Electronic Money Association
Crescent House
5 The Crescent
Surbiton, Surrey
KT6 4BN
United Kingdom
Telephone: +44 (0) 20 8399 2066
www.e-ma.org

Economic Crime Information Sharing Call for Evidence

Homeland Security Group,
6th Floor, Peel Building,
Home Office,
2 Marsham Street,
London, SW1P 4DF

6 May 2026

Dear Sir/Madam

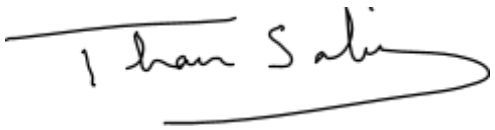
Re: EMA response to Home Office Economic Crime Information Sharing Call for Evidence

The EMA is the EU trade body representing Fintech electronic money issuers and alternative payment service providers. Our members include leading payments and e-commerce businesses worldwide, providing online payments, card-based products, electronic vouchers, and mobile payment instruments. Most members operate in the UK and the EU, as well as globally, and are often indirect participants in payment schemes. A list of current EMA members is provided at the end of this document.

We welcome the opportunity to provide this input to this consultation.

I would be grateful for your consideration of our input and comments.

Yours sincerely,



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

Overarching comment

The Electronic Money Association very much welcomes the permissive data sharing environment created by the Economic Crime and Corporate Transparency Act 2023 legislation. Firms have historically been hesitant to cooperate or share data, citing perceived legal constraints within AML and GDPR frameworks; for example, the POCA offence of 'tipping off' can be interpreted to discourage data sharing. Whilst ECCTA is a huge step forward, the legal landscape supporting data sharing remains fragmented and overly complex.

The EMA views the ECCTA as the foundational step towards establishing a coherent legal basis for information reporting and real-time intelligence sharing across UK sectors - payments, social media and telecoms – essential to effectively combatting economic crime. We thus welcome the opportunity to provide input to this consultation.

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?

EMA Members have benefitted from the permissive data sharing regime created by ECCTA to enable cooperation with the other counterparty to a payment to investigate and resolve fraudulent transactions. The new wide definition of 'economic crime offences' covering effectively all forms of financial crime including fraud, money laundering and terrorist financing, removes the previous fragmented legal complexity.

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?

For years, financial firms have been deterred from data sharing by a deeply entrenched landscape of AML and GDPR regulations. The Government and its regulatory bodies should actively promote use of ECCTA to more quickly affect the behavioural change necessary to gain fully the crime prevention benefits.

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

Yes, see answer to Q. 1.4.

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

A significant proportion of economic crime originates within non-financial firms. It would be beneficial to include firms in these sectors, specifically social media and telecoms sectors, to foster data sharing and cooperation on economic crime prevention.

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

The EMA welcomes the current wide and comprehensive definition of 'economic crime offences' under Schedule 11.

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?

The EMA has no experiences to share; this is most likely due to the infrequent circumstances and preconditions necessitating use of the Section 11, 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?

Wide adoption of ECCTA 2023 will further reduce use of Section 11, CFA 2017.

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

It would be more beneficial to incorporate measures supporting the creation and submission of joint SARs within ECCTA. Improvements to be incorporated would be to clarify which of the firms should take the lead in submitting a joint SAR and the discharge of the reporting responsibility on the other party.

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?

Previously, firms have been highly reluctant to cooperate and share data due to existing AML and GDPR perceived legal constraints. Before the ECCTA, data-sharing provisions within the regulatory framework were somewhat limited, appearing secondary to the more restrictive elements of the legislation and lacking the clarity needed for effective implementation. Therefore, in order to share data, firms had to navigate around mostly restrictive legislation that made it an awkward and slow process. The ECCT Act creates a more permissive data sharing regime that encourages sharing of information between

regulated businesses for the purposes of preventing, detecting and investigating economic crime. It came into effect relatively recently, in November 2023, and it's yet to realise its full potential.

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?

The introduction of crime prevention as a 'recognised legitimate interests' that removes the requirement for a legitimate interest assessment is very welcome. This removes an operational barrier to the use of personal data; however, this is very recent legislation and thus the impact is difficult to assess.

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

The EMA would welcome a government sponsored **Smart Data** [DUAA 2025] initiative to promote real-time intelligence sharing between regulated firms for the purpose of economic crime prevention. Firms currently operate isolated or in silos where the valuable intelligence that they gather from profiling organised criminal gangs (OCGs) remains. OCGs will move from one target firm to another exploiting the same mode of operation. The sharing of insights into the modes of operation, vulnerabilities, sources of data will assist firms recognise and resist attack as well as track specific OCGs with a view to law enforcement intervention.

We envisage a Smart Data Scheme creating a regulated framework to allow the sharing of intelligence within and between sectors and law enforcement to foster innovation from the private sector.

A key requirement to support Smart Data Initiatives is the standardisation of data formats and definition of typologies etc. This is an exercise that could be commenced immediately to avoid the current payment industry proceeding with varying formats.

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?

No comment.

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?

No comment.

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.

No comments at this time.

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.

No comments at this time.

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?

No comments.

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?

No comments.

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?

The EMA welcomes the clearer definition of 'suspicion' and operational guidance with a view to generating better quality report submissions and fewer low-quality defensive reporting. However, the NCA is better able to discern whether this is leading to improved investigation packages for law enforcement.

7.2. What 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?

The application of AI presents the prospect of improved report handling and analysis of SARs with the objective of producing high value intelligence and investigation packages that are timely and actionable by 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?

Whilst further improvements to the SAR reporting regime should be sought, they are just one source of crime data. The crime reports submitted by victims potentially provides a rich source of intelligence into the methods, means and vulnerabilities exploited by organised criminal gangs.

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?

We do not believe that moving the SAR reporting threshold to 'reasonable grounds to suspect' only would reduce the number of SARs reported if this is based on the established legal interpretation of 'reasonable grounds' as an objective standard. We would also caution against the removal of actual knowledge and suspicion from the definition of the reporting offence.

If the aim of the contemplated amendment is to prevent SARs being made where there is little objective evidence supporting the suspicion, this could be achieved through the following means:

a) New technology, particularly the application of AI, offers the prospects of achieving a reduced volume of SARs and also of improving the quality of intelligence generated.

b) Guidance could be introduced to prevent SARs from being made that lack a sufficient evidence base. This could helpfully elaborate on the condition in s 330(3A) of POCA.

c) An alternative approach might be to introduce a minimum case threshold for reporting that would reduce the volume of low-value reports and alleviate some of the burden of reporting from firms. The value of crime cases that are of interest to law enforcement primarily relate to organised criminal activity and there is a wide disparity between this and the value of the cases firms most report.

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?

No comments at this time.

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?

No comments at this time.

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?

This is a less problematic area that operates efficiently and has no perceived barriers to the provision of information to law enforcement.

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

The current legal framework is adequate.

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?

No comment.

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

No comment.

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

No comment

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?

The majority of EMA Members operate across the UK, European Union countries and increasingly internationally. The different legal frameworks cause complexity and challenges to data sharing within a single group, even with the close alignment of regulations such as GDPR. The fostering of fraud data sharing within the European Union (e.g. through Public Private Partnerships) encounters similar difficulties to the advantage of organised criminal gangs.

The EMA has observer status with EFIPPP and supports work for data sharing across borders along with our Members.

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

Whilst the NCA has managed to maintain a good level of information sharing and cooperation with Europol including improved digital integration with Interpol, the loss of direct access to Europol and EU agency databases is an impediment.

The EMA is further concerned that the data sharing and cooperation agreements with Europol are subject to the Trade and Cooperation Agreement that could be suspended or terminated if the UK diverges on data protection or fundamental rights. The recently reported NCA Operation Destabilise illustrates the success that can be achieved through international cooperation between FIUs.

The UK must seek unconditional bilateral agreements to build resilient data sharing and cooperation with FIUs across Europe and internationally.

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.

We envisage and welcome a Smart Data Scheme creating a regulated framework to permission the sharing of intelligence within and between sectors and law enforcement would foster innovation from the private sector.

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?

The EMA would like to highlight two additional areas for improved data sharing:

Victim Crime Reporting: EMA Members support amending the **Consumer Standard of Caution** to make crime case reporting and co-operation by victims a requirement in order to qualify for full financial compensation.

This obligation is considered a fair contribution by victims in reflection of the compensation provided to victims by the payments industry. We foresee significant benefits to fraud prevention and law enforcement from this approach:

- More timely crime reporting by victims;
- Provision of a comprehensive and rich data set informing law enforcement intelligence and prioritisation; and
- Training AI fraud risk modelling and scoring.

Automated PSP Crime Reporting: Automating the collection of fraud case reporting from PSPs offers the prospective benefits of removing the largely manual burden of reporting from firms whilst also vastly improving the data quality, granularity of the data captured, and the frequency of reporting. This will by necessity require the **standardisation of data formats and definition of typologies** that will improve data quality and potential for automated processing and analysis.

The planned roll-out of industry-wide IT platforms, such as BPS 2.0 for APP Scam claims handling puts this ambitious goal clearly within sight.

Cardaq Ltd
CashFlows
Circle
Coinbase
Crypto.com
Currenxie Technologies Limited
Decta Limited
Deel
eBay Sarl
ECOMMPAY Limited
emerchantpay Group Ltd
EML Payments
EPG Financial Services Limited
eToro Money
Etsy Ireland UC
Euronet Worldwide Inc
Finance Incorporated Limited
Financial House Limited
FinXP
First Rate Exchange Services
Fiserv
Flywire
Globepay Limited
GoCardless Ltd
Google Payment Ltd
IDT Financial Services Limited
iFAST Global Bank Limited
Imagor SA
Intersolve
Kraken
Loodapay LU S.A.
Modulr Finance B.V.
MONAVATE
MONETLEY LTD
Moneyhub Financial Technology Ltd
Moorwand Ltd
pay.cetera B.V.
Payhawk Financial Services Limited
Paymentsense Limited
Payoneer Europe Limited
PayPal
Paysafe Group
Paysend EU DAC
Peratera UK Ltd
Plaid B.V.
Pleo Financial Services A/S
PPS
Push Labs Limited
Remitly
Revolut
Ripple
Satispay Europe S.A.
Securiclick Limited
Segpay
Soldo Financial Services Ireland DAC
Square
Stripe
SumUp Limited
Syspay Ltd
TransactPay
TransferGo Ltd
TransferMate Global Payments
TrueLayer Limited
Uber BV
Unzer Luxembourg SA
Vitesse PSP Ltd
VIVA WALLET.COM LTD
Weavr Limited
WEX Europe UK Limited
Wise
WorldFirst
Worldpay