

# National Payment Committees' actions on fraud prevention

---

Outcome of 2025 stock-take on national payment  
committees and national payment strategies



Directorate-General for  
Financial Stability, Financial  
Services and Capital Markets  
Union



26 June 2025

# Introduction

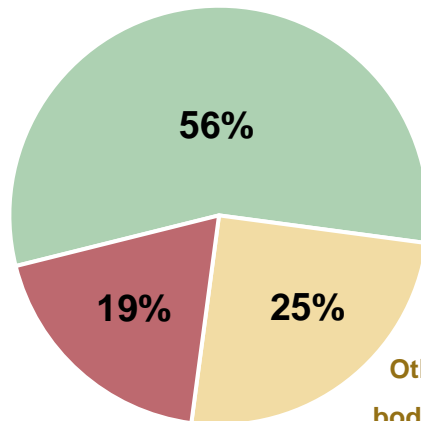
- **2025 Stock-take on National Payment Committees** and National Payment Strategies
- **19 responses** received and analysed
- **Main topics** covered:
  - Functioning and current activities of national payment committees
  - National Retail Payment Strategies
  - **Fraud prevention**

# National Payment Committee Functioning

- **16 respondents** have established a committee or a forum in charge of discussing payment matters - *no changes reported compared to previous stock-take.*
- **More than half** of National Payment Committees are reportedly **competent for payment security/financial crime/fraud prevention** matters - *but not always solely/for all aspects.*
  - In **6 countries**, **another relevant body** has competence for these topics in addition to the National Payment Committee
- **1 Member State** is working on setting up a payment committee
  - payment security, financial crime and fraud prevention topics *may be part of the mandate of the committee* under discussion

**Is the payment committee competent for payment security (incl. cyber security)/ financial crime/fraud prevention topics?**

**Yes, in 9 Member States.**



**No relevant bodies** have such competence in **3 Member States.**

**Other relevant bodies** have such competence in **4 Member States.**

# National Retail Payment Strategies

- **11** responding countries **have adopted or follow** some form of national strategy for payments.
- **5** countries are **planning to adopt** a specific national strategy.
  - *Of which 2 currently follow the Eurosystem strategy.*
- Since the previous stock-take:
  - **1 country** has now **adopted a national payment strategy**
  - **2 Member States** have **begun planning** to adopt/develop a national strategy for payments.



# Main priorities for national retail payment strategies

**Most frequently included key points in national retail payment strategies** (including those following the Eurosystem RPS):

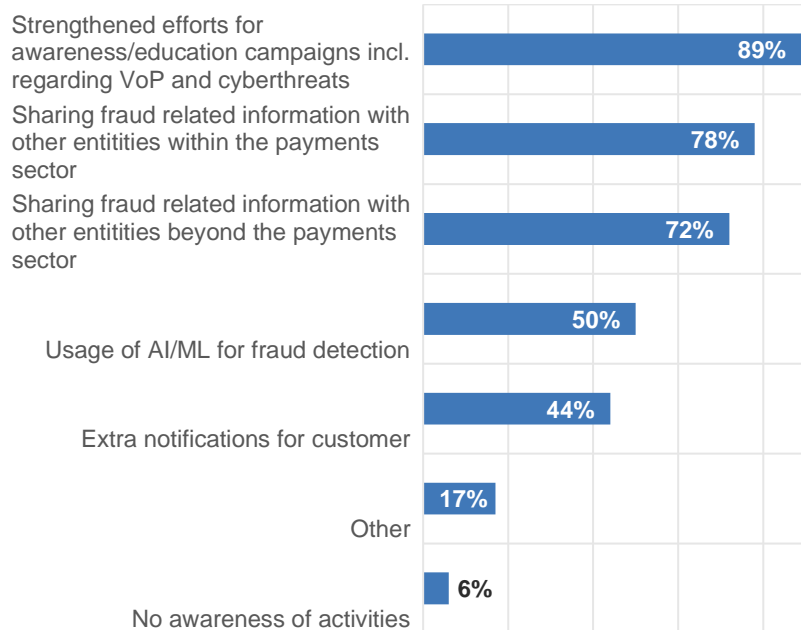
- Fostering integrated pan- European payment solutions
- Working on CBDCs
- Increasing the use of instant payments (including at the POI)
- Promoting mobile payments

**7 out of 12 respondents\*** include payment fraud prevention within their national payment strategy.

*\*Including three who currently do not have a National Payment Strategy but are in the process of adopting one*

# Activities taken to prevent or combat fraud

## Which activities have been taken in your community to prevent or combat fraud?



- Several targeted (or broad) **educational media campaigns**, concentrating on trends/types of fraud and related mitigation measures
- Development and promotion of VoP and CoP services
- Majority report ongoing **sharing of fraud related information with other entities both within and beyond the payment sector**.
  - Including via dedicated fora, authorities and initiatives related to payment security.
  - *In some jurisdictions, this is limited by law.*
- 9 respondents report some usage of **AI for fraud detection/transaction monitoring**.
- 7 countries report the existence of **extra notifications for customers** (e.g. within internet banking/mobile apps and via text messages)

# Fraud and innovation

## How can innovation contribute to fraud prevention?

- **Real-time transaction monitoring** using **AI/ML**
- **New SCA methods** (e.g. voice ID, facial recognition & behavioural biometrics)
- **Dynamic systems** can reduce fraud exposure (e.g. smart limits which adjust based on risk profile)
- **Verification and Confirmation of Payee** services
- **Privacy-enhancing technologies** for secure data sharing
- **Tokenisation** and **end-to-end encryption** of sensitive data to prevent data theft
- **Open banking APIs** and **secure integrations** increasing the safety of **cross-institution** data sharing and fraud monitoring

## How can payment innovation lead to more fraud?

- **User unfamiliarity** with new payment channels may be exploited (e.g. through social engineering and impersonation scams)
- **AI** can increase the **scale and sophistication** of fraud and **lower the entry barrier** for fraudsters.
- **Speed/convenience and security trade-off** (especially for instant payments)
- **Cryptocurrencies and DeFi** make it harder to **trace fraudulent transactions**.
- **Regulatory lag** as innovation often outpaces innovation
- Innovative **cross-border** payment systems may also **bypass traditional controls** & allow fraudsters to exploit **regulatory and enforcement gaps between jurisdictions**

# In which areas should collaboration be strengthened?

- Much agreement that **cross-sectoral collaboration**, as well as collaboration at both a **national** and **international level** should be strengthened.
- **Cross-sectoral** perspective:
  - New features of fraud and fraud realisation channels are increasingly involving different actors – not limited just to the financial environment.
  - Potential collaboration with law enforcement, banks, telecommunication service providers...
- **International** dimension:
  - Fraud is often not an isolated problem of one country
  - Cross-border collaboration and information exchange can help reduce fraud risks

But there is always a **trade-off** between **legal privacy requirements** and the extent to which PSPs can **share personal information** to combat fraud.



# How can central banks contribute to fraud prevention?

**Suggestions include:**

**Fostering dialogue** within and beyond the payment sector

Promoting/providing **information-sharing platforms**

**Supporting innovation** in the field of fraud prevention

Running and supporting **public awareness campaigns**

Collecting **fraud statistics**, **analysing trends** and **publishing findings**

Contributing to the development of **regulations to enhance fraud prevention measures**

Promoting and implementing **technical measures to reduce fraud** (*e.g. VoP and CoP services*)

Setting up **committee(s) to combat payment fraud**

# Suggested next steps

- **National Payment Committees** to act on fraud prevention by **setting up** or **strengthening** existing **cross-sectoral collaboration**.
  - *While PSD3/PSR negotiations (notably relating to the EU network on fraud) are still ongoing, this should not be a reason to delay addressing the issue on a national level.*
- Continue to **exchange on experiences** to raise awareness and identify actionable measures, **following up as relevant in national contexts**.
- Encourage the **creation of a committee/forum in Member States where they do not yet exist** and monitor planned efforts to ensure establishment progresses within a reasonable timeframe
- **Review** the **actions taken by National Payment Committees** and any identified issues in **6 months'** time via a **follow-up (written) stock-take**.