EUROPEAN CENTRAL BANK

EUROSYSTEM

Fraud prevention and detection

Market Advisory Group

10 May 2023

Digital euro project team

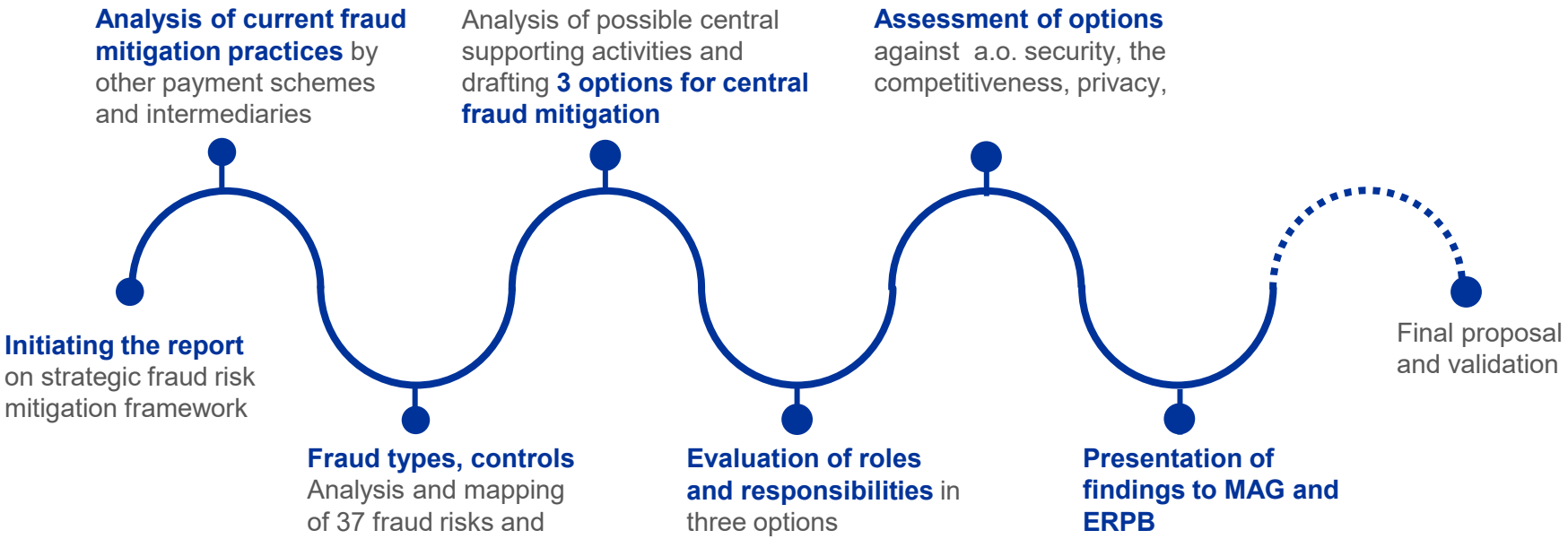
Objective of today's exchange

Present the investigation of fraud risk prevention and detection for the digital euro.

Invite your feedback on the analysis of the fraud risk prevention and detection approach identified by Eurosystem (followed by written procedure until 16 June 2023) as input for Eurosystem preparations of final decisions on these functionalities by Governing Council.

Fraud in the context of a digital euro

1. Strategic fraud risk mitigation approach



1.Solid fraud prevention and detection is essential for ensuring a safe and secure digital euro

Fraud definition from European Banking Authority's Guidelines on reporting requirements for payment fraud data under Article 96(6) PSD2:

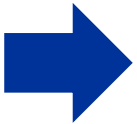
- "**Unauthorized payment transactions** made, including as a **result of the loss, theft or misappropriation of sensitive payment data or a payment instrument,** whether detectable or not to the payer prior to a payment and whether or not caused by gross negligence of the payer or executed in the absence of consent by the payer ('unauthorized payment transactions')"
- "Payment transactions made as a result of the payer **being manipulated by the fraudster** to issue a payment order, or to give the instruction to do so to the payment service provider, in good-faith, to a payment account it believes belongs to a legitimate payee ('manipulation of the payer')." Payment transactions made as a result of the payer being manipulated by the fraudster to issue a payment order are often referred to as scams.

1. Most of today's fraud risks are relevant for the digital euro use cases.

Analysis:

37 fraud risks have been analyzed on their potential relevance for the digital euro
- separately for P2P, POS & e-commerce use cases, among them

- *trusted counterparty,*
- *investment fraud,*
- *online shopping fraud,*
- *emotional manipulation,*
- *account takeover,*
- *money mule,*
- *phishing,*
- *malware,*
- *CEO scam,*
- *invoice redirection,*
- *Impersonating police / tax authority,*
- *…*



Newly emerging fraud risks need to be vigilantly followed and assessed regarding the digital euro.

1. Key activities in retail payment fraud management

01

Customer onboarding and continuous due diligence, i.e., collecting KYC data

02

Fraud prevention, i.e., risk appetite & risk assessment

03

Fraud detection, i.e., fraud monitoring, action to stop/hold fraudulent transactions*

04

Fraud investigation, i.e., fraud case & alert handling

05

Resolution activities, i.e., reimbursements & list management

06

Fraud reporting, i.e., PSD2 reporting

07

Collaboration with supervisors & authorities ,i.e., information requests from authorities

08

Fraud management strategy, i.e., fraud risk governance

*Actions to stop/hold of suspected fraudulent transactions or sessions: Intermediaries shall always make the final decision for actions: rejecting, holding, stopping, or releasing transactions.

How a digital euro can effectively tackle fraud

2. How a digital euro can effectively tackle fraud

Lesson learned from current schemes:

- Schemes with **instant settlement are seeing central components being added - by scheme itself or by scheme participants** (e.g. PIX, SCT Inst, Faster Payments (UK)**;**
- While latency can be impacted, **a central component can decrease fraud losses**
  → Central Support Service activities can further reduce the attractiveness to fraudsters of using digital euro

Key roles involved in fraud management

• Intermediaries (IM)	Supervised entities, servicing end-users
• End-users (EnU)	Individual end-users, business end-users
• Scheme Owner (SO)	Eurosystem
• Settlement Provider (SP)	Eurosystem
• **Central Support Service (CSS)**	**Central entity, separate from the Settlement Provider**

2. How can the key roles contribute to mitigate fraud risks?

Scheme Owner (SO) "applies" controls via the rulebook providing, e.g.
- scheme-wide limits

Intermediaries (IM) implement controls, e.g.
- fraud monitoring and investigation,
- risk assessments and Strong Customer Authentication (similar to other existing retail payment solutions)

Settlement Provider (SP) could apply a limited number of specific controls, e.g.:
- providing a waiting time or pre-registration period before an account or a new device can be used.
- offboarding a fraudulent intermediary.

Central Support Service (CSS) can provide controls, e.g.
- such as fraud monitoring and risk scoring,
- maintaining gray and blacklists and information sharing between intermediaries.
- the Central Support Service is not meant to compensate for any potential fraud control weaknesses of IMs.

2. Degrees of support via the Central Support Service

On top of fraud prevention and detection at intermediaries

Option 3. Central Support Service directly involved in pre- and post-fraud analysis, also in real-time

- perform monitoring and **risk scoring of transactions in real-time** before they are settled.
- Additional responsibilities in case fraud is detected in real-time.
- **Utilizes either pseudonymized data or needs full visibility of data**

Option 2. Central Support Service involved directly in post-fraud analysis, not in real-time

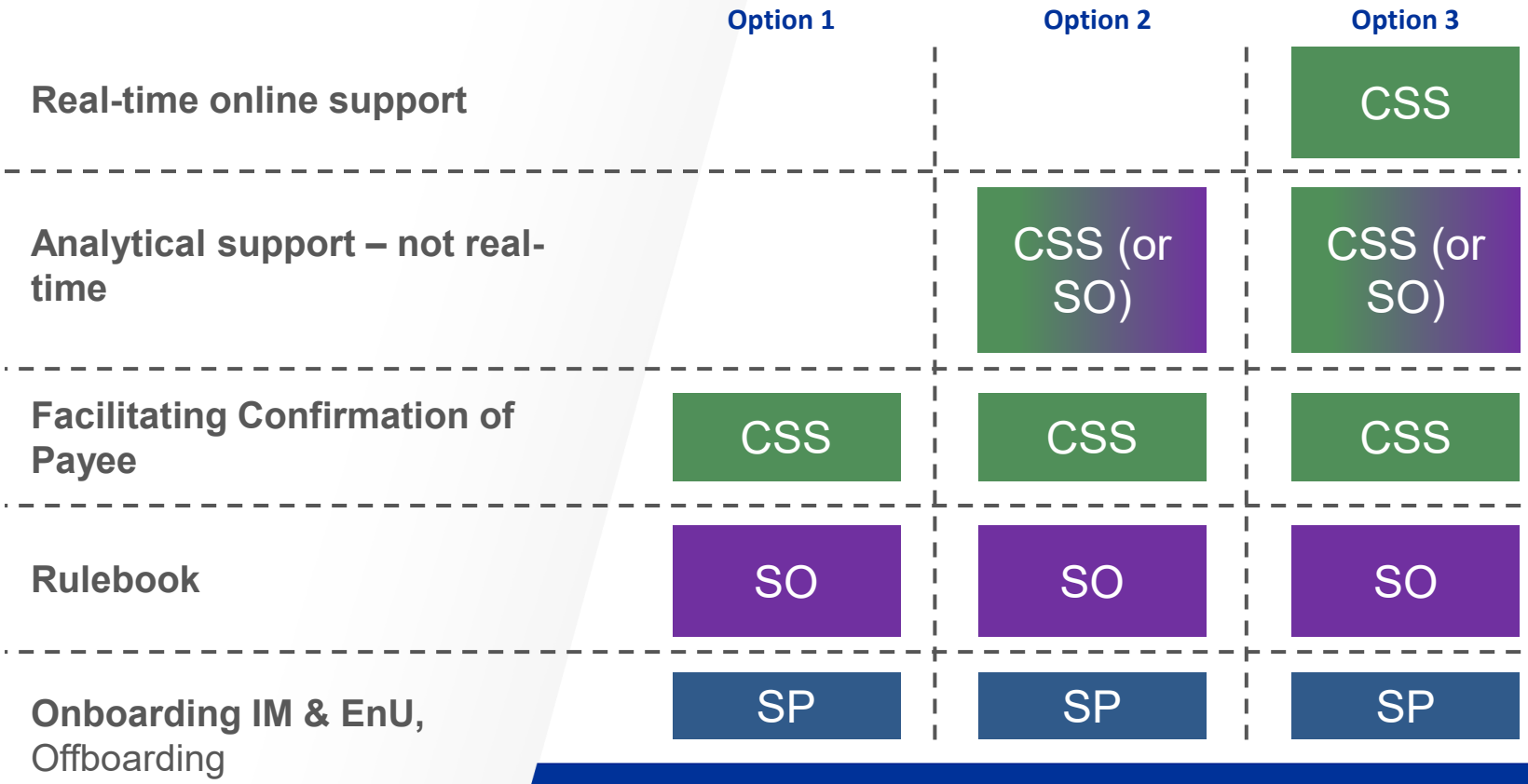
- conducts post-fraud analysis.
- Provides regular **threat intelligence** and **situation awareness** for IMs based on overall visibility.
- Utilizes **pseudonymized customer data, transaction data** and possibly **session data**.

Option 1. Central Support Service involved indirectly only

- Inclusion of fraud in the **scheme rulebook.**
- IMs performs fraud management on their own.
- **The CSS does not handle any end-user data.**

Increased Eurosystem responsibility

2. Allocation of responsibilities



2. Assessment of the 3 options

Implications for privacy and sourcing to be investigated

Based on current comparative assessment,

- **Option 3 is seen as providing the best long-term solution** for fraud prevention and detection and should be ready to be deployed at the time of full launch of digital euro.
  - Dedicated assessment of interplay with privacy objective required
  - Assessment result might have an effect on sourcing strategy

- **Option 1 should be in place from day 1**
  - Minimum requirement and possible first step towards Option 3

- **Option 2 could be added sometime between soft launch and full launch**
  - Possible next evolution step towards Option 3

Way forward and discussion

For feedback

We invite **reflections on all aspects of the analysis**, including the following questions:

- Does MAG share the view from the functional analysis, with a role for a central fraud support service (CSS)?
- What is MAG view on potential opportunity for PSPs to combine (specific) digital € fraud case information, with the PSP's (general) fraud profiles obtained from fraud monitoring of all other payment methods supported by the PSP?
- Would MAG have any suggestions to complement the fraud prevention and detection approach?

Thank you