FRAUD, THEFT AND AML PREVENTION

CHRISTOPHER P. BUTTIGIEG
Chief Officer Supervision – Malta Financial Services Authority (MFSA)

Effectively mitigating fraud: Coordination and informed supervision

Malta's financial sector has seen steady growth over the past three decades. A pro-regulatory approach that encourages innovation and sustainabile growth, rather than excluding new technologies, has allowed the country to position itself as a forward-thinking jurisdiction. However, with increased openness comes increased risk. As Malta continues to attract investment, efforts have intensified to ensure the financial sector is not exploited for illicit purposes. Central to these efforts is the country's evolving understanding of risk.

Malta's most recent National Risk Assessment (NRA), published in 2023, offers a detailed overview of the jurisdiction's exposure to money laundering and terrorism financing (ML/FT), while also covering a range of predicate offences. Among these, fraud stands out as a concern. The NRA notes that fraud is the most common predicate offence in local financial crime investigations and appears frequently in suspicious transaction reports (STRs) submitted to the Financial Intelligence Analysis Unit (FIAU), affecting both natural and legal persons.

In a 2024 report, the ECB and EBA noted that fraud via payments amounted to €4.3 billion in 2022, with €2 billion recorded in just the first half of 2023. Malta's Arbiter for Financial Services has also observed a growing number of fraud cases. Within financial services, fraud risk is particularly associated with crypto-assets, e-money, and payment processing. The NRA highlights the inherently non-face-to-face nature of these sectors as a key vulnerability, with threats such as investment scams, identity theft, and document forgery frequently reported. These same sectors are central to Malta's strategic vision for financial services and have received increased supervisory attention.

Malta's supervisory and law enforcement model is decentralised, with the Malta Financial Services Authority (MFSA), the FIAU, the Sanctions Monitoring Board, the Central Bank of Malta and the Malta Business Registry, holding distinct mandates. However, effectively mitigating fraud requires coordination and informed supervision. Authorities must identify areas of convergence while avoiding duplicated efforts. By aligning supervisory tools and leveraging infrastructure, agencies can act more swiftly and base decisions on broader information. This article focuses on the MFSA approach and inter-agency cooperation in the fight against fraud.

As Malta's single financial regulator, the MFSA is the primary gatekeeper to the financial sector. Its mandate spans licensing, supervision, and maintaining sectoral integrity. While not an AMLCFT authority (the FIAU is the AMLCFT Authority for Malta), the MFSA incorporates financial crime considerations across its operations, making it a key stakeholder in the national framework. This is reflected in its strategy, guidance, and risk-based supervision.

Central to the MFSA's methodology is ensuring that unsuitable actors are denied access to the financial system. This includes rigorous competence and fitness assessments of Money Laundering Reporting Officers (MLROs), who are critical to detecting and reporting suspicious activity. The MFSA's guidance to MLROs addresses governance, conflicts of interest, resource needs, and internal awareness. These issues are not only relevant to AML/CFT, but also to fraud prevention.

This approach has led to the generation of additional supervisory information. In 2024, alongside 35 STRs, the MFSA submitted 6 'red flag reports' to the FIAU on issues that were deemed significant for early prevention or identification. This reflects the growing inter-agency cooperation and more efficient sharing of insights. The MFSA also shares information with the Police, Attorney General, and Courts when requested.

Another important element in fraud prevention is the MFSA's publication of warnings about entities misusing or imitating legitimate license holders. These alerts protect consumers, raise awareness, and provide early indicators of potential scams. They are a valuable tool for promoting transparency and safeguarding market integrity.

Looking ahead, national authorities must adopt increasingly data-driven tools to address complex financial crime risks. Data analytics can improve detection capabilities and support faster, more informed decisions. These innovations should build on the holistic supervisory frameworks already in place, like those applied by the MFSA, to increase the sector's resilience to fraud.

Finally, there is a growing case for greater focus on fraud within supervisory strategies. The EU's work on AML/CFT harmonisation provides a useful model. While the new AML legislative package is primarily focused on ML/FT, it could also accommodate fraud-related risks where overlaps occur. Aligning national fraud mitigation strategies with EU-level reforms can promote consistency, reduce vulnerabilities, and strengthen the broader fight against financial crime.

SARA MELLA
Head of Personal Banking – Nordea Bank

Fighting fraud together across society

Fraud is a severe problem, not only for the financial industry and its customers, but for the society as a whole. Proceeds from fraud often finance other criminal activities such as drugs, weapons and trafficking. This is why Nordea takes fraud very seriously and has invested heavily in resources, technology, products and processes to combat fraud to protect our customers and their assets. We consider this a key part of our social responsibility.

Online banking and digitalisation – convenient for customers but often exploited by fraudsters

In the wakes of digitalisation, banking services have become available 24/7/365. Whilst being very beneficial to customers, fraudsters have in several ways relentlessly and rapidly taken advantage of the new digital era of remote, non-physical, access to banking. In Nordea, many different kinds of online banking fraud attempts have been observed. Through intelligence, monitoring and collaboration, both internally in Nordea and externally, we learn about new threats the second they emerge. Thanks to the cross-Nordic presence, we are often prepared as fraud types propagate from one Nordic country to another.

> To successfully combat fraud in society, it requires that every part of the value chain takes own and adequate action.

Different types of social engineering have been the most dominant fraud type in Nordic online banking over the last years. Manipulation via phishing, vishing, smishing, investment- and romance scams has dominated the Nordic fraud picture. The fraudsters are becoming more and more sophisticated in their attempts to lure the customers to take desired action e.g., using fake web page from well-known government agencies. This requires the customers to become even more vigilant in their on-line presence. In fact 70 per cent of the fraudulent money transfers are initiated by the customer themselves.

Stay ahead of the curve – with a dynamic and flexible control environment

Nordea continues to enhance its fraud prevention and detection capabilities by implementing detection systems and several other mitigating actions. Apart from the advanced detection systems per se, with multi-layered monitoring, other successful fraud mitigation actions have been the introduction of payment limits, the cooperation between banks and other institutions, Nordea's Nordic coverage and importantly a focus on customer awareness. With social engineering being the dominating modus used by fraudsters, educating customers on how to avoid being defrauded has proven very successful and is much appreciated by customers.

Further collaboration across the industries and with authorities is key to combat fraud

To successfully combat fraud in society, it requires that every part of the value chain continue to take own and adequate action. Even more cooperation between several parties like authorities, network operators, social media platforms, financial institutions etc. is required as well as continued focus on informing society about any new threats. Again, customer awareness is key in preventing fraud based on social engineering.

How can the regulatory environment and policy setting support collaboration?

Regulations and policies, primarily in the areas of data sharing need to be less rigid in order for banks to quicker share fraud intelligence with other financial institutions etc. to support early identification of new modus, improvement of detection systems and quicker identification of fraud networks. Also, legislations enforcing rapid payments, like EU's Instant Payment Regulation (IPR), whilst of course enhancing the customer's payment experience, complicate fraud prevention, as well as anti-money laundering/counter terrorist financing (AML/CTF). Such legislations must be aligned with legislations dictating fraud prevention, e.g. the coming Payment Service Regulation (PSR), such that they are not conflicting but rather jointly boost both the customer payment journey as well as fraud prevention and AML/CTF.

With harmonised legislation as a foundation, more flexible possibilities for data sharing, we can easier join forces and take common actions to even better prevent fraud attacks in the future, without obstructing or complicating the customer payment journey. Nordea stays committed to duly fulfil our role in the joint societal fight against fraud.

FABRICE BORSELLO
Chief Compliance Officer and Authorized Manager – PayPal (Europe) Sarl et Cie S.C.A.

Rethinking fraud prevention in a digitally connected world

In today's hyper-connected world, fraud is evolving faster than ever before. Our digital lifestyles - online shopping, digital banking, social media - bring convenience but also create fertile ground for cybercriminals. Individuals and businesses now face increasingly sophisticated forms of fraud.

While technology enhances customer experiences, it also equips fraudsters with advanced tools like artificial intelligence to conduct sophisticated phishing attacks or create deep-fake videos and synthetic identities on an unprecedented scale. Fraud is not new and unlikely to be fully eradicated given human behavior and criminal adaptability. The focus should therefore be on minimizing its impact through prevention, early detection, and agile response.

The EU's Payment Services Directive review (PSD3/R) signals strong commitment to boosting fraud safeguards and consumer protection. However, the traditional "one-size-fits-all" approach with static thresholds and uniform rules is no longer effective given diverse consumer behaviors and evolving fraud tactics.

As legislative discussions progress, two paradigm shifts are urgently needed to equip the digital ecosystem with more effective tools for preventing fraud.

1. Future-proofing the fraud prevention toolbox

Payment Service Providers (PSP) are deploying increasingly advanced fraud prevention tools to tackle new threats. For instance, PayPal's new AI-powered scam alert system delivers dynamic warnings to consumers according to transaction risk.

It is equally crucial to continue evolving existing tools - like Strong Customer Authentication (SCA) - to ensure they remain effective. Attackers now target the technical elements of SCA, using phishing, malware, and data breaches to steal passwords, fueling credential stuffing attacks. Techniques like SIM swapping and social engineering have diminished the value of SMS one-time passwords (OTP).

This calls for moving beyond static SCA toward adaptive, risk-based authentication frameworks, enabling PSPs to adopt approaches that are innovative and resilient. Passkeys, for example, offer robust, phishing-resistant authentication, allowing users to sign in with biometrics (fingerprint or face scan), removing reliance on traditional passwords.

Failing to modernize SCA under the PSD3/R framework risks locking in outdated practices, limiting PSPs' ability to strengthen defenses while fraudsters continue to evolve and exploit static security measures.

2. Tackling fraud requires an ecosystem-wide approach

Today's fraud patterns are clear: fraudsters are using technology to exploit human trust—manipulating consumers into authorizing fraudulent payments via impersonation and emotional tactics. Most scams target individuals long before the payment itself.

This points to a broader reality: modern fraud extends well beyond the financial sector. It spreads across a complex digital ecosystem that includes social media platforms, online marketplaces, search engines, ad networks, telecoms, and messaging apps - many of which fall outside traditional financial regulation.

Improved intelligence sharing both among PSPs and across sectors is essential to tackle sophisticated, organized, cross-border fraud. Yet, collaboration alone is not enough: all actors in the ecosystem must implement controls to prevent and mitigate fraud on their own platforms. While some national or corporate initiatives exist, efforts remain fragmented and inadequate.

Current policy discussions, including under PSD3/R, continue to focus on the responsibilities of banks and PSPs. Far less attention is given to other ecosystem actors in proactive prevention, despite the urgency of addressing fraud at every stage of the fraud chain.

> The EU must modernise its fraud prevention framework to ensure consumers stay protected.

What is needed is a coordinated, EU-wide, cross-sector fraud prevention strategy that goes beyond isolated measures, bringing all actors in the fraud chain under a common framework. Such a strategy should establish clear accountability for each sector's role, incentivise proactive risk management, and introduce shared liability mechanisms to ensure that the burden of protecting consumers does not rest on PSPs alone.

To conclude, as the EU shapes the future of digital payments, it must also modernize its fraud prevention framework. This includes future-proofing security standards like SCA under PSD3/R and adopting an EU-wide cross-sector approach aligning incentives, responsibilities, and liability. Only bold, coordinated action will keep pace with sophisticated fraud threats to ensure consumers stay protected.

MARC FUNGARD
Global Regulatory Compliance & Enterprise Risk Lead – Stripe

Building trust in digital payments: How AI can help combat fraud

Digital fraud scales proportionally with the digital economy; global online payment fraud losses in 2024 surpassed $44.3 billion. Beyond payment fraud's immediate financial losses, businesses also face potential erosion of customer trust and loyalty, as well as increased scrutiny from regulators and law enforcement agencies. To combat this growing threat, organizations, like Stripe, have harnessed innovative new technologies, including artificial intelligence.

Artificial intelligence offers powerful and adaptive solutions to tackle the complex and evolving nature of payment fraud. Stripe's approach mobilises large datasets and advanced algorithms, to identify indications of fraudulent behavior in real time. Our approach seeks to protect our users, their customers, and the ecosystem to create a secure environment for payments. As a platform serving millions of merchants over billions of transactions and trillions of payment volume, Stripe is well positioned to detect and adapt to new fraud patterns quickly. To effectively prevent fraudsters from onboarding onto the platform, Stripe employs advanced AI-driven models that analyze various data points during the account creation process.

The AI models are also used to detect and block fraud in real time, analyzing a payment in just 100 milliseconds. At Stripe, we're also seeing how an LLM-style approach can help with fighting fraud. So we built a payments foundation model—a self-supervised network that learns dense, general-purpose vectors for every transaction, much like a language model embeds words. Trained on tens of billions of transactions, it distills each charge's key signals into a single, versatile embedding. And these efforts have worked well: +15% conversion, -30% fraud.

These models are constantly learning and improving, notably to reduce card testing among other fraud typologies. Card testing is a type of fraud where criminals use stolen card numbers to make small purchases to verify their validity. That's why the systems we use to prevent it need to be both accurate—correctly distinguishing card testing from legitimate traffic, with rapid detection and retraining—and nimble, built to adapt to the evolving landscape of threats. Our approach has shown significant benefit in recent years—successful attacks on merchants served by Stripe have decreased by 80% over the last two years, even as Stripe's payment volume had expanded to over $1 trillion last year. AI allows the creation of dynamic, risk-based fraud-prevention rules, automatically adjusted based on the evolving threat landscape, providing a flexible and powerful defense against new fraud vectors.

Fraud models often face a tradeoff between security and successful authorization; our recent AI enhancements have expanded the frontier, allowing merchants to optimise their payment performance while also better protecting against fraud. Stripe addresses this issue through an AI-powered product designed to increase payment acceptance, in part by recovering false declines and intelligently retrying payments. As a result of these continuous improvements, the average authorization rate has improved by 61 basis points since its launch.

In a landscape where fraudsters leverage AI to discover innovative ways to bypass financial institutions' controls on a large scale, traditional methods of combating fraud have become obsolete. Technology and innovation are playing an increasingly vital role in detecting and preventing fraud, consequently, the fight against fraud must involve using AI to counteract AI.

AI offers powerful and adaptive solutions to tackle the complex and evolving payment frauds.

To achieve this, we've found that effective regulation facilitates innovation rather than imposes fixed technological solutions that may soon become outdated. Firms should be encouraged to adopt a risk-based approach that incorporates technology to enhance risk management practices from the onboarding stage onward. Specifically, model-based transaction monitoring and fraud detection systems should be utilized to effectively identify and mitigate risks. Additionally, such an approach should include and leverage non-traditional technological data to identify a user. This dual approach fosters a more robust and proactive risk management framework. Traditional regulatory frameworks—built from the underlying presumption of an in-person interaction based on a physical proof of identity—are rapidly becoming outmoded. Incentivizing an improved risk-based approach to combat fraud and other financial crimes would allow financial institutions and their customers to innovate flexibly while requiring them to demonstrate improved effectiveness with emerging AI approaches.