Home Office

Call for Evidence:
Economic Crime Information Sharing

This consultation begins on 9 March 2026

This consultation ends on 18 May 2026

About this consultation

To:	This Call for Evidence is open to the public, with a particular focus on organisations and individuals across the public and private sectors who play a role in detecting, preventing, investigating, or disrupting economic crime in the United Kingdom.
Duration:	From 9 March 2026 to 18 May 2026
Responses and enquiries (including requests for the paper in an alternative format) to:	The Smart Survey link is the preferred method of receiving feedback. If feedback can only be provided by paper, please send responses to: Economic Crime Information Sharing Call for Evidence, Homeland Security Group, 6th Floor, Peel Building, Home Office, 2 Marsham Street, London, SW1P 4DF Please direct any questions to **ecinformationsharingcfe@homeoffice.gov.uk**

Contents

Glossary

AI – Artificial Intelligence

AML – Anti-money laundering

AMLA – EU Authority for Anti-Money Laundering and Countering the Financing of Terrorism

API – Application Programming Interface

CCA 2013 - Crime and Courts Act 2013

CD – Communications data

CFA 2017 – Criminal Finances Act 2017

CTF – Counterterrorism Financing

DATF – Defence Against Terrorist Financing Suspicious Activity Report

DAML – Defence Against Money Laundering Suspicious Activity Report

DEA 2017 – Digital Economy Act 2017

DPA 2018 – Data Protection Act 2018

DUAA 2025 – Data Use and Access Act 2025

ECCTA 2023 – Economic Crime and Corporate Transparency Act 2023

FATF – Financial Action Taskforce

FIUs – Financial Intelligence Units

ICO – Information Commissioner's Office

IPA 2016 – Investigatory Powers Act 2016

JMLIT – Joint Money Laundering Intelligence Taskforce

MLA – Mutual Legal Assistance

MLRs – Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2027

NCA – National Crime Agency

POCA 2002 – Proceeds of Crime Act 2002

PPPs – Public-private partnerships

SAR/SARs – Suspicious Activity Report

SDS – SARs Digital Service

SOC – Serious and Organised Crime

UK GDPR – United Kingdom General Data Protection Regulation

UKFIU – United Kingdom Financial Intelligence Unit

Introduction

1. **Economic crime poses a significant threat to our national security and to the prosperity of the UK.** To effectively prevent, investigate and recover the proceeds of economic crime – including fraud, money laundering, and corruption – law enforcement, prosecutors, regulators, other public bodies and private sector entities must have access to the right information at the right time.

2. As we accelerate into a 'Data Age', the volume, variety and strategic value of information is increasing exponentially. **Criminals are adapting quickly, using personal data, digital platforms, and emerging technologies to commit economic crime at scale.** To effectively address criminal activity, both the Government and the private sector must capitalise on access to, and exploitation of, information on criminal activity. This requires clear understanding of the legal environment, including upholding data privacy, whilst taking decisive action to utilise the information available and leverage data as a strategic resource to create actionable intelligence for impactful, disruptive outcomes.

3. **Tackling economic crime is the shared responsibility of Government, law enforcement, regulators and the private sector and requires close collaboration.** The Home Office and UK Finance committed in Economic Crime Plan 2[1] to producing an Economic Crime Data Strategy to enhance the exploitation of available data across the ecosystem. Public-private and private cross-sector cooperation is critical to this response and effective information sharing is the key enabler of that cooperation. Where information from the private sector can provide the critical indicators for law enforcement to build a network view of criminal activity for enforcement and recovery action, law enforcement insights and risk alerts can support the private sector in putting robust controls in place for preventative action. This disrupts criminality from occurring, protects consumers and builds economic resilience.

[1] https://www.gov.uk/government/publications/economic-crime-plan-2023-to-2026

The current economic crime information sharing system

4. **Economic crime information sharing operates within a complex legal and governance framework that balances the need for effective crime prevention with the protection of individual privacy and confidentiality to keep customers and their data safe.** The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) regulate the processing of personal data, including where necessary to tackle all forms of economic crime, including fraud, money laundering and corruption. The legislation requires that data sharing is necessary, proportionate, and supported by a lawful basis for processing under Article 6 of the UK GDPR. There are stricter conditions for sensitive personal data in Article 9 of the UK, but Schedule 1 to the Data Protection Act 2018 makes it clear that processing of such data is permitted where necessary to prevent or detect an unlawful act for reasons of substantial public interest. Building on this, the Data Use and Access Act 2025 ('DUAA 2025') introduced a new lawful basis under Article 6 of the UK GDPR to encourage the processing of personal data for "recognised legitimate interests". Processing that is necessary for detecting, investigating, or preventing crime is one such interest, as is making disclosures to public bodies on request where necessary to help them deliver their public functions.

5. Meanwhile, case law on economic crime has developed to support the sharing of customer information with law enforcement for specific purposes. Tournier v National Provincial and Union Bank of England (1924) set a precedence on rules related to customer confidentiality and financial institutions, creating four instances where confidentiality could be overridden (compelled by law, if there is a public duty, if it's necessary for the bank's own interest and if there is customer consent). While this sets rules for financial institutions, it does not apply to any other private sector entities that could hold critical indicators of economic crime activity.

6. Government has specifically introduced measures compelling regulated entities to provide information on money laundering and terrorist financing. The Suspicious Activity Reporting (SAR) provisions in the Proceeds of Crime Act 2002 (POCA 2002) and Terrorism Act 2000 alert law enforcement to potential instances of money laundering and terrorist financing. This has resulted in a large number of reports - 866,616 in the 2025 reporting year - to the UK Financial Intelligence Unit (UKFIU) on

suspected money laundering or terrorist financing activity.[2] The provisions create a failure to disclose offence for those in the regulated sector who fail to report suspicions or knowledge of money laundering and terrorist financing activity to the UKFIU. There is no offence for failure to report outside of the regulated sector.

7. In addition to the SARs regime, over the last decade the National Crime Agency (NCA) has leveraged Section 7 of the Crime and Courts Act 2013 (CCA 2013) which governs information sharing to and from the NCA, to pioneer new public-private partnerships (PPPs) to combat money laundering and wider economic crime. Since its launch in 2015, the UK's Joint Money Laundering Investigations Taskforce (JMLIT) has evolved into a multi-layered capability that now includes Public Private Threat Groups and time-limited cells that address specific economic crimes. More recently, also underpinned by Section 7 of the CCA, the NCA, and financial sector partners have created a dynamic data-led arm to PPP that integrates banking data with law enforcement data to target poly-criminality, known as Data Fusion. In addition to its use in money laundering, Section 7 of the CCA applies to the full range of Serious and Organised Crime (SOC) threats including in fraud-related contexts.

8. Simultaneously, there have been advancements in private-private information sharing. The Economic Crime and Corporate Transparency Act 2023 (ECCTA 2023) provided clarity and comfort to the AML regulated firms that in prescribed circumstances AML regulated firms can share customer information between themselves for the purposes of preventing, detecting, or investigating economic crime, without fear of breaching confidentiality or incurring civil liability.

9. Within the telecoms sector, Government also launched in November 2025 the new Telecoms Fraud Charter which involves mobile network operators sharing data and intelligence responsibly with each other and with law enforcement to prevent fraud and protect consumer fraud.[3] This involves cooperation from the tech and banking industry to ensure there is a holistic and unified approach to tackle fraud.

[2] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/786-sars-annual-report-2025/file
[3] https://www.gov.uk/government/publications/fraud-sector-charter-telecommunications

Challenges of the economic crime information sharing system

10. **Despite progress in establishing legal gateways and operational mechanisms, the UK's economic crime information sharing system remains a complex patchwork of general frameworks and more targeted information sharing gateways.** While these mechanisms enable information sharing in principle, in practice they are often underutilised or inconsistently applied. This is due to:
    - Complexity due to fragmented laws and regulations requiring system clarity
    - Operational challenges in sharing information requiring enhanced capabilities
    - Lack of confidence and cultural appetite in using the existing gateways

Complexity due to fragmented legal system

11. The sheer number of laws and regulations, ranging from organisation-specific gateways, legal obligations and case law, alongside broader privacy and confidentiality frameworks, is vast. This can make even the process of navigating which information can be shared with whom time consuming and costly to operate in practice. This complexity can build up reactive behaviours like overcompliance and defensive reporting which diverts resources away from core activities.

Operational challenges to sharing information

12. Operational challenges also hinder the effectiveness of the current system. At a systemic level, the scale and diversity of stakeholders involved contributes significantly to the complexity of the current information sharing landscape. There are over 250 organisations enabled by POCA 2002 that have the authority to request information from the private sector, including over 90,000 regulated entities. The absence of standardised data formats and interoperable systems has led to a reliance on bespoke bilateral arrangements that are often inefficient and resource intensive. There is little clarity or consensus on what types of data should be prioritised for collection and sharing. Many organisations lack the capability to assess the relative value of the information they hold or to triage it effectively.

13. Meanwhile, organisations assess their data protection obligations and risks differently, resulting in an inconsistent approach of what can be shared under different powers. This creates a fragmented ecosystem which is particularly problematic given that economic crimes span multiple sectors and industries. This fragmentation increases

the cost and complexity of participation, particularly for smaller organisations, and limits the scalability of information sharing efforts to create actionable intelligence.

14. There is also no clear system leader with an identifiable authority on information sharing for economic crime purposes and confusion over roles and responsibilities further drives fragmentation. This leads to duplication and, inevitably missed opportunities, with data initiatives often working in siloes.

Lack of confidence in using the existing gateways

15. Hesitancy to share can also be due to wider considerations. Despite interventions in the information-sharing system such as ECCTA 2023 and amendments to UK GDPR and to the DPA 2018, there remains a culture of caution, where concerns about privacy, reputational harm, regulatory scrutiny and actions of civil liability deter organisations from sharing information even when legal gateways are available. Where there is no established history of collaboration, scepticism about motives and benefits can also inhibit sharing.

16. Risk aversion is often shaped by the differing levels of legal protection and clarity available across sectors. For instance, the AML-regulated sectors benefit from legal safeguards under ECCTA 2023 but there are currently no equivalent legal protections or disapplication of liability provisions for non-AML-regulated sectors. As a result, sectors such as technology platforms, telecommunications providers and online marketplaces often face greater uncertainty and risk when considering whether to share information. In the absence of clear safeguards, there can be caution around sharing such information.

17. Together, these legal, operational and cultural barriers create a system in which information sharing is technically possible in most circumstances but is practically constrained. Addressing these challenges will require building a coherent and confident approach to data sharing, underpinned by legal clarity, operational alignment and a shared understanding of risk and responsibility across all sectors.

The Call for Evidence

18. **This Call for Evidence seeks input from stakeholders across the public, private, and third sectors, on how information is currently shared to tackle economic crime specifically, and how it could be improved.** It focuses on identifying legal, operational, and cultural barriers to effective data sharing, as well as opportunities to strengthen the system through reform. The scope of this project will look at information sharing in relation to any economic crime activity including fraud, money laundering, corruption and asset recovery which is likely to be interchangeable with information shared on the underlying offences to money laundering such as drug offences.

19. **This Call for Evidence will support work to build a public-private Data Strategy as well as other Economic Crime Plan 2 initiatives such as System Prioritisation.** It also delivers a commitment in the Fraud Strategy and responds to **a recommendation Jonathan Fisher KC is considering in Part Two of the Independent Review of Disclosure and Fraud Offences to review the data sharing landscape.**

20. **This Call for Evidence marks the beginning of a strategic effort to reform the UK's information-sharing framework for economic crime,** to inform future policy development and make any required improvements to the legal and operational framework for economic crime information sharing. This will support and enable both the public and private sectors to share critical information in a timely manner, improving the monitoring and mapping of illicit financial flows, our collective understanding of economic crime threats, analysis of economic crime risks and disruption of criminal activity to protect the public and maintain the integrity of the financial system.

Chapter 1: Private-Private Information Sharing

21. **A robust response to economic crime is dependent on the private sector being effectively equipped with access to information on key indicators of economic crime behaviour.**

22. This requires timely and effective information sharing between themselves and other private sector organisations, within and cross-sectors. This not only allows a private sector entity to build their own information picture on a suspected criminal's behaviour and escalate it to law enforcement, regulators or prosecutors but also allows them to take their own preventative action to protect consumers and disrupt economic crime networks.

23. This section seeks views on what economic crime-related private to private information sharing currently occurs, what barriers exist, and how the system could be improved to support more confident and effective collaboration across sectors.

Economic Crime and Corporate Transparency Act 2023

24. In addition to data protection obligations, private sector entities must also consider their duties to customers – particularly those relating to confidentiality – when sharing information to combat economic crime. Historically, the absence of clear statutory protections created uncertainty around whether disclosing customer information on criminal activity could expose firms to civil claims, including in relation to breach of contract or negligence. This legal ambiguity had a chilling effect on information sharing, discouraging firms from collaborating even where it is in their interest.

25. To address this, ECCTA 2023 permits private sector businesses regulated under the Money Laundering Regulations (MLRs) to share customer information directly with each other to prevent, detect, or investigate economic crime. ECCTA 2023 removes the risk of breaching confidentiality or civil liability for these disclosures. These

provisions do not exempt an organisation from complying with UK GDPR. Regulated businesses under the MLRs can directly share information under two conditions:

a. Warning condition: If a firm is taking action to safeguard against a customer due to concerns about economic crime risk, even if the customer is not yet onboarded.
b. Request condition: If a firm believes another regulated firm under the MLRs holds information about its customer, and that sharing the information may help in preventing or investigating economic crime.

26. For the following businesses within the AML-regulated sector, ECCTA 2023 also provides similar protections when – under the warning condition only – they engage in the indirect sharing of customer information through a third-party intermediary:
    - deposit taking bodies
    - electronic money institutions and payment institutions
    - cryptoassets exchange providers and custodian wallet providers
    - large or very large law firms
    - large or very large accountancy firms
    - large or very large insolvency practitioners
    - large or very large auditors, and
    - large or very large tax advisers

27. Since the powers came into force, sectors have been considering how best to embed the new provisions. This has involved development of general guidance, sector specific guidance, piloting the use of the provisions and the development of a strategic vision to maximise use of these provisions. Anecdotal feedback that we have received so far is that use of the direct sharing power – particularly the warning condition – is increasing as firms grow more familiar with the legislation, but the use of the indirect sharing power remains low. Additionally, we understand that when information has been shared, there have been varying approaches to formatting and standardising the data, as well as differing views on the mechanisms that can and should be used for sharing. This has led to an inconsistent approach being applied across industry.

28. ECCTA 2023 holds immense potential for private-private sharing for detecting and disrupting economic crime without the involvement of law enforcement. Government would like to realise the full potential of this by identifying its challenges and gathering

suggestions for scaling up its use and application across multiple sectors. In particular, we are interested in views on whether there would be merit for the provisions to be expanded to non-AML regulated sectors who currently cannot benefit from the provisions.

Criminal Finances Act 2017

29. Prior to ECCTA 2023, section 11 of the Criminal Finances Act 2017 (CFA 2017) was introduced to allow businesses in the AML-regulated sector to share information with each other when they suspect that a transaction may involve criminal property and where the purpose is to help decide whether to file a SAR to the NCA**.** Before information is shared, the NCA (in practice the UKFIU) must be notified. A joint disclosure report – or 'Super SAR' – can then be made to the NCA in respect of a suspicion of money laundering made on behalf of two or more entities.

30. While the CFA 2017's ambition was to incentivise private-private sharing ahead of reporting to the UKFIU on suspicion, it is our understanding that the use of the Super SAR model is low which is primarily due to the NCA notification requirements. With the ECCTA 2023 provisions now in force, the private-private sharing benefits of using section 11 arguably have been reduced. However, there would still appear to be value in the mechanism to facilitate the reporting of joint SARs. The Government would therefore like to improve its understanding and identify any barriers that may be limiting the use of the Super SAR model, determine if there is still utility in the Super SAR tool and whether the Super SAR could, or should, be made more effective.

Private-Private Questions (for private sector only)

When answering all questions, please be descriptive of legal, operational and cultural factors related to the sharing of information.

Question 1: Economic Crime and Corporate Transparency Act 2023

1.1. Please describe your experience of sharing or receiving information with other private sector organisations using section 188 and 189 of the Economic Crime and Corporate Transparency Act 2023?

1.2. How could Government better support organisations to share information with one another using section 188 and 189 of the Economic Crime and Corporate Transparency Act 2023?

1.3. Should, if any, improvements be made to section 188 and 189 of the Economic Crime and Corporate Transparency Act 2023?

1.4. Should more organisations be added to section 188 and/or 189 Economic Crime and Corporate Transparency Act 2023 and, if so, who?

1.5. Should new offences be added to Schedule 11 of the Economic Crime and Corporate Transparency Act 2023 and, if so, which?

Question 2: Criminal Finances Act 2017

2.1. Please describe your experience of sharing or receiving information with other private sector organisations for economic crime purposes using Section 11 of the CFA 2017?

2.2. Please describe your perspective on the role of the Section 11 of the CFA 2017 information-sharing provisions now that Sections 189 and 199 of the Economic Crime and Corporate Transparency Act 2023 are in force?

2.3. Should, if any, improvements be made to Section 11 of the CFA 2017?

Question 3: General private-private sharing questions

3.1. Please describe your experiences of applying the Data Protection Act 2018 and UK GDPR when sharing or receiving information with other private sector organisations for economic crime purposes?

3.2. Please describe the impact that the Data (Use and Access Act) 2025 will have on how organisations share or receive information with other private sector organisations for economic crime purposes?

3.3. How else could Government better support private-private information sharing for economic crime purposes?

Chapter 2: Private-Public Information Sharing

31. **To effectively prevent, investigate and disrupt economic crime, it is essential that routes for the private sector to share information with law enforcement, regulators and prosecutors are both legally clear and operationally viable.**

32. This means receiving the right information at the right time and in a clear format that law enforcement, regulators and prosecutors can act immediately or utilise multiple data sources to build a wider intelligence picture. This is not just to support criminal investigations and proceedings, but also to inform the utilisation of other powers such as asset recovery including civil recovery, regulatory action and civil orders such as Serious Crime Prevention Orders in the High Court. Likewise, tactical intelligence sharing as well as crime typologies and risk alerts issued by law enforcement and the wider public sector enables the private sector to strengthen controls, detect suspicious activity earlier, and collaborate effectively to block criminal networks and illicit financial flows.

33. Given the pervasive nature of economic crime and the volume of intelligence held by the private sector to support its prevention, specific legal obligations and gateways have been created to share information between the private and public. These fall under two general types:
    a. Public sector-initiated private-public information sharing
    b. Private sector- led disclosures to comply with a legal obligation or voluntary use of a legal gateway.

34. This chapter explores the current public-private pathways, seeking views on their effectiveness and opportunities to strengthen collaboration between the public and private sector through information sharing gateways and the use of new technologies.

Public sector-led requests, disclosures and orders

Pre-order enquiries

35. Law enforcement and other public sector agencies may seek information from private sector businesses through voluntary gateways and mechanisms. For example, law enforcement or prosecuting agencies may contact financial institutions within the regulated sector via the Financial Intelligence Gateway to obtain basic information. The Financial Intelligence Gateway list also provides financial institutions with a mechanism to confirm they are only dealing with trained and accredited financial investigators who understand and acknowledge the sensitive nature of the material being requested, along with how to handle it.

36. The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) regulate the processing of personal data. The sharing of data by competent authorities is governed by Part 2 of the DPA that allows a competent authority to share information for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security

37. Sharing information can also be on a voluntary basis under principles established in case law referred to as the ‘Tournier rules’. Tournier v National Provincial and Union Bank of England (1924) established that the implied duty of confidentiality between a bank and its customer does not apply where the sharing of information is under the compulsion of law or where there is a duty to the public to disclose information, including cases involving the prevention or detection of crime. Enquiries undertaken through this route tend to be quite specific, and information acquired through this route can be used for intelligence purposes only.

38. Law enforcement can also send pre-order enquiries to validate information in advance of a Production Order (discussed further in paragraph 37). The scope of pre-order enquiries tends to be more limited as it seeks to confirm if material is held and give notice of the production order prior to submitting an application to the courts.

Crime and Courts Act 2013

39. A pivotal gateway for the NCA to voluntarily request information from other organisations, including private sector bodies, is Section 7 of the CCA. Information requested can be for any of the purposes of the NCA's functions, including economic crime investigation and disruption. Information disclosed to the NCA can then be disclosed to another party for the purpose of the NCA's functions, meaning information can be shared with other agencies and public bodies. Section 7 forms the legal basis for the bulk of AML public-private information sharing activity with the NCA through JMLIT's public-private cells. Under Part 7 of POCA, the UKFIU can apply for an Information Order which is a specialist intelligence power to compel information from AML regulated businesses regarding suspected money laundering.

Investigatory Powers Act 2016 and relevant amendments

40. The Investigatory Powers Act 2016 (IPA 2016) provides a framework for the use and oversight of investigatory powers by law enforcement, intelligence agencies and other public authorities. Part 3 of the IPA 2016 sets out the circumstances for communications data (CD) acquisition, including the statutory purposes it can be acquired for. CD provides information on the who, where, when and how of a communication and is vital for detecting fraud and money laundering. An authorisation under Part 3 of the IPA 2016 is not available for all types of asset recovery investigations (for example, where the purpose of the investigation is depriving criminals of the benefit of their crimes). The Investigatory Powers (Amendment) Act 2024 made targeted reforms to the IPA 2016 to keep pace with emerging threats and technologies. The Home Office published revised codes of practice to guide the use of these powers, ensuring understanding of the changes and application of appropriate safeguards.[4]

41. Since the introduction of the IPA 2016 and its relevant amendments, the Home Office has received feedback that challenges remain on what constitutes communications data from financial institutions. The Home Office has since developed and provided guidance for financial institutions. The Government is seeking views on how the IPA 2016 is currently used to support economic crime investigations, and whether further

[4] https://www.gov.uk/government/collections/investigatory-powers-act-codes-of-practice

clarification or reform may be needed to improve its effectiveness in both fraud and money laundering contexts.

Proceeds of Crime Act 2002

42. The private sector can also be compelled to provide information by court order. Evidence obtained through these orders often provides vital information to progress criminal investigations and asset recovery proceedings. Part 8 of POCA 2002[5] provides law enforcement agencies with powers to compel individuals and organisations to provide information for economic crime investigations, including money laundering investigations and asset recovery investigations. These powers take the form of a wide range of Orders which are made by the Court including Production Orders, Disclosure Orders, Unexplained Wealth Orders, Customer Information Orders and Account Monitoring Orders. Codes of Practice[6] have been produced to guide law enforcement officers in the exercise of their functions when conducting such investigations and requesting information. More recently, in September 2025, the Home Office issued a circular to ensure consistency in the use of disclosure orders[7].

43. There are various conditions and thresholds that must be met before Orders are granted. There is a statutory requirement that there must be reasonable grounds for believing that the material or information is likely to be of substantial value by itself or to the investigation. The appropriate officer must be satisfied that the material or information will progress the investigation.

44. In advance of applying for a formal Order through the Court, law enforcement may utilise some of the other information sharing options and undertake pre-order enquiries. As set out in the relevant codes of practice, law enforcement should use these to build the intelligence picture and ensure that a formal Order would be appropriate and proportionate. These requests are often made for information to be provided for prevention, investigation, detection or prosecution of criminal offences. If the information is requested from a private sector organisation, the Information

[5] Proceeds of Crime Act 2002

[6] Draft code of practice issued under section 377 of the Proceeds of Crime Act 2002

[7] Circular 006/2025: Disclosure Orders (Proceeds of Crime Act 2002) - GOV.UK

Commissioner's Office (ICO) has published guidance on sharing with law enforcement bodies ('competent authorities').[8]

45. This Call for Evidence seeks views on the experiences of sending and receiving information using the various POCA 2002 court orders and whether there could be suggested improvements for their operation. We invite views on all or specific orders in Part 8 of POCA 2002.

Private sector-led disclosures

Crime and Courts Act 2013

46. Section 7 of the CCA can also be used by private sector entities to voluntarily disclose information to the NCA for the purpose of any of the NCA's functions. This has supported public-private partnerships including high value intelligence gathering through analysis of large-scale financial datasets with the financial sector through Data Fusion.

Suspicious Activity Reports

47. A SAR is a required disclosure under sections 330 and 331 of POCA 2002 (or section 21A of the Terrorism Act 2000), obliging businesses in the regulated sector to report knowledge or suspicion of money laundering or terrorist financing to the NCA. Failure to submit a SAR when required is a criminal offence. By contrast, a Defence Against Money Laundering (DAML) or Defence Against Terrorist Financing (TAFT) SAR is an authorised disclosure under section 338 of POCA 2002 (or section 21ZA of the Terrorism Act 2000), allowing a person who suspects that property they intend to deal with is criminal to seek "appropriate consent" from the NCA. This consent provides a statutory defence against committing one of the principal money laundering or terrorist financing offences (sections 327–329 in POCA 2002; sections 15-18 of the Terrorist Act 2000) when carrying out the specified act. In short, SARs fulfil a mandatory reporting duty on persons operating in the regulated sector, while DAMLs or DATFs can provide a statutory defence for reporters wishing to proceed with a transaction that might otherwise constitute a money laundering or terrorist financing offence

[8] Sharing personal data with law enforcement authorities | ICO

48. To ensure the SARs regime remains effective, agile and minimises adverse consequences on reporters and customers, the Government has kept the regime under regular review and made several improvements since its inception. The UK Anti-Corruption Plan in December 2014 committed to carrying out a review of the SARs regime which ran in 2015. The findings from this Call for Evidence[9] centred on poor feedback, lack of clarity on reporting thresholds and limited use of SARs intelligence, calling for clearer guidance and stronger collaboration.

49. In 2017, the Law Commission was commissioned by the Home Office to undertake an independent review into parts of the UK's anti-money laundering and terrorist financing regimes. Specifically, the Law Commission were asked to consider whether there is scope, within the existing legislative framework, for reform of the DAML regime. The Law Commission's report[10] published in June 2019 made fifteen recommendations for reform including introducing guidance and clarity on aspects of the regime. The Government responded to these recommendations in 2024.[11]

50. In 2023, via the Economic Crime and Corporate Transparency Act 2023, the Government also introduced a series of reporting exemptions from the principal money laundering offences intended to reduce the number of low-value reports in the system and the burden on reporters.[12] In July 2025, the Government then increased the threshold below which certain regulated businesses can carry out certain transactions without submitting a DAML SAR to £3,000 to continue to make the regime more effective. No such exemption applies for DATFs.

51. Outside of legislative reform, the Home Office established the SARs Reform Programme in 2019 to introduce new guidance, recruit more staff in the UKFIU and Regional Organised Crime Units to increase exploitation of SARs, and replace the legacy IT systems underpinning the SARs regime with the SARs Digital Service (SDS). This new service has already delivered an online portal to streamline SAR submissions

[9] https://assets.publishing.service.gov.uk/media/5a807761ed915d74e33fa970/6-2118-Action_Plan_for_Anti-Money_Laundering__web_.pdf

[10] Anti-money laundering – Law Commission

[11] Response to Law Commission review of the SARs regime - GOV.UK

[12] Guidance on the exemptions from the money laundering obligations and money laundering reporting obligations in the Proceeds of Crime Act 2002 - GOV.UK

and an Application Programming Interface (API) for high-volume SAR reporting. The next stage of the reform will focus on the continued rollout of the SDS for UKFIU and law enforcement users.

52. These reforms have made important and necessary changes to improve the operation of the regime and to the UKFIU's capacity and capability. However, with the growth of new technologies, including automation and analytical capabilities, alongside the continued high volume of SARs and the burden this continues to place on the public and private sector, the Government would like to understand how the SARs regime can remain effective and responsive to the threat, whilst minimising negative impacts. This includes exploring whether additional legislative changes are needed, in particular whether changes to the suspicion threshold in POCA 2002 would keep the system focussed on the most meaningful intelligence and reduce burdens on the public and private sector.

53. Additionally, Government has also received feedback from industry about duplicative reporting requirements on businesses. For example, there can be duplication in reporting suspicious fraudulent activity as a SAR report and also to Report Fraud, while in relation to sanctions businesses can have to make SAR reports as well as separate reports to the Office of Financial Sanctions Implementation within HM Treasury. The Government would welcome views on whether and how these duplicative reporting requirements could be minimised as part of the response.

54. More broadly, with public-private partnership work between law enforcement and the private sector – such as JMLIT and the NCA-financial sector Data Fusion project – now expanding into mature financial intelligence capabilities, the Government would also welcome views on whether the SAR regime should be tightened to focus on where it provides unique value.

Private-public questions (for all)

Question 4: Financial intelligence gateway and pre-order enquiries

4.1. Please describe your experience of sharing or receiving information via the Financial Intelligence Gateway, or in pre-order enquiries in advance of a production order, for economic crime purposes?

4.2. Could Government introduce improvements to the way information is shared via the Financial Intelligence Gateway or in pre-order enquiries in advance of a Production Order?

Question 5: Proceeds of Crime Act 2002 Part 8

5.1. Please describe your experience of sharing or receiving information in response to a Part 8 Proceeds of Crime Act 2002 Order (Production Orders, Disclosure Orders, Unexplained Wealth Orders, Customer Information Orders and Account Monitoring Orders)? Please feel able to comment on all or specific orders.

5.2. Please consider how Government could improve or better support sharing of information in response to a Part 8 Order (Production Orders, Disclosure Orders, Unexplained Wealth Orders, Customer Information Orders and Account Monitoring Orders)? Please feel able to comment on all or specific orders.

Question 6: Crime and Courts Act 2013

6.1. Please describe your experience of sharing or receiving information with the NCA using Section 7 of the Crime and Courts Act 2013?

6.2. Should a similar gateway to Section 7 of the Crime and Courts Act 2013 be available to other public bodies and, if so, which public bodies?

Question 7: Suspicious Activity Reporting

7.1. Noting recent improvements to the Suspicious Activity Reporting regime, please describe your current experiences of sharing or receiving information through Suspicious Activity Reporting in Part 7 of the Proceeds of Crime Act 2002?

7.2. What further changes, if any, could be made to the Suspicious Activity Reporting regime to make it more effective in delivering its objective to provide high value intelligence to law enforcement?

7.3. With the growth of public-private partnerships and real-time data sharing such as Data Fusion, please describe your perspective on the role, utility and value-add of the Suspicious Activity Reporting regime?

7.4. What benefits or risks, if any, would there be to changing the suspicion threshold to 'reasonable grounds to suspect' in the Suspicious Activity Reporting regime and would you support this change?

Question 8: Investigatory Powers Act 2016 and related amendments

8.1. Please describe your experience of acquiring or sharing communications data under the Investigatory Powers Act 2016, including any related amendments, for economic crime purposes?

8.2. Please consider how Government could improve or better support the acquisition of communications data under the Investigatory Powers Act 2016, including any related amendments, for economic crime purposes?

Question 9: General public-private sharing questions

9.1. Please describe your experiences of applying the Data Protection Act 2018 and UK GDPR when sharing information or receiving information owned by the private sector with law enforcement for economic crime purposes?

9.2. Please consider how else Government could better support information-sharing between public and private bodies for economic crime purposes?

Chapter 3: Public-Public Information Sharing

55. **An effective public sector response to economic crime relies on seamless collaboration between agencies. Law enforcement, regulators, prosecutors and other public bodies each have visibility of different information depending on their jurisdiction or access to powers.**

56. As a result, building an intelligence picture can be a lengthy and resource-intensive process for individual organisations, often requiring separate requests or formal agreements to access information, along with training, accreditation, and acquisition of licenses. Organisations can also take different interpretations of the same legal gateway.

57. With no intentional design, the legal framework within the public sector to share information is also a patchwork of different powers. This can make it complex to navigate, particularly for organisations and forces who do not have broad legal gateways designed for their functions. In general terms, there is no unconditional power to share information within the public sector for economic crime purposes. Before considering whether there are any restrictions on data sharing, a public body must have a power to share data. The processing of personal data by competent authorities for the purpose of preventing, investigating and detecting crime is under the DPA 2018. If you are a competent authority, and the sharing is to another competent authority for law enforcement purposes, then Part 3 of the DPA should provide a framework allowing you to share data. In practice, information sharing agreements and memorandums of understanding are usually established between organisations.

58. Some organisations have their own legal frameworks for information-sharing to support their operation. Alongside the NCA and Section 7 of the CCA, HMRC have extensive information-sharing powers to support their function[13] and, more specially, have a legal gateway to support their proceeds of crime function in Section 85 of the Serious Crime

[13] Sections 17, 18 and 20 of Commissioner for Revenue and Customs Act 2005

Act 2007.[14] However, to date, the Criminal Assets Bureau Northern Ireland is the only public body included in that legal gateway with HMRC. ECCTA 2023 also gave greater data-sharing powers to Companies House which means, among other things, that Companies House will proactively be able to share any suppressed and protected information with law enforcement agencies if deemed proportionate and necessary.

59. Similarly, AML/CTF supervisors can share and receive information with other authorities where the information relates to their supervisory functions under Regulation 52 of the MLRs. This supports the supervisor to build information and take effective supervisory action although this provision is limited to which organisations can share and receive information with the supervisor. Government would like to understand whether the scope of Regulation 52 is correct and if any other authorities should be included in the information sharing provisions under the Regulation.

60. To better understand the public sector landscape for all information-sharing (beyond economic crime), the Government commissioned the Law Commission in 2013 to review the national and European framework for information sharing between public bodies. In July 2014, the Law Commission published its findings as part of a Scoping Report[15] that made a recommendation to conduct full review as the next phase of work.

61. In response to the report, the Government created the Digital Economy Act 2017 (DEA 2017) to improve the infrastructure of information sharing between public bodies by creating broad legal gateways. Rather than being agency specific, the DEA allows for the disclosure of information between a range of public bodies for specific purposes. This has recently included a broad gateway to share information in instances where there is debt against the public sector. A similar approach could be employed for economic crime with a broad gateway similar to the DEA 2017. This call for evidence seeks to understand the appetite for, value and risks of a broad gateway.

Private-public questions (public sector only)

Question 10: General public-public information sharing questions

10.1. Should Regulation 52 of the MLRs be amended to include any other public bodies?

[14] Section 85 of the Serious Crime Act 2007

[15] https://assets.publishing.service.gov.uk/media/5a747bfded915d0e8bf18a9b/41831_HC_505_Law_Commission_351_Web.pdf

10.2. What impact would a broad legal gateway such as the Digital Economy Act 2017 have on public-public information-sharing?

10.3. How else could Government improve or better support the sharing of information within the public sector for economic crime purposes?

Chapter 4: Cross-Border Information Sharing

62. **Economic crime is increasingly transnational. A robust economic crime response relies on the frameworks for sharing information across borders to be clear and easily accessible.**

63. Criminal networks exploit global financial systems, international trade, and digital technologies to evade taxes, commit fraud across jurisdictions and launder the funds of criminality across borders. The speed with which criminals can move funds through the financial system means that the ability to trace and secure assets degrades significantly over time. Systems designed for ease of use by the consumer, provide the sophisticated criminal with the opportunity to lay complex trails. Funds transferred overseas, particularly via the banking system, are often dissipated quickly within the foreign jurisdictions.

64. Tackling these threats requires a coordinated international response. However, this can be a considerable undertaking given the UK must not only have the law and capability to share information but the law of the corresponding country must also allow for information to be shared. Sharing is also subject to the availability of the appropriate resources, local legislation and the political will to assist. Where some countries are open to cooperating cross-border, some countries lack fundamental capabilities to enable such activity. For example, they may lack transparency in beneficial ownership information, may not have central property registers, or their wider AML frameworks make cross-border cooperation difficult.

65. Recognising this, international bodies are increasingly acknowledging the need to collaborate across borders to detect, prevent and disrupt economic crime and the Financial Action Taskforce (FATF) has identified effective information sharing as central to a well-functioning AML/CTF framework".[16]

[16] https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Consolidated-FATF-Standards-information sharing.pdf.coredownload.inline.pdf

66. In the UK, cross-border data sharing is underpinned by the UK GDPR and the DPA 2018. Together, they govern the conditions under which personal data can be transferred to third countries or international organisations. Chapter V of the UK GDPR outlines the conditions for lawful international transfers which include standard contractual clauses, or binding corporate rules, to ensure the protection of individuals' rights. The DPA 2018 has a similar framework, outlining the routes for lawful international transfers by competent authorities for law enforcement purposes. The ICO provides detailed guidance on international transfers, including tools such as the International Data Transfer Agreement and the UK Addendum to the EU Standard Contractual Clauses, which help organisations comply with data protection law when sharing data across-borders.

67. Despite the existence of legal frameworks and international standards, cross-border information sharing remains operationally complex. The UK's cross-border information sharing framework mirrors its domestic structure, relying on a combination of international agreements and domestic legal gateways with cross-border applicability. While this provides a coherent and legally sound basis for cooperation, it is not always interoperable with other jurisdictions. Differences in legal regimes, regulatory frameworks, and differing national appetites to share data can limit the practical effectiveness of UK mechanisms when applied internationally. These structural challenges are compounded by practical barriers. Variations in technical data infrastructures within countries may hinder the interoperability of datasets.

68. Meeting data standards, handling ancillary issues (e.g. handling subject access requests or other data requests such as correction or deletion), and preparing data for sharing can place a significant burden on the resources of the sending institution. This includes increased workload for data management and compliance teams, the need for specialised software and tools, potential delays in other operational activities, and the allocation of additional personnel time and expertise to ensure data quality and regulatory compliance before sharing.

69. As with domestic sharing, cross-border economic crime information sharing can be categorised into public–public, public–private, and private–private arrangements. Each presents distinct legal and operational considerations, and stakeholders are invited to

respond to Government on how these mechanisms are currently used and where improvements may be needed.

Public-public cross-border information sharing

70. Historically, public-public information sharing has operated through the Mutual Legal Assistance (MLA) framework, underpinned by Mutual Legal Assistance Treaties (MLATs).[17] These treaties apply to all types of criminal investigations, enabling law enforcement agencies to request assistance on matters such as locating suspects, freezing assets, conducting searches, and gathering testimony. While applicable to all crimes, they are frequently used in fraud and economic crime investigations, particularly where evidence or assets are held overseas. In recent years, there is the perception that the MLAT system has struggled to keep pace. This is largely due to the increase in globalised data flows and the expansion of cloud-based services and data storage, particularly in cases where data is stored in United States (US) cloud servers. Meanwhile, many telecommunications entities operate under US jurisdiction where legal restrictions prevent them from sharing certain types of data directly with foreign governments. As a result, UK authorities must rely on complex MLA processes to access critical information, which can delay investigations and increase harm to victims.

71. On asset recovery specifically, Part 11 of POCA 2002 (Co-operation) creates the scheme for the UK to provide assistance to other countries for POCA 2002 purposes, where property and evidence is in the UK. There are similar provisions in POCA 2002 for the UK to make requests to other countries in relation to property and evidence located abroad relating to a domestic case. The provisions provide a basis for some information sharing with international partners to achieve transnational law enforcement objectives. Additional to POCA 2002 is the ability to make financial intelligence enquiries. However, initial anecdotal findings show that these routes are likely to be less widely known by law enforcement despite many asset recovery cases having an extraterritorial element.

[17] Mutual legal assistance - GOV.UK

72. As data governance becomes increasingly fragmented across jurisdictions, the UK must consider how to maintain effective access to digital evidence while safeguarding privacy, legal certainty, and investigative agility. This includes evaluating the adequacy of existing agreements and exploring new bilateral or multilateral arrangements to support economic crime including fraud enforcement. The MLA structure is reinforced in specific crime areas through international conventions such as the Budapest Convention on Cybercrime and the United Nations Convention Against Corruption, both of which promote the adoption of effective MLA practices relevant to cyber-enabled fraud and corruption.

73. Underpinning the broader framework, multinational organisations are established to promote and govern cross-border sharing on economic crime. The Egmont Group facilitates intelligence exchange between national FIUs via a secure platform, enabling the tracing of illicit flows, identification of criminal networks, and disruption of their operations. To improve sharing in real time, Europol's Secure Information Exchange Network Application (SIENA) is a web-based platform designed for secure and efficient cross-border information sharing between law enforcement agencies within the EU member states and third parties which the UK has membership to.

74. Section 7 of the CCA supports outbound and inbound international information-sharing. This enables the UKFIU to exchange SARs and financial intelligence with foreign FIUs through the Egmont Group secure platform. This is particularly relevant in money laundering investigations, provided data protection and international cooperation standards are met. It also supports the NCA hosting the International Anti-Corruption Coordination Centre, launched in 2016, which pioneered global collaboration of law enforcement agencies targeting grand corruption.

75. More recently, the new EU Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA) will facilitate the secure exchange of information between FIUs across the EU by coordinating the operational activities of member FIUs, promoting best practices, harmonising investigative techniques and encouraging cross-border information sharing between FIUs. AMLA is expected to become operational in

2027.[18] The UK is not a member state but will need to build a strong relationship with AMLA to foster cross-border sharing.

Public-private cross-border information sharing

76. Public-private partnerships are also essential at the international level to unlock information on cross-border criminal networks. Section 7 of the CCA largely forms the basis of cross-border public-private partnerships established by the NCA, with private sector information being fed cross-border through JMLIT cells.

77. Additionally, bilateral and multilateral agreements are made between countries to share information for specific purposes, and operational groups are established for public-private cross-border purposes. Europol's Financial Intelligence Public-Private Partnership (EFIPPP) creates a secure and efficient platform for sharing information between law enforcement agencies, FIUs, and regulated financial institutions. These groups focus on building a cross-border intelligence picture to understand the economic crime risks and risk indicators faced by multiple jurisdictions.

78. The UK-US Data Access Agreement is a critical tool for UK law enforcement and intelligence agencies in the context of accessing data held in the US. The Agreement, which came into force in 2022, ensures that UK authorities can submit requests for the content of communications directly to communications service providers, including social media platforms and messaging services, located in the United States. The Agreement's impact has been transformative, ensuring our intelligence agencies and law enforcement have access to more data, more quickly than ever before to support the prevention, detection, investigation and prosecution of serious crime, including fraud and money laundering. Serious crime is defined under the Agreement as an offence that is punishable by a maximum term of imprisonment of at least three years. The Home Office will continue to work closely with operational partners over the coming years to maximise the benefits that the Agreement provides.

[18] Homepage - Authority for Anti-Money Laundering and Countering the Financing of Terrorism

Private-private cross-border information sharing

79. Cross-border private-to-private information sharing in the context of economic crime is often constrained by a complex interplay of legal, operational, and institutional factors. Internal policies may prioritise the protection of commercially sensitive information and client confidentiality over voluntary crime fighting objectives. Balancing robust data protection with the need for information sharing remains a key challenge, particularly where the private sector may be concerned around intellectual property theft, competition law and other legal risk.

80. UK domestic legislation does provide some support for cross-border sharing, particularly in the AML context. The MLRs create an environment that supports cross-border sharing by requiring regulated entities to conduct due diligence and maintain records that can be shared with overseas counterparts under appropriate legal frameworks. Regulation 20 of the MLRs also specifically allows for information sharing within a group of connected businesses for AML/CTF purposes, provided it is compliant with the DPA and UK GDPR, even if entities within the group are in different countries.

81. However, there is no single, clear legal gateway for private-to-private cross-border information sharing across the full spectrum of economic crime. Without clear gateways, organisations may be disinclined to share information with each other. This can be exacerbated in the case of cross-border sharing which might involve collaboration with organisations outside of established networks or with whom there is limited prior engagement. This hesitancy can stem from concerns about data security, potential misuse of information, or reputational risks associated with data breaches or unauthorised disclosures.

82. We recognise that important work has already begun to address cross-border information-sharing, particularly in areas such as data protection, interoperability, and legal frameworks. The Government would like to deepen our understanding of how cross-border information-sharing is being implemented in practice, where gaps and challenges remain, what innovative approaches are emerging, and where the Government should focus its efforts.

Cross-border Sharing (all)

Question 11: General cross-border information sharing question

11.1. Please describe your experience of sharing or receiving information cross-border for economic crime purposes?

11.2. How could Government improve or better support the sharing of information cross-border for economic crime purposes?

Technology

83. The Government is increasingly adopting new technologies to create efficiency gains, having launched Smart Data. Smart Data tackles data fragmentation through common data formats, API-driven platforms, and risk-based sharing embedded with privacy-by-design, including cross-border standards and pilots which will further support secure, real-time collaboration. Government also introduced the AI playbook in February 2025 that builds on the Generative AI Framework for HMG and supports the public sector to harness AI. Meanwhile, the private sector has adopted AI models rapidly to tackle economic crime and comply effectively with regulations including adopting AI models on datasets, operating machine learning and training data including on transaction monitoring and risk assessments. Government is interested to learn industry's experiences with new technologies specifically in an economic crime context, any success stories and any suggested improvements to support both the public and private sector to increase their impact and efficiencies.

New technologies

Question 12: New Technologies

12.1. How could Government best optimise the growth of new technologies such as automation or artificial intelligence to support the public sector and private sector to detect and act upon information related to economic crime? Please share detail of the technology, its benefits, risks including any operational and legal considerations.

Full list of questions

Responses can be submitted anonymously. If you wish to be identified, please share the name of yourself and / or your organisation. If you wish to be identified, we may follow up with further questions.

Private-Private Questions (for private sector only)

When answering all questions, please be descriptive of legal, operational and cultural factors related to the sharing of information.

Question 1: Economic Crime and Corporate Transparency Act 2023

1.6. Please describe your experience of sharing or receiving information with other private sector organisations using section 188 and 189 of the Economic Crime and Corporate Transparency Act 2023?

1.7. How could Government better support organisations to share information with one another using section 188 and 189 of the Economic Crime and Corporate Transparency Act 2023?

1.8. Should, if any, improvements be made to section 188 and 189 of the Economic Crime and Corporate Transparency Act 2023?

1.9. Should more organisations be added to section 188 and/or 189 Economic Crime and Corporate Transparency Act 2023 and, if so, who?

1.10. Should new offences be added to Schedule 11 of the Economic Crime and Corporate Transparency Act 2023 and, if so, which?

Question 2: Criminal Finances Act 2017

2.4. Please describe your experience of sharing or receiving information with other private sector organisations for economic crime purposes using Section 11 of the CFA 2017?

2.5. Please describe your perspective on the role of the Section 11 of the CFA 2017 information-sharing provisions now that Sections 189 and 199 of the Economic Crime and Corporate Transparency Act 2023 are in force?

2.6. Should, if any, improvements be made to Section 11 of the CFA 2017?

Question 3: General private-private sharing questions

3.4. Please describe your experiences of applying the Data Protection Act 2018 and UK GDPR when sharing or receiving information with other private sector organisations for economic crime purposes?

3.5. Please describe the impact that the Data (Use and Access Act) 2025 will have on how organisations share or receive information with other private sector organisations for economic crime purposes?

3.6. How else could Government better support private-private information sharing for economic crime purposes?

Private-public questions (for all)

Question 4: Financial intelligence gateway and pre-order enquiries

4.3. Please describe your experience of sharing or receiving information via the Financial Intelligence Gateway, or in pre-order enquiries in advance of a production order, for economic crime purposes?

4.4. Could Government introduce improvements to the way information is shared via the Financial Intelligence Gateway or in pre-order enquiries in advance of a Production Order?

Question 5: Proceeds of Crime Act 2002 Part 8

5.3. Please describe your experience of sharing or receiving information in response to a Part 8 Proceeds of Crime Act 2002 Order (Production Orders, Disclosure Orders, Unexplained Wealth Orders, Customer Information Orders and Account Monitoring Orders)? Please feel able to comment on all or specific orders.

5.4. Please consider how Government could improve or better support sharing of information in response to a Part 8 Order (Production Orders, Disclosure Orders, Unexplained Wealth Orders, Customer Information Orders and Account Monitoring Orders)? Please feel able to comment on all or specific orders.

Question 6: Crime and Courts Act 2013

6.3. Please describe your experience of sharing or receiving information with the NCA using Section 7 of the Crime and Courts Act 2013?

6.4. Should a similar gateway to Section 7 of the Crime and Courts Act 2013 be available to other public bodies and, if so, which public bodies?

Question 7: Suspicious Activity Reporting

7.5. Noting recent improvements to the Suspicious Activity Reporting regime, please describe your current experiences of sharing or receiving information through Suspicious Activity Reporting in Part 7 of the Proceeds of Crime Act 2002?

7.6. What further changes, if any, could be made to the Suspicious Activity Reporting regime to make it more effective in delivering its objective to provide high value intelligence to law enforcement?

7.7. With the growth of public-private partnerships and real-time data sharing such as Data Fusion, please describe your perspective on the role, utility and value-add of the Suspicious Activity Reporting regime?

7.8. What benefits or risks, if any, would there be to changing the suspicion threshold to 'reasonable grounds to suspect' in the Suspicious Activity Reporting regime and would you support this change?

Question 8: Investigatory Powers Act 2016 and related amendments

8.3. Please describe your experience of acquiring or sharing communications data under the Investigatory Powers Act 2016, including any related amendments, for economic crime purposes?

8.4. Please consider how Government could improve or better support the acquisition of communications data under the Investigatory Powers Act 2016, including any related amendments, for economic crime purposes?

Question 9: General public-private sharing questions

9.3. Please describe your experiences of applying the Data Protection Act 2018 and UK GDPR when sharing information or receiving information owned by the private sector with law enforcement for economic crime purposes?

9.4. Please consider how else Government could better support information-sharing between public and private bodies for economic crime purposes?

Private-public questions (public sector only)

Question 10: General public-public information sharing questions

10.1. Should Regulation 52 of the MLRs be amended to include any other public bodies?

10.2. What impact would a broad legal gateway such as the Digital Economy Act 2017 have on public-public information-sharing?

10.3. How else could Government improve or better support the sharing of information within the public sector for economic crime purposes?

Cross-border Sharing (all)

Question 11: General cross-border information sharing question

11.1. Please describe your experience of sharing or receiving information cross-border for economic crime purposes?

11.2. How could Government improve or better support the sharing of information cross-border for economic crime purposes?

New technologies

12.1. How could Government best optimise the growth of new technologies such as automation or artificial intelligence to support the public sector and private sector to detect and act upon information related to economic crime? Please share detail of the technology, its benefits, risks including any operational and legal considerations.

Anything else

Question 13: Any other areas

13.1. Are there any other areas not covered by the above 1-12 questions that could be addressed to improve economic crime information sharing?