Fraud, theft and AML prevention

1. Accelerating sophistication of fraud requires a whole-ecosystem approach

1.1 Fraud is becoming faster, smarter and more devastating

The Chair initiated proceedings by acknowledging that losses stemming from payment fraud exceeded €4 billion in 2022, as estimated by the European Banking Authority (EBA), and a substantial increase can be anticipated for the current year. Fraud is becoming faster, smarter and more devastating. While digitalisation offers opportunities for innovation, efficiency and financial inclusion, it simultaneously reshapes risks and expands avenues for fraudulent activity.

1.2 Social media and messaging platforms are central fraud enablers

A regulator detailed findings from national risk assessments conducted in Malta, which identified three key sectors experiencing prevalent fraudulent activity: the crypto asset sector, the e-money sector, and payment processing services. Specific areas of concern include investment scams, identity theft, and increasingly sophisticated document forgery, including instances of forged licences issued by the Malta Financial Services Authority (MFSA) used to defraud banks and other financial institutions.

There are three critical questions for regulators to address. The first is whether financial institutions have implemented appropriately robust internal controls, processes and procedures capable of identifying potentially fraudulent activities. The second is whether supervisors maintain effective cooperation arrangements with fellow supervisory bodies and law enforcement agencies to identify emerging trends and respond effectively. The third is the adequacy of regulation governing social media platforms, given their increasing use as tools for perpetrating fraud.

An industry representative acknowledged the illustrative power of the opening anecdote, noting that it accurately reflects current fraud patterns observed within the industry. Criminals exploit aspects of human psychology, crafting scenarios that create a false sense of urgency, appealing to emotional vulnerabilities and impersonating trusted organisations. It is not solely a payment issue, and concerns where individuals initially encounter scams, including social media platforms, messaging applications, SMS communications, search engines and advertising networks. A holistic approach addressing the entire ecosystem is integral to effective solutions.

1.3 Fraud and money laundering are intrinsically linked and must not be treated in silos

A regulator underscored that both preventing fraud and combating money laundering are shared responsibilities that involve collaboration between EU institutions and Member States, as well as between the public sector and private industry. Fraud and money laundering are often intrinsically linked, as fraudulent activities generate illicit proceeds that are then subject to integration into the financial system through money laundering processes, which anti-money laundering (AML) frameworks are designed to stop.

Fraud is not just a matter for the police and of consumer protection; it is a major source of criminal profits through money laundering. Treating these issues in isolation risks creating significant blind spots. Fraud and money laundering are not issues to respond to in silos, because the identification of suspicious transactions often begins with the detection of fraud signals. Despite differences in the industry players' developments, there are technological advances that can support in those efforts, that enhance efficiency and accuracy.

2. Outdated controls and regulatory gaps leave critical vulnerabilities

2.1 Internal fraud controls and supervision efforts remain inconsistent and fragmented

A regulator stated that their organisation actively engages through a financial crime task force comprised of representatives from supervisory authorities, the Financial Intelligence Analysis Unit (FIAU) and law enforcement, alongside ongoing consideration of how to address the role of social media in facilitating fraudulent schemes.

The Chair asked how supervisors are adapting their approach to keep pace with the evolving fraud practices. A Regulator detailed three areas where supervisory approaches have been adapted within Denmark. The first involves increased dialogue across the entire fraud ecosystem, encompassing formal and informal fora with industry colleagues, law enforcement agencies and telecommunications providers, with recognition that no single entity can effectively combat fraud in isolation. Secondly, Danish supervisors conducted a thematic inspection of banks' anti-fraud measures, which provided valuable insights into existing practices and revealed significant disparities in preparedness among institutions, with some doing a great deal and others not. This lack of consistency in implementation is surprising, given the reputational, financial and broader societal risks associated with fraud.

2.2 PSD2 lacks sufficient emphasis on fraud risks

A regulator stated that Denmark has increased its focus on identifying and addressing providers of financial services operating without appropriate licences. Within the last month, the Danish Financial Supervisory Authority (DFSA) issued warnings against seven such

companies. This represents a challenge due to the reactive nature of such efforts, as they typically only occur after individuals have been defrauded, and there is limited legal authority to proactively intervene. Payment Services Directive 2 (PSD2) lacks sufficient emphasis on fraud risks, and it is hoped that the forthcoming PSD3 Payment Services Regulation (PSR) will address those shortcomings.

The Chair confirmed that point will be addressed with private sector colleagues and asked about the relevance of national measures in conjunction with EU-wide legislation like PSD3, particularly concerning evolving fraud risks.

A regulator emphasised the strong desire there is for a flexible regulatory framework that allows organisations to take steps to combat the evolving crime. It is a highly dynamic area, and companies need to be able to adapt. However, detailed regulation is often necessary to ensure some action is taken, as often without those details nothing is done. The direction of PSD/PSR appears to be leaning towards more prescriptive measures. National measures remain relevant, as they address legal areas not yet harmonised across Europe, such as bankruptcy law and court systems, or discrepancies in how something like gross negligence is defined. Until that is all harmonised, the need for national initiatives will persist.

2.3 AML and fraud prevention lack the speed, scale and coordination required

The Chair referred to discussions the previous day regarding the development of an IT infrastructure for information sharing to ensure fraud prevention. The issue is pertinent not only to regulations such as PSD3 and AML regulations, but also to the General Data Protection Regulation (GDPR), thereby complicating the undertaking.

An industry representative highlighted that there is an ongoing 'arms race', with increasingly sophisticated fraudsters also utilising generative AI. Fraudsters only need to be successful once, and with a 40% success rate, as another industry participant had identified, they can repeatedly generate new identities. Attacks can be seen that successfully navigate know your customer (KYC) and stepped-up KYC procedures, selfie checks and likeness detection measures.

3. Moving towards risk-based and technology-driven security solutions

3.1 Passwords are the weakest link: transitioning to phishing-resistant authentication

An industry representative reported that their firm sees a high level of sophistication in criminal activity targeting areas that have received less attention recently, such as unauthorised fraud and account takeovers. There are persistent issues with people using weak passwords, password reuse, data breaches and the prevalence of credential stuffing attacks. Fraudsters are adapting to controls implemented by payment service providers (PSPs), specifically authentication measures, by employing sophisticated techniques like SIM-swapping attacks and utilising readily available phishing kits to create deceptive websites designed to steal credentials, including both passwords and one-time passwords (OTPs) delivered via SMS.

Social engineering is used in that respect as well, and people can be convinced to share their credentials rather than being defrauded through making payments directly. There is a prevailing focus on addressing fraud occurring when individuals are deceived into making payments, but there should simultaneously be a strengthening of account security measures. Moving forward involves removing the reliance on passwords, as they are the weakest link in authentication controls. Resilient methods resistant to phishing, social engineering and credential theft should be shifted to, alongside enhanced collaboration across multiple industries, given the multifaceted nature of the problem.

Furthermore, industry players can actively work to reduce the reliance on passwords by championing phishing-resistant authentication methods such as passkeys, which are cryptographic key pairs that are more secure than traditional passwords and demonstrate good results.

3.2 AI-powered tools and behavioural biometrics offer new fraud detection capabilities

An industry representative commented that their firm's approach centres on leveraging scale and data. For any card payment, there is a 92% chance that the firm has seen the card before, enabling its platform to mobilise a comprehensive data picture and assess activity against established patterns. The company has integrated machine learning and AI from its inception. Recently, it incorporated large language models to interpret payments as kinds of linguistic structures. This allows for generalisation of the models to not only to detect fraud and money laundering, and to facilitate low-risk payments, thereby increasing speed and adoption rates. This innovation has yielded significant results, reducing fraud losses by 30%, increasing merchant conversion rates by 15% and lowering successful attacks overall by 80%.

Both the public and private sectors should adopt a risk-based regulatory approach. Verification methods should move beyond static documents like passports sent as PDFs to include, for example, behavioural biometrics like analysing how individuals hold or tap their phones, historical patterns and location data. These elements collectively contribute to a more comprehensive identity picture that can be actively verified.

3.3 Convenience and security are not mutually exclusive – proportionality is key

An industry representative explained that combining security and convenience is a primary objective, as customer trust relies on both. The most convenient system will not be used if it is not considered safe. Technology plays a crucial role, including transaction

monitoring mechanisms, risk engines, and the use of AI and machine learning. These systems must be continually updated. Beyond this, there can be consideration of the broader ecosystem, recognising that scams are not solely a payments issue and require participation from the likes of social media platforms.

An industry representative argued in favour of a risk-based approach that filters low-risk payments through while applying heightened scrutiny to high-risk transactions, based on factors such as larger sums, unusual geolocations or out-of-pattern behaviours. Transparent communication regarding the rationale behind security measures is also vital to foster customer acceptance; when customers understand why controls are in place, they are more likely to accept them and feel secure. Flexibility in fraud controls is needed to enable swift responses to emerging threats and adjustments for when fraudsters shift their focus. This dynamic approach also allows for the lifting of controls when fraudulent activity subsides. Technology plays a pivotal role in enhancing detection capabilities and potentially facilitating more invisible controls that minimise customer friction.

4. Liability allocation must be fair and society wide

4.1 Clear and fair liability rules are essential for trust and resilience

The Chair referred to the evolving risk patterns and the regulatory landscape and asked about protecting customers and consumers from falling victim to fraud, how liabilities should be allocated and how effective redress can be ensured.

A regulator reported that developments are underway that will deliver more consumer protection through stronger customer authentication, greater transparency, and more direction in terms of liability and refunds. These developments also promote outside court dispute resolution systems. From local experience, the Office of the Arbiter for Financial Services (OAFS) has established guidance on shared liabilities, how liability will be shared and detailing instances when payment processors may be fully or partially liable. This guidance is publicly available to both industry participants and clients. Having such guidance at the European level and having cooperation between the different outside of court mechanisms, are fundamental. Cases of fraud are assessed across Europe, so enhanced consistency in assessing liability is vital.

An industry representative stated that fair and clear liability rules are paramount for maintaining trust in the banking system. Consideration must also be given to the financial stress and harm experienced by fraud victims, particularly when they were unable to prevent the fraud. Placing all liability on banks could incentivise careless behaviour among consumers, creating a moral hazard with long-term negative consequences. High reimbursement rates may also encourage exploitation by fraudsters, leading to even more fraud, and, ultimately, bank losses would increase costs for customers.

4.2 Liability should reflect the ability to prevent fraud, not just the position in the payment flow

An industry representative emphasised that liability should align with the ability to reasonably prevent the fraud. Frauds often originate on social media platforms, and banks are not at the origin of fraud. A societal approach is needed to address this issue, which extends to liability rules. Regulation towards banks should be risk-based rather than overly detailed, allowing them to allocate resources effectively to reduce risks and avoid simply 'ticking boxes'. Continued dialogue between all parties is essential.

The Chair suggested that that raises a sensitive question regarding the distribution of liability between victims and financial institutions.

5. Enhancing cross-border intelligence sharing and collaboration

5.1 Fraud is inherently cross-border, but intelligence-sharing is too slow

The Chair commented that technological innovation has a crucial role to play. Fraud is inherently cross border.

An industry representative stated that effective information sharing is achievable, citing decades of experience in financial crime investigations that demonstrate that public-private collaboration can be successful in significant cases. However, speed and scale are primary obstacles to existing systems. Delays of days or weeks render shared intelligence obsolete by the time it reaches relevant parties. This is a particularly acute issue given the speed that fraudsters work at.

In the first instance, there is a question around the participants that are included. Expanding participation beyond traditional public-private partnerships to include fintech companies, payment providers, social media platforms, and other relevant entities is essential. The amount of data pertinent to understanding fraud networks extends far beyond the regulated sector.

5.2 API-based systems and pre/post-filing SAR mechanisms can enable real-time response

An industry representative highlighted that there are privacy-protecting technologies and various approaches to determining that, within a system, some information can be shared. One approach is pre-filing Suspicious Activity Reports (SARs), enabling proactive collaboration, or there can be post-filing of information. A robust reporting framework, Application programming interface-based (API) sharing capabilities, the right set of partners and the ability to share real-time data are key components of an effective cross-border reporting system.

5.3 GDPR must be clarified to enable protective data sharing for fraud investigations

The Chair agreed about the need for speed and scale and asked how the Anti-Money Laundering Authority (AMLA) can help in facilitating effective cross-border intelligence sharing.

A regulator recounted a personal experience of purchasing items online where a payment was flagged as potentially fraudulent by her bank, which prompted reflection on the infrastructure required by banks for such detection, and current limitations in information sharing. It should be asked why each individual entity must address this issue independently. There are GDPR concerns, but there are potential solutions.

Privacy must be respected, but citizens also need to be protected. Even relatively small attempted fraudulent payments erode trust in the financial sector. There is a shared responsibility for addressing these issues. AMLA is focused on foundational development and staffing, but information sharing and technological enhancement of both AML and fraud prevention will be tasks it takes on. Vigilant engagement with the sector will be undertaken to facilitate these practices and explore effective methods.