Council of the European Union
General Secretariat

PUBLIC

Interinstitutional files:
2023/0212 (COD)

Brussels, 25 June 2025

WK 8740/2025 INIT

LIMITE

EF
ECOFIN
UEM
CONSOM
CODEC

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	EUROPEAN CENTRAL BANK
To:	Working Party on Financial Services and the Banking Union (Digital Euro Package) Financial Services Attachés
Subject:	Digital euro - WP (VTC) technical seminar - Fraud detection and prevention mechanism for online transactions

EUROPEAN CENTRAL BANK

EUROSYSTEM

PUBLIC

CWP technical seminar

Fraud mechanism – functional elements



30 June 2025

This presentation has not been adopted or endorsed by ECB decision making bodies and therefore any views expressed shall not, under any circumstances, be regarded as an official position of the ECB. Its content is intended only for the purpose of facilitating discussions within the Council Working Party

Agenda

PUBLIC

1. Risk of fraud
2. Fraud detection and prevention mechanism for online transactions
3. Q&A

PUBLIC

1

The risk of fraud

Risk of fraud

PUBLIC

Digital payment systems face an increasing risk of fraud

- Financial fraud is a serious and constantly evolving **threat** to the stability and integrity of the European financial system and the customer confidence in payment systems, to which the digital euro does not form an exception.
- **Social engineering techniques** such as phishing, smishing, vishing or impersonation (manipulation of the payer) are expanding and account for more than half of the total value of fraudulent credit transfers.[1]
- **Fraud techniques** are constantly **evolving**, as their targets are users of payment systems rather than the technical infrastructure.[2]
- The **Eurosystem has a duty of care** especially for less digitally savvy and elderly users.

- Together with industry experts, the **ECB has evaluated** existing and emerging anti-fraud technologies.
- The digital euro will cater for **a robust fraud prevention and detection mechanism** with the establishment of the Risk and Fraud Management (RFM) service that will provide a fraud risk score to PSPs **leveraging information at scheme level** on online transactions.
- Information gathered at **scheme level is crucial to tackle social engineering**, whereas each PSP's fraud prevention system alone is effective in other fraud scenarios (identity theft, unauthorised payments).
- **Protecting payment systems** from financial crime, while **upholding user privacy**, is an important challenge and crucial for the digital euro.
- Further improvement of PSP’s fraud prevention through **learning** from situation awareness and threat intelligence reporting.
- This **enhances PSP’s ability to detect fraudulent transactions** prior to settlement.

Privacy measures in the digital euro still allow for strong fraud protection at scheme level

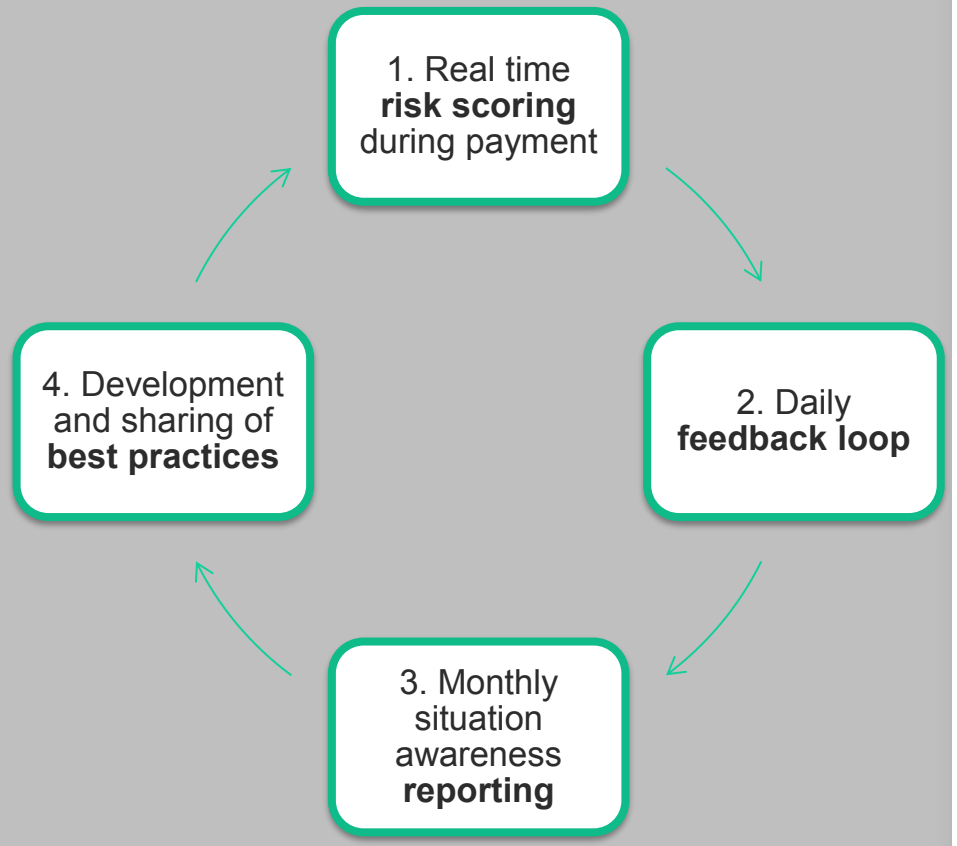
[1] EBA 2024 Report on payment fraud
[2] EPC 2024 Payment Threats and Fraud Trends Report

PUBLIC

2

Fraud detection and prevention mechanism for online transactions

Fraud detection and prevention mechanism: functions



✓ Fraud prevention **during the payment process**:

1. **Risk scoring** – PSPs request the **risk score** from the Risk and Fraud Management service during the payment process of online transactions.

The risk score is a value that represents the **possibility** of a transaction being fraudulent.

PSPs can include the scheme-level assessment into their own risk management process, and take a decision based on the entirety of information available to it.

✓ Fraud detection **post payment:**

1. **Feedback loop** – PSPs shall provide information on transactions that have been confirmed as fraudulent or reassessed as non-fraudulent to the Risk and Fraud Management service, to maintain capabilities and improve its effectiveness on a continuous basis.

2. **Reporting** – the Risk and Fraud Management service will provide to PSPs a situation awareness report including aggregated monthly review on the systemic fraud statistics, top fraud categories and trends.

3. **Engagement** in **development and sharing of best practices** at scheme level help in building a secure ecosystem.

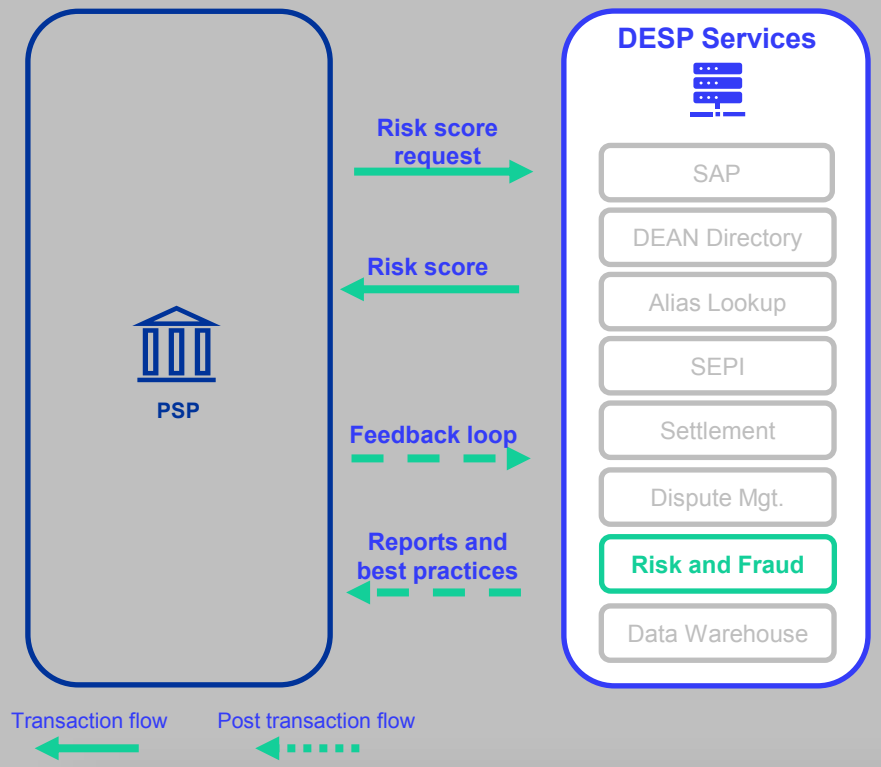
The Rulebook will include rules for PSPs' interaction with the Risk and Fraud Management service.

www.ecb.europa.eu ©

Fraud detection and prevention mechanism: service and data flows

PUBLIC

For the purposes of point (a) of Article 36(1) [1], **processing of data by PoSS for this service shall be limited to the data required** for the prevention and detection of fraud across payment service providers for the **following information**:



Elements and examples for the risk score request based on the draft legislation:

- **End-user data:** hashed Customer ID.
- **Payment transaction data:** payer and payee PSP IDs, transaction ID and amount, transaction type, e.g., e-commerce or purchase.
- **Session data** such as device IP.

A risk score is a value that represents the possibility of a transaction being fraudulent.

Possible elements for the feedback loop:

- **Payment transaction data**: Payer PSP ID, transaction ID, timestamp.
- **Fraud categorisation**: fraud status, fraud type

Possible elements for the situation awareness reports:

- Reports with **statistics per fraud type** incl. data on fraud rate, number of fraudulent transaction, false positive rate - % and count.

While the final dataset is subject to the provider selection process, the data processed shall be in line with the legislative and data segregation requirements.

1 (…) providers of support services shall provide payment-related services across PSPs. (…): (a) supporting the prevention and detection of fraud across payment service providers in accordance with Article 32;

Fraud detection and prevention mechanism: privacy by design

PUBLIC

Privacy, as a key element of the digital euro design for the Eurosystem, has been at the core of the design of the DESP's backend infrastructure [1] **:**

- The **Eurosystem** will not be able to infer from the data it processes any identity attributes nor their link to transactions.
- The digital euro will apply **strict segregation and minimisation of data**:
  - Between PSPs and the DESP: **Only PSPs will be able to know the identity of the end user** and link it to individual transactions or balances, data in DESP cannot do so.
  - Within the DESP, between Providers of Support Services (PoSS) [2] and the Eurosystem: leveraging the opportunity provided by the draft regulation, splitting the allocation of tasks with PoSS and putting in place contractual safeguards will **segregate data** and **prevent the linking or onward transmission of personal data** that shall only be used for specific purposes and when strictly necessary.
  - **Data minimisation:** data processing of D€ payment transactions is unprecedentedly segregated and minimized. The visibility of data to the central infrastructure providers (Eurosystem or PoSS) is minimal and may be further reduced as technology evolves. The Eurosystem will actively engage with industry experts to foster innovation and apply innovative privacy enhancing technologies (PETs)

1 Based on ECB Technical seminar, 6th March, 2025, Introduction

2 Art. 36 of the draft digital euro regulation

www.ecb.europa.eu ©

Conclusions

PUBLIC

- ✓**Financial fraud is a** serious **threat** to the stability and integrity of the European financial system and the customer confidence in payment systems.

- ✓The **fraud detection and prevention mechanism** offered by Risk and Fraud Management services **for online transactions** on a **scheme level** to enhance the participating PSPs' internal capabilities. Moreover, through the **regular exchange of fraud related information** (feedback loop and reporting) the entire digital euro ecosystem will become **a highly secure environment for the users**.

- ✓Only the **minimum** strictly necessary **data** shall be **processed**. The Risk and Fraud Management services shall adhere to the **highest privacy and data protection standards** and obligations among the currently known, digital payment systems and shall be in **line with** data protection and payment services **legislation**.

PUBLIC

Q&A