The future of fraud in Europe

October 2026



The better the question. The better the answer.
The better the world works.

EY
Shape the future with confidence



Executive Summary

Continued investment, innovation and collaboration could materially reduce fraud losses across Europe by 2030.

The future of fraud in Europe is not inevitable. How the ecosystem responds today will shape the scale and impact of fraud through to 2030 and beyond. The analysis shows that continued progress in technology-enabled detection, intelligence sharing and coordinated prevention could avoid a cumulation of around €6 billion in fraud losses by 2030. However, maintaining this progress will require defensive capabilities to continue evolving as criminal tactics become more sophisticated.

Fraud is evolving, but its future trajectory is not predetermined. Organised criminal networks are leveraging technological advancements to automate, scale and personalise fraud attacks, increasing the volume and success of attempts. Improvements in defences across the industry are aiding fraud prevention however the adaptive nature of fraudsters and advances in AI and technology provide ongoing challenges to mitigating and reducing fraud losses.

The fraud landscape is shifting

+10%
Reported fraudulent transactions in the European Economic Area (EEA) in 2024

€5.6 billion
The total value of fraud increasing by 15% from 2023

Approx. 70%*
Reported fraud is concentrated in the UK, France, Germany, Spain, Italy and Belgium

Data Source: EBA 2025 Report on Payment Fraud and UK Finance Annual Fraud Report 2026.

**The concentration largely reflects the size, digital maturity and payment volumes of these markets, alongside differences in payment behaviour and fraud reporting. Larger, highly digitised payments ecosystems naturally have greater absolute exposure to fraud, while developed monitoring and reporting frameworks can increase the visibility of losses.*

Not only is the scale of fraud increasing, but the way in which fraud is conducted is evolving. AI advancements and the digitalisation of payment channels are allowing fraudsters to exploit trust and human behaviour to bypass authentication and payment controls. Conversely, traditional methods targeting payment accounts or credentials are declining in response to strengthened authentication and security controls.[1]

1 Visa Spring 2026 Biannual Threats Report

The industry has demonstrated resilience and agility adapting to new risks

The rapid advancement of AI and automation is accelerating the industrialisation of fraud, enabling criminal networks to operate with greater scale, speed and sophistication. At the same time, these technologies are strengthening the industry's ability to detect suspicious activity, identify emerging patterns and prevent fraud at scale. Alongside this, industry, regulators and law enforcement are strengthening collaboration and investing in advanced fraud prevention capabilities, helping to build a more resilient payment ecosystem in the face of evolving threats.



"Over the next decade, the most significant fraud threats in Europe will emerge from the combination of increasingly sophisticated criminal networks, AI-enabled deception, and the growing interconnectedness of digital markets. No single organisation can address these risks alone. Success will depend on trusted collaboration between industry, government, and technology providers, supported by responsible data sharing and a collective commitment to protecting consumers and businesses.

Elie Beyrouthy, Chair of the European Payment Institutions Federation (EPIF)

"Fraud continues to operate on an industrial scale, harming consumers and businesses, while funding serious and organised crime in the UK and beyond. As fraud becomes increasingly sophisticated, failing to tackle its root causes will only allow the problem to grow. The Future of Fraud report is an important warning of the scale of the challenge we face and the need for a strong response. Only through collective action, sharing intelligence and disrupting fraud before it reaches the point of payment, can we reduce harm and stop criminal gangs profiting from these devastating crimes.

Ruth Ray, Managing Director, Economic Crime, UK Finance

"Fraud does not begin or stop at the boundaries of the banking sector, and neither can our response. Banks have a crucial role to play, but protecting consumers requires coordinated action across the whole digital fraud ecosystem. Closer cooperation between banks, technology companies, telecom operators, online platforms and public authorities, and better information-sharing to enable the swift takedown of fraudulent content on online platforms will help Europe respond more effectively as fraud continues to evolve.

Alexandra Maniati, Senior Director, Innovation & Cybersecurity, European Banking Federation (EBF)

Looking ahead to 2030

Three overarching themes are expected to shape the future of fraud, influencing both the tactics used by fraudsters and the capabilities required to prevent and combat fraud effectively.

AI and the industrialisation of fraud

- AI is accelerating the industrialisation of fraud enabling fraudsters to scale deepfake impersonation, social engineering, automated account testing and Fraud-as-a-Service operations.
- At the same time, AI is already central to fraud prevention, supporting real-time risk analysis, anomaly detection, authentication and network-level monitoring.

Displacement of fraud

- Fraudsters continuously adapt to new controls, shifting attacks across the payment journey to exploit emerging vulnerabilities.
- Fraud is increasingly focused on the manipulation of legitimate users, credential fraud and wallet compromise.
- In parallel, first party fraud is growing through the misuse of customer protection mechanisms.

The evolving payments ecosystem

- The payments ecosystem has become faster and more interconnected, making fraud harder to disrupt and recover.
- Faster payments, mule networks and digital assets such as stablecoins are enabling fraud proceeds to be moved rapidly across jurisdictions.
- Emerging technologies such as adaptive authentication are strengthening payment security and reducing the risk of credential compromise.

Four scenarios have been developed to illustrate how fraud losses may evolve to 2030

To evaluate how fraud may evolve between now and 2030 in Europe, four scenarios were analysed against a "no-change" baseline.[2] Bringing together some of the key challenges facing the payment industry and potential defensive responses, the scenarios compare two adverse pathways (downside scenarios) to two prevention-led ones (upside scenarios).

These scenarios are not predictions and are not considered equally likely. They illustrate how different levels of industry investment, collaboration and criminal capability could influence outcomes. Current industry investment and regulatory initiatives mean that elements of the prevention-led scenarios are already under way. Sustaining and expanding these efforts will be critical to achieving the more favourable outcomes. Additionally, the scenarios may occur in tandem meaning the coupling of prevention efforts could drive down fraud losses further than what is illustrated in the analysis.

No additional prevention action occurs

Technology arms race where fraudsters outpace defences

Fraudsters exploit advanced AI, autonomous agents and synthetic identities faster than institutions can adapt their defences.

Organised crime and fraud-as-a-service grows

Fraud evolves further into a highly specialised and globally connected industry where criminal groups buy technology, victim information, identity creation and laundering capabilities as services.

Additional prevention action occurs

Technology arms race offset by defences

Institutions collaborate and react and adapt to advancements deploying targeted defences reducing the expected impact on fraud.

Public and private data sharing is widespread

Participants share intelligence in near real time, transforming fraud prevention from an institutional challenge into an ecosystem capability.

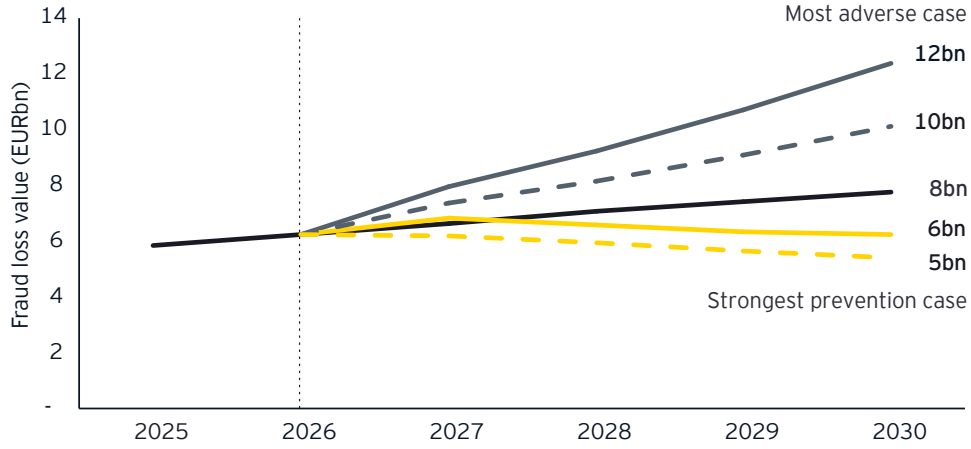
2 The modelling excludes the payment channel direct debits due to a lack of available data for the European area. The total fraud loss is therefore likely to understate total figures. Fraud trajectories are for illustrative purposes only; they do not predict the actual future fraud losses. Scenarios are not additive. Figures are rounded; totals and percentages are based on unrounded values.



Collaboration and investment in defences can materially change the trajectory of fraud losses

In the downside scenarios where no additional prevention action occurs, fraud losses could rise to €12 billion by 2030 if technology-enabled crime outpaces defences, or to €10 billion if organised criminal activity becomes further industrialised. By contrast, in the upside scenarios where additional prevention occurs, losses could fall to €6 billion where technology strengthens defences, or €5 billion under widespread data and intelligence sharing alongside defensive responses.

Europe level fraud loss values (EURbn) from 2025–2030



€7 billion

Difference in fraud losses where collaboration and data sharing is widespread, the strongest prevention case, to where fraudsters take advantage of AI and technology without defences in place, the most adverse case.

€6 billion

In cumulative avoided fraud losses over the next four years in the strongest prevention case where collaboration and data sharing is widespread, when compared to the baseline over the same period.

Baseline

Upside scenarios:
- Technology arms race offset by defences
- Widespread data sharing

Downside scenarios:
- Technology arms race outpaces defences
- Industrialised crime grows

The evaluation of these different fraud pathways illustrates that the emerging risks have implications for the payment ecosystem, while equally there are opportunities to advance defensive capabilities and a coordinated ecosystem response.

How the industry could respond to the risks and opportunities:

AI fraud and defence

- AI-driven fraud detection
- Stronger identity and authentication solutions
- Enhanced real-time decision making
- Maintaining consumer trust in digital payments.

Organised crime disruption

- Intelligence-led disruption
- Mule account identification
- Cross-border collaboration
- Coordinated enforcement efforts.

Data enabled defences

- Widespread reporting and intelligence sharing
- Common data standards and interoperability
- Privacy and governance frameworks
- Collective fraud prevention capabilities.

Ongoing initiatives across Europe are already strengthening collaboration, intelligence sharing and collective resilience. Emerging technologies are also enhancing fraud prevention capabilities year-on-year. All of this provides material benefits for fraud prevention. However, continued cooperation across industry, policymakers and consumers will be essential to keeping pace with evolving fraud threats.

Building on the priority actions identified above, the following recommendations set out practical steps to strengthen the ecosystem's ability to prevent and respond to fraud, enhance collective fraud prevention capabilities and support a more coordinated ecosystem response. Together, they recognise that fraud prevention is a shared responsibility requiring sustained action across all stakeholders.

Recommendations for industry

- Strengthen detection across the full customer lifecycle.
- Strengthen identity assurance across onboarding and recovery.
- Prioritise mule-network disruption.
- Coordinate fraud intelligence and controls at ecosystem level.
- Prepare for frontier AI and quantum technologies.

Recommendations for policymakers

- Evolve regulatory expectations beyond authentication.
- Enhance existing Verification of Payee (VoP) framework to enable the sharing of more detailed counterparty-risk information.
- Enable proportionate, intelligence-led friction.
- Align incentives and responsibilities across the fraud ecosystem.
- Promote harmonised fraud reporting and taxonomy across Europe.

Recommendations for consumers

- Verify unusual requests through a trusted channel.
- Pause and pay attention to typical fraud red flags.
- Apply enhanced checks to investments and alternative assets.
- Act quickly if fraud is suspected and preserve evidence.
- Use available security features offered by financial institutions or service providers.



EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP

The UK firm Ernst & Young LLP is a limited liability partnership registered in England and Wales with registered number OC300001 and is a member firm of Ernst & Young Global Limited.

Ernst & Young LLP, 1 More London Place, London, SE1 2AF.

© 2026 Ernst & Young LLP. Published in the UK.
All Rights Reserved.

UKC-045577.indd (UK) 10/26. Artwork by Creative UK.

ED None

Information in this publication is intended to provide only a general outline of the subjects covered. It should neither be regarded as comprehensive nor sufficient for making decisions, nor should it be used in place of professional advice. Ernst & Young LLP accepts no responsibility for any loss arising from any action taken or not taken by anyone using this material.

ey.com/uk