25 July 2025

FSB taskforce on legal, regulatory and supervisory matters (LRS Taskforce)

Monday 30 June 2025 (Basel)

Summary

The LRS Taskforce held an in-person workshop on payment fraud to discuss current risks and trends, public and private sector initiatives, and relevant international work. From the outset, the G20 Roadmap for Enhancing Cross-border Payments has emphasised the importance of ensuring safety and security while improving the cost, speed, accessibility, and transparency of cross-border payments. In light of increased digitalisation and innovative technologies enabling faster payments, mitigating and addressing financial scams and fraud has become even more important to ensure trust in payment services. The workshop was attended by LRS Taskforce members and subject matter experts. The workshop provided an opportunity for the private and public sector to develop a common understanding of the current risks and trends as well as share experiences in addressing payment fraud, which is a growing concern for stakeholders worldwide. The workshop will inform the FSB's work for progressing the G20 Roadmap goals.

1. Current risks and trends

Both public and private sector stakeholders expressed concerns in the increasing trend of payments fraud. Some recurring themes from the discussion include:

- **Cross-border payments have particular vulnerabilities related to payments fraud.** While there can be difficulty in assessing how much fraud is currently occurring in cross-border payments as compared to domestic payments, several participants stressed the increasing potential for fraudsters to target cross-border payments due to their size and lack of cross-jurisdictional approaches for addressing fraud, including the lack of effective measures to recover funds. As such, appropriate controls need to be in place to ensure faster payments do not lead to faster fraud or scams

- **Payment fraud requires a comprehensive approach to cover the whole transaction chain beyond the financial sector.** Participants noted the linkage between telecommunication services, social media services, and payment services and stressed the need to involve all relevant sectors to prevent, detect, and react to fraud. It was also emphasised that a reconsideration of traditional

frameworks for financial loss sharing and data sharing may be warranted to include the non-financial sector.

- **Innovative technologies can be leveraged for addressing fraud risk but may be exploited by fraudsters.** The financial sector can utilise innovative technologies to address fraud risk including for monitoring transactions. However, fraudsters can also exploit innovative technologies to manipulate payment service users in ways that can be difficult for payment service providers (PSPs) to detect. Technology is enabling sophistication in fraud techniques with different fraud types having different relevance for jurisdictions according to factors such as payment system development, payment behaviour and social norm. Participants also noted the large investment necessary for PSPs to keep pace with developments in anti-fraud technology and the need to consider leveraging such technology at the design phase of payment infrastructure. This could enable building in risk-based frictions which balance user needs for frictionless payments with ensuring appropriate security measures to prevent fraudulent payments.

2. Public and private sector initiatives relevant for payment fraud

Participants shared initiatives to address fraud and discussed potential areas of work which could enhance payment fraud mitigation. The various initiatives that were raised indicated the heightened interest of all stakeholders involved and the importance of coordinating across sectors and jurisdictions to establish an effective approach against payment fraud. Some recurring themes from the discussion include:

- **A common taxonomy could provide a sound basis to ensure common understanding and support any future work related to payment fraud.** Discussion of initiatives among participants revealed that terminology such as fraud or scams and how they are used may differ by jurisdiction or sector. To ensure common understanding, some participants suggested defining a minimum set of terms related to fraud and scam including their typology. That said, a note of caution was raised against focusing extensively on taxonomy as it could deter swift policy actions from being developed.

- **The public sector is undertaking various domestic initiatives to address fraud while initiatives addressing cross-border challenges are nascent.** Domestic initiatives include: setting up national frameworks to coordinate public and private sector stakeholders to agree on guidelines for fraud reimbursement or to organise consumer awareness campaigns; targeting standardisation of fraud reporting and information-sharing to improve detection and prevention; introducing confirmation of payee mechanisms or obliging customer authentication processes; establishing a platform for PSPs to connect and share fraud information; codifying a framework for reimbursing certain fraud victims with the aim of incentivising PSPs to improve risk-based management of fraud; and introducing measures to enable sharing of fraud data between PSPs and to enhance the framework on fraud victim protection.

- **Private sector initiatives to address fraud can benefit from cross-sector collaboration and public sector support.** Private sector initiatives include: fraud signal sharing involving tech companies and credit card networks with the potential for expansion to include the banking sector; increasing resilience to fraud by adopting technological capabilities and aligning this with user needs to ensure sufficient adoption; engaging with consumer protection authorities and their associations to ensure holistic coverage of relevant sectors; analysing the fraud chain involving a cross-border payment, leveraging the visibility of individual institutions (i.e. banks and platform companies), and sharing the analysis among stakeholders in the chain. Multiple participants raised legal uncertainty as a recurring issue for sharing fraud or financial crime related information and data, particularly cross-border. Relatedly, there were comments on siloed approaches among authorities which could complicate information sharing among private sector stakeholders.