Fraud Detection and Prevention:
Enhanced data exchange - Call for input questions:

5 November 2025

Organisation: **e-Money Association**

Name and title of contributor: **David Brunsdon, Economic Crime Lead**

The EMA welcomes the opportunity to participate in this important payments industry counter fraud initiative and fully supports its objectives.

1. Which of the above models does your organisation consider should be taken forward to the next stage of design? Please explain any preference or ranking for the models.

   Our preference is for model B where both Payment Sender and Receiver can be Requestor and Responder of additional data attributes.

2. To what extent do you support these data points forming the Day 1 Value Attributes?

   The Day 1 Value Attributes are supported as initial data attributes.

3. Do you have any challenges with these data attributes that you would like to highlight?

   The EMA or Members would like to see the more detailed data set from the Proofs of Concept undertaken by UK Finance in order to form a more informed view on our preferred data value attributes. We would also like to better understand the way in which the metrics have been calculated. One key point of concern is the 'customer inconvenience factor' the percentage of false positives (i.e. genuine transactions assessed as fraudulent) as a proportion of genuine transactions.

   The non-bank PSPs have a different position in the industry and a variety of different business models and customer segments. Some Members have expressed concern that the chosen Day 1 Value Attributes may prove to be biased against non-bank PSPs and ultimately uncompetitive.

4. Are there any other data points you feel should be included in the day 1 Value Attributes?

   The EMA or Members would like to see the more detailed data set from the Proofs of Concept undertaken by UK Finance in order to form a more informed view on our preferred data value attributes.

   Criminals rapidly evolve their mode of operation in response to counter measures. Whilst Data Value Attributes selected from a static data set are a reasonable starting point their utility might quickly diminish in real-world application.

5. When considering account identification, are there any attributes that you would consider essential outside of sort code and account number? (consider scenarios where an account number may not designate a single individual; e.g. joint accounts, E-Wallets etc).

   Yes, we hope to see the EDEx to develop and expand to include many more data attributes over time. It is difficult to predict what the specific data attributes should be but it will be important to be able to test, trial and learn by deploying different data attributes over time. This might be done perhaps using a sub-set of more technically agile firms prior to wider adoption.

6. How do you see this being built into your existing processes?

   6.1 Would it be deployed primarily on a technical/rules based/risk engine basis?
   6.2 Would you expect the exchanged data to be used by operational staff during case investigation, or supporting explainability of decisions?

   We envisage both: Automated decisioning supporting manual review; for risk modelling and further case investigation.

7. What types of fraud or financial crime, or other behaviours would the utility help you target?

   We would envisage potentially use for indicators of victims, mules and accounts opened for the purpose of committing all economic crime.

8. How would you measure the success and value of the service (e.g. is it in operational efficiencies, reduced levels of fraud, fewer genuine payments disrupted?)

   The key measure of success will be the fraud detection versus the 'customer inconvenience factor' the percentage of false positives (i.e. genuine transactions assessed as fraudulent) as a proportion of genuine transactions. A high incidence of genuine customers' transactions suspended will likely be unacceptable.

9. Do you have any figures, or high-level indication of value you could anticipate the service having?

   This is difficult to foresee but would like to see some thought given to establishing target KPIs and acceptable thresholds prior to launch.

10. Do you feel that the exchanged data should be used in prevention?

    Yes, certainly.

11. How critical is this to the value case for the service?

    This is critical, the ability to provide tailored warnings to customers in support of the Consumer Standard of Caution requirements is an important use-case.

12. Broadly, what controls would you anticipate being required to ensure the information is used appropriately?

Beyond the obvious data security requirement the data provided must be used only to fulfil the legal purpose of preventing Economic Crime under the ECCTA 2023.

13. What would your primary concerns be?

    We view fraud prevention as a public good and an individual good, as such there is a 'legitimate interest' basis for use of this data.

    It will be necessary to work thought the decisioning trade-offs with the FOS to establish a fair balance to ensure the EDEx can fulfil its objectives.

14. Please share the key factors or considerations you would like us to take into account during the design phase to ensure the integration process is as simple as possible for your organisation.

    Developing a wide range of standardised data formats, definitions and terminology.

15. If your organisation were to choose to adopt such a service, what would be an indicative timeline to 'go live' with the service once Pay.UK has completed the technical build, rules and standards?

    Nil response.

16. Any indicative information on how much adoption will cost your organisation (whilst you might not have this, if you are able to provide any ROM its very useful for value case assessment)

    Nil response.

17. Do you have a preference on data format (ISO20022, JSON, etc?)

    Nil response.

18. We understand that some PSPs may require an aggregator or other 3rd party arrangement to enable participation. Would your organisation anticipate needing an aggregator or 3rd party to connect to the service?

    Nil response.

19. Additionally, do you have any concerns or considerations you'd like to highlight that relate to aggregator models?

    Nil response.

20. Please suggest any preference you may have for one of the above models, with consideration of how different models might influence your usage or adoption of the utility.

    Model B has strong support versus Model A.

21. Please provide any indicative volumes of EDEx requests you could anticipate making over the course of a year? (note: we acknowledge this will change depending on certain design factors, but even a rough order of magnitude can help)

    Nil response.

Additional Question:

We've adopted the approach outlined in this document as a result of strong industry sentiment and clear preference for a solution of this type.

Having addressed the questions in this document, do you still feel this is the best direction, or would you suggest alternative approaches?

The EMA welcomes the opportunity to participate in this important payments industry counter fraud initiative and fully supports its objectives.

Responses Deadline:

There is an 8-week window for responds, therefore the deadline for Call for Input responses is **Wednesday 9 November 2025**. Please send responses to: fraudprevention@wearepay.UK

This document is restricted and is designed for recipients and relevant colleagues within their organisation. This document is not intended to be circulated to further third parties. For the avoidance of doubt, trade body members are considered an extension of the trade bodies "organisation" for this purpose.