceeds of crime through the UK economy. Russian aggression in Ukraine is enabled by the elites who control Russia's economic interests. Designated Persons (DPs) are using a range of techniques in order to evade sanctions impacting on their personal and commercial holdings.

Example Public Private Partnership Actions:

- Support the identification of complicit and/or non-compliant PEs operating in and/or impacting the UK in order to effectively direct operational and supervisory activity.
- Enhance the understanding of the most significant PEs impacting the UK, how they are recruited, enabling services and behaviours, and which sectors are most exposed.
- Identify sectors and services exposed to the greatest risk to enable prevent-style outreach and engagement and understand customer populations which may include PEs.
- Identify and map professional enablers of direct/indirect high-risk customers and refer any potential professional enablers to the NCA
- Review customers at high risk of providing services to DPs and refer any potentially suspicious activity to the NCA, as well as through public private partnership fora.
- Improve public-private investigations of front company networks to deepen our understanding of sanctions evasion networks, involving Russia but also Iran and DPRK, to inform future sanctions strategy.

Sources and Further Detail:

2025 NCA National Strategic Assessment (NSA), Cross System Professional Enablers Strategy, 0697-NECC Financial Sanctions Evasion Russian Elites and Enablers

Transaction flows and corporate structures associated with the abuse of power by overseas Politically Exposed Persons (PEPs)

Individuals in jurisdictions outside the UK who are or have been entrusted with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials. This can also include professional and non-professional enablers of the abuse of power. Non-professional enablers can include family members, particularly children, spouses, ex-spouses and in-laws, as well as associates. Please refer to the Section 35 of the Money Laundering Regulations 2017 for further detail.

Example Public Private Partnership Actions:

- Support the NCA's international anti-corruption efforts through suspicious activity referrals and public private collaboration efforts.
- Identify risk factors associated with UK enablers of bribery and corruption and factor these into onboarding and due diligence processes.
- Members of the UK legal, private banking, accountancy, wealth management, company service providers and family office sectors are uniquely placed to enhance our collective understanding of the threats and risks of PEPs and other corrupt elites.
- Proactively refer cases of overseas PEP bribery solicitation involving your company to the NCA International Corruption Unit, either on an intelligence basis or as a witness to an offence, going beyond legal requirements on mandatory self-reporting

Sources and Further Detail:

OFSI Financial Services Threat assessment February 2025

How to contact the NCA International Corruption Unit

Protecting the public by creating a cryptoasset ecosystem that is increasingly resilient to criminal abuse

Illicit entities seek to utilise crypto-assets and supporting technology to transfer proceeds of crime originating from fraud related schemes, ransomware, sanctions evasion and other activities, across jurisdictions. Cryptocurrencies are considered to offer anonymising and obfuscation capabilities that provide opportunities for illicit actors to integrate such funds into the global financial system. The use of Cryptocurrencies for terrorist financing purposes is a known typology used across jurisdictions to support international terrorist activity. Reporting confirms organised criminal use of crypto to support criminal operating models which, along with other factors, reduces public confidence in the sector.

Example Public Private Partnership Actions:

- Work with UK law enforcement to identify and embed awareness of risk factors indicative of illicit crypto activity / share data sets to create a fuller intelligence picture for both public and private bodies to protect the public/ the legitimacy of crypto within the financial system.
- Engagement across regulated sectors to identify proceeds of crime and potential victim funds tied to illicit crypto activity. Collecting and sharing indicators of suspected fraudulent activity such as fraudulent Initial Coin Offerings or Rugpulls (where developers abandon a project after raising assets, leaving participants with worthless tokens).
- Develop communications campaigns across public / private networks to increase awareness of fraud & money laundering risks associated with crypto-assets, including contributing to public communications campaigns for both users of cryptocurrencies and the wider population. Establish critical processes for the freezing and restraint of suspect funds held on VASP platforms.
- Develop and enhance existing engagement groups and forums to share and enhance the understanding of cryptocurrency use for terrorist financing purposes. Identify those sectors and services exposed to the greatest risk to enable prevent-style outreach and engagement.

Sources and Further Detail:

2025 NCA National Strategic Assessment (NSA)

Criminal cash consolidation, cross-border movement and deposit into the UK banking system (including via the Post Office)

It's estimated that over £12 billion of this is generated from criminal enterprises in the UK every year, the majority of which is believed to come from illicit drugs and excise fraud, but can include the full range of predicate offences including Organised Immigration Crime, where the collection and movement of cash is an integral part of the criminal business model, as well as terrorist financing. OCGs continue to use a range of businesses, including those on UK Highstreets as well as Post Office branches to launder the proceeds of crime.

Example Public Private Partnership Actions:

- Develop an end-to-end understanding of how criminals are laundering criminal cash in the UK, including which stakeholders are involved, how criminal gangs are operating, what indicators of activity can be identified and where the biggest opportunities to intervene and prevent/disrupt activity are.
- Build the joint understanding of the typical methods used by criminals to launder criminal cash in the UK, identifies the relevant stakeholders in the chain and the intervention/collaboration opportunities.
- Identification of the priority changes that could be made to private sectors systems and controls to better prevent and disrupt criminal cash being laundered in the UK
- Increase the flow of intelligence between key cash depositing environments and financial sector to help inform financial crime controls such as KYC, customer reviews and transaction monitoring. This type of sharing will also help to identify key information to be used to help focus and target disruption activity.

Sources and Further Detail:

2025 NCA National Strategic Assessment (NSA),

FCA – Cash Based Money Laundering

Money laundering in the UK or through UK corporate structures on behalf of the OCGs with links to priority Jurisdictions including, Albania, China, Russia, and the UAE. This includes the activity of International Controller Networks and Underground Banking

The UK economy, its institutions and the corporate registration system are undermined by International Organised Criminal Groups (OCGs) laundering their illicit finances to hide their illegal activity. Russian-language OCGs are responsible for many high-profile cybercrime attacks against the UK, laundering their proceeds through a variety of mechanisms. International Controllers exploit international financial centres such as the UAE to provide money laundering services through global Informal Value Transfer Systems (IVTS) for OCGs involved in activity including; Organised Immigration Crime, drugs trafficking, terrorism and state threats. Chinese Underground Banking (CUB) is a form of IVTS, common within the Chinese community in the UK and many other countries. The scale of Albania-linked criminality the associated cash smuggling and money laundering from this activity is significant.

Example Public Private Partnership Actions:

- Development of an international funds flow data framework.
- Exploring options to target and disincentivise Overseas Criminal Gangs use of the UK financial system
- Consider the expansion of private-to-private sector intelligence sharing through the system in relation to identified international ML threats.
- Supporting the identification of identified international networks operating in the UK, targeting victims in the UK or exploiting the UK financial sector. Exploring options for the return or repatriation of proceeds of crime from these networks.

Sources and Further Detail:

2025 NCA National Strategic Assessment (NSA)

Fraud perpetrated by international offenders against victims in the UK, including OCGs with links to criminality in priority Jurisdictions including, Ghana, Nigeria, India and Southeast Asia (with a focus on Cambodia, Laos and Myanmar)

It is assessed that over 70% of the fraud perpetrated against UK citizens or businesses emanates from, or is facilitated via, overseas jurisdictions. The regions stated above being those posing the most significant level of threat, particularly in relation to high-harm frauds, including Investment Fraud, Romance Fraud and Payment Diversion Fraud.

Example Public Private Partnership Actions:

- Development of a framework for the identification and trend sharing on emerging/changing Jurisdictions of Risk for Fraud impacting on the UK.
- Continue to utilise and expand how reported data can be shared between public and private across JoR threats.
- Identify which systems, legislation, recruitment routes, and geographic hotspots JoR-linked networks are exploiting in furtherance of their criminality.

Sources and Further Detail:

2025 NCA National Strategic Assessment (NSA)

The exploitation of money mules by mule herders running networks to obfuscate the origin, movement and cashing out of the proceeds of crime, often Fraud, as well as for other purposes, including the financing of terrorism

Bank accounts used by criminals (either without the holder's knowledge or with their knowledge with varying degrees of culpability) to store & transfer illicit funds to other accounts, often very quickly, helping to hide the dirty money and to make it available as required for criminal purposes. Money mule networks play a significant and growing role in enabling fraud. In 2022, banks identified over 39,000 accounts indicative of mule activity.

Example Public Private Partnership Actions:

- Collaborate to build the understanding of the methodologies being utilised to recruit money mules and to cash out funds moved through mule accounts.
- Consider how communications and awareness initiatives to customers/the public could be improved as part of an aligned approach, along with the development of customer treatment strategies.
- Work towards an agreed industry methodology and data-sharing model focusing on mules and mule herders.

Sources and Further Detail:

Tackling fraud and rebuilding trust

Tackling the significant percentage of the value of frauds in the UK which originate from a telecommunications service or online platforms

Telecommunication and technology companies provide infrastructure and services which are increasingly being targeted and exploited by criminals for the purposes of fraud, including Courier Fraud. This includes frauds which are enabled by social media personalities promoting financial products or advice, so called ‘Finfluencers’. Funds generated from fraud are used for personal gain as well as enabling further criminality including the financing of terrorism. This also means these companies are well placed to

Example Public Private Partnership Actions:

- Assist in the identification and targeting of financial flows and system vulnerabilities associated with the abuse of telecoms & online platforms for fraud.
- Continue to fulfil commitments made under the Telecommunications Charter and Online Fraud Charters, and continue to make ambitious commitments in the refreshed Charters
- There is significant opportunity to learn more through more strategic and tactical intelligence sharing between Law Enforcement, banks, telecommunications & technology companies and the regulator.

Sources and Further Detail:

Experiences of fraud online and through calls and texts - Ofcom

Online scams and fraud research: summary report

The financing of terrorist attacks or plots in the UK, or individuals or groups engaged in attack planning or propagating terrorist ideology.

An individual, group or organisation that provides money or other property to finance terrorism, including for the purposes of planning attacks, or for the benefit of a proscribed organisation would be committing a terrorist financing offence (sections 15-18 of the Terrorism Act 2000). Terrorist financiers play a fundamental role in maintaining terrorist organisations, by spreading their ideologies and recruiting new members. In the UK terrorist financing is generally for the individual's own purposes, such as to fund travel or for living expenses, and they will utilise methods, such as cryptoassets, Money Service Businesses, Electronic Money Institutions and crowdfunding donation-based platforms, to help to hide their legitimate or illicit funding flows for terrorist causes.

Example Public Private Partnership Actions:

- Improve the collective understanding of what constitutes terrorist financing behaviour through ongoing support in enhanced TACT SAR reporting, to enable effective operational and supervisory activity.
- Identify the terrorist financing commonalities in the regulated sectors through the provision of recent case studies and, where required, bring them into scope of the public private partnership fora.
- Work with UK law enforcement to identify terrorist financing activity indicators and share these with financial institutions through higher classification public private partnership reading rooms, to help improve understanding of the terrorist financing threat picture.
- Continue to identify those legislative and regulatory gaps within which terrorist financing behaviour takes place and work with both HMG and UK law enforcement to develop proposals to close these gaps.
- Continue to identify prevalent and emerging terrorist financing threats and vulnerabilities to develop focussed, collaborative opportunities for disruption and mitigation through public private partnership activity.

Sources and Further Detail:

0720-NECC Alert Upstream Terrorist Financing Risks and Typologies (Available to JMLIT members)

0723-NECC Potential Vulnerabilities for Terrorist Financing and other Illicit Finance Behaviours Following the Taleban Takeover of Afghanistan (Available to JMLIT members)