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

Contents

Foreword 2

1. Executive Summary 4

2. Introduction: a rapidly evolving fraud landscape 9

3. Emerging and future fraud risks 14
   - 3.1. Overview 14
   - 3.2. AI and the industrialisation of fraud 15
   - 3.3. Displacement of fraud 17
   - 3.4. The evolving payments ecosystem 20
   - 3.5. Other emerging fraud risks 21
   - 3.6. The evolving defence ecosystem 24

4. Trajectory of fraud losses to 2030 25
   - 4.1. Overview 26
   - 4.2. Evaluating the risks and opportunities relevant to the future of fraud 27
   - 4.3. A baseline of fraud in Europe 28
   - 4.4. Assessment of the fraud scenarios 29
   - 4.5. Outcomes and implications 34

5. Preventing the fraud of the future 36
   - 5.1. Overview 36
   - 5.2. Recommendations for industry 37
   - 5.3. Recommendations for policymakers 38
   - 5.4. Recommendations for consumers 40
   - 5.5. Case studies 41

6. Technical Appendix 42
   - 6.1. Overview of the modelling approach 42
   - 6.2. Conceptual framework 42
   - 6.3. Econometric modelling 44
   - 6.4. Data sources 46
   - 6.5. Limitations 47
   - 6.6. Payment channel definitions 48

Foreword

Over the last five years across Europe, extensive effort and resources have been invested into anti-fraud measures from data-sharing and collaboration initiatives to innovation in detection, to consumer awareness campaigns as well as law enforcement and strategic disruption of organised crime. Those efforts have made a meaningful difference – however, the next few years are going to be pivotal in the fight against fraud.

Fraud has always evolved alongside innovation in financial services and payments. What is different today is the speed at which new technologies, payment methods and criminal capabilities are converging, changing not only how fraud is committed, but how quickly it can be scaled.

Across Europe, we are already seeing signs of this shift. AI is making social engineering more convincing and scalable. Deepfakes and synthetic identities are challenging established authentication and identity controls. Criminal groups are becoming increasingly sophisticated, while fraud-as-a-service is lowering the technical barriers to sophisticated attacks.

Many of these developments are still evolving. Some of what we observe today can be viewed as experimentation, but what happens when experimentation becomes industrialised? What happens when AI-enabled deception can be personalised at scale? When synthetic identities and deepfakes become increasingly difficult to distinguish from genuine customers? These questions matter because the future of fraud will not be determined by technology alone. It will be shaped by the interaction between criminal capabilities, payments evolution, regulation, consumer behaviour and the ability of organisations across the payments ecosystem to collaborate and respond.

This report explores these interactions and how they could reshape Europe's fraud landscape through 2030. It considers plausible outcomes, from stronger defences enabled by technology and collaboration to industrialised criminal activity outpacing the ecosystem's response.

Yet the same advances also create a significant opportunity for the anti-fraud ecosystem. AI, advanced analytics, digital identity and real-time intelligence sharing have the potential to identify threats early and enable interventions at a greater pace. The challenge is ensuring defensive capabilities evolve as quickly as the threats they are designed to counter.



Ivan Heard

EY Partner

UK Financial Services Head of Fraud



David Capezza

Chief Risk Officer
(Senior Vice President),
Visa Europe

“

As commerce becomes increasingly digital, trust must remain at the core of how we innovate. That means staying ahead of a fraud landscape that is growing ever more sophisticated, while continually strengthening the technology, intelligence and partnerships needed to fight it.

The scale of the challenge is significant. Since its creation just over two years ago, Visa’s dedicated Scam Disruption team has identified more than €2.2 billion ($2.6 billion) in fraud attempts globally, including more than €1.4 billion ($1.6 billion) uncovered since October 2025. Technology is transforming our ability to detect and disrupt fraud, but staying ahead of evolving threats requires more than technology alone.

We are already working across industry, government and the technology sector to tackle fraud, sharing intelligence, developing new solutions and strengthening our collective defences. But as the threat evolves, our collaboration must evolve with it. We need to go further, particularly on responsible data sharing, shared intelligence and secure innovation. By doing so, we can make it harder for fraudsters to operate, preserve trust in the digital economy, and build a more secure, resilient Europe.



Mette Grolleman

Senior Vice President,
Government Affairs,
Visa Europe

“

Europe has an opportunity to set the standard for a digital economy built on innovation, security and trust. But as fraud evolves, staying ahead will require industry, governments and technology providers to move together, anticipating emerging threats while protecting the significant benefits of digital innovation. Trust isn’t just what makes digital commerce work today; it is what will enable it to grow tomorrow.



1 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.

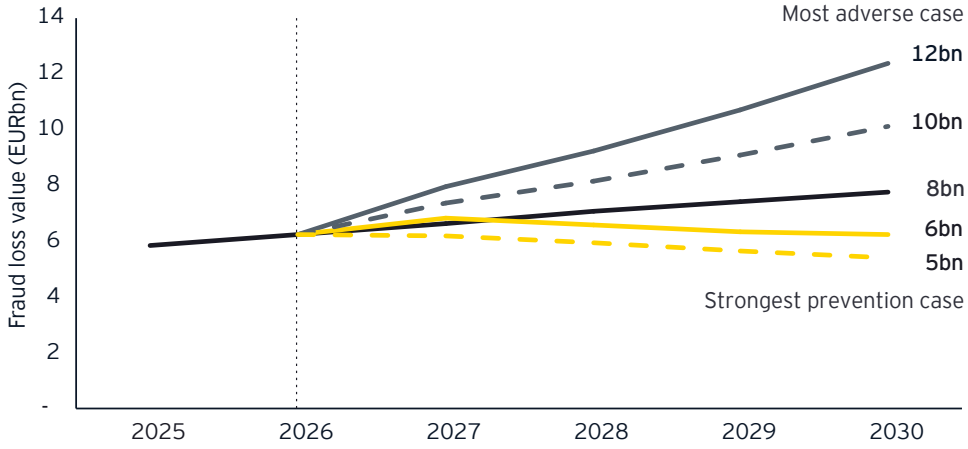
2 The modelling excludes the payment channel direct debits due to a lack of available data for the European area. The total fraud loss is therefore likely to understate total figures. Fraud trajectories are for illustrative purposes only; they do not predict the actual future fraud losses. Scenarios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



2 Introduction: a rapidly evolving fraud landscape

Introduction

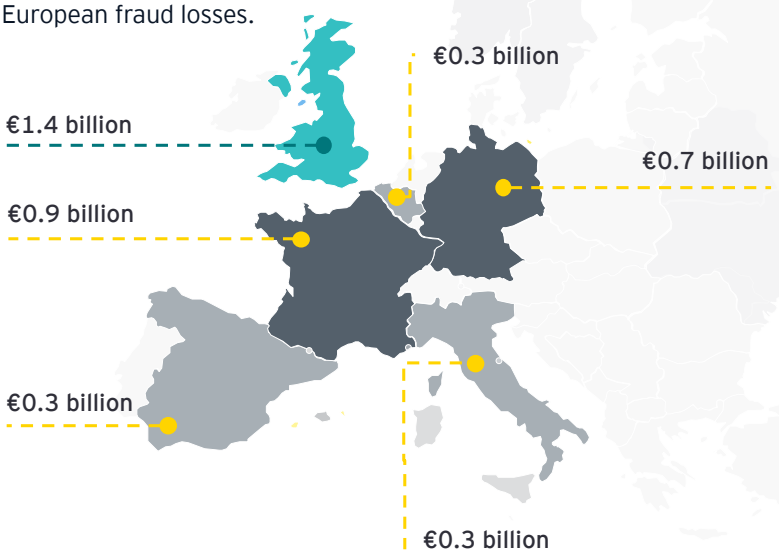
Fraud across Europe is evolving from largely isolated attacks into a more automated, pervasive and organised threat. Fraudsters are now using emerging technologies to personalise deception, create synthetic identities, imitate legitimate customers and businesses, and deploy reusable criminal infrastructure across multiple markets. Although stronger authentication, tokenisation and network-level controls are improving protection against traditional fraud vectors, criminals are redirecting their efforts towards human behaviour, operational processes and less-protected points across the payments ecosystem.

As a result of this evolution, online fraud has become a significant threat in Europe and globally. Europol's spotlight report[3] estimates that online fraud schemes generate billions in illicit profits each year, supported by accessible crime-as-a-service capabilities and adaptable criminal networks. Similarly, INTERPOL's Threat Assessment[4] identifies financial fraud as one of the world's most severe and rapidly evolving transnational crimes, embedded within broader criminal ecosystems involving organised crime, human trafficking and cybercrime.

Our analysis of the 2024 reported data from UK Finance (UKF) and European Banking Authority's (EBA)/European Central Bank (ECB) shows a concentration of fraud across selected European markets.

Absolute fraud losses are concentrated across select European markets:

Around 60% of fraud losses in the European Economic Area are in France, Germany, Spain, Italy and Belgium with the UK also driving the absolute value of reported European fraud losses.



Fraud in the UK is mainly driven by card fraud through remote purchase. Fraud is concentrated in digital channels.

France has the highest card fraud volumes in Europe (about 7 million cases). Credit-transfer fraud, cash and direct-debit fraud are significant contributors.

Germany ranks highly in credit-transfer and direct-debit fraud losses. Direct-debit fraud has a high average loss per incident.

Spain has high card-fraud volumes (greater than 2.5 million cases) but relatively low average losses per incident. Spain leads in cash and direct-debit fraud.

2024 fraud data is sourced from EBA 2025 Report on Payment Fraud and UK Finance Annual Fraud Report 2026.
The UK fraud figure may not be directly comparable to that of other EU countries due to differences in data reporting and collection.

3 Europol Spotlight Report on Online Fraud
4 INTERPOL's 2026 Global Financial Threat Assessment

Absolute losses reflect both fraud exposure, the scale and composition of payment activity. They should not be interpreted as a direct measure of relative fraud performance across markets. Larger and more digitally active markets may account for a greater share of reported fraud partly because they process higher volumes and values of payments. The UK's larger share, for example, should be viewed in the context of the scale and maturity of its financial services and payments market, alongside its relatively developed fraud reporting framework.

The reported figures are unlikely to reflect the full scale of the threat, as many incidents remain unreported. A 2026 European Union (EU)-wide survey of 26,453 respondents by the European Union Agency for Fundamental Rights[5] found that 24% had experienced online fraud during their lifetime, yet only 15% of victims reported the incident to the police. Overall, 44% reported the fraud to a bank, online platform or telecommunications provider. This reporting gap limits visibility of emerging fraud trends and means that official crime and loss statistics may materially understate the prevalence and impact of online fraud.

Despite this limitation, recent reporting demonstrates the scale and changing composition of fraud. This is summarised in the table below:



Indicator	Reported figure	Change/ comparison	What it indicates
European Economic Area (EEA) fraudulent transactions, 2024	19.6m	+10% YoY	Growing volume of reported fraud
EEA fraud value, 2024	€4.2bn	+17% YoY	Fraud value growing faster than incident volumes
EU/EEA payer manipulation in fraudulent credit transfers	71%	Up from 55% in 2023	Shift towards manipulating customers into authorising payments
UK fraud cases, 2025	4.06m	+11% YoY	Continued increase in reported cases
UK unauthorised fraud	£703m	-5% YoY	Traditional fraud losses declining
UK Authorised Push Payment fraud	£576m	+19% YoY	Growth increasingly concentrated in scams/authorised fraud

Source: EBA 2025 Report on Payment Fraud and UK Finance Annual Fraud Report 2026.
The UK fraud figures may not be directly comparable to that of other EU countries due to differences in data reporting and collection.

5 The European Union Agency for Fundamental Rights

Visa's Spring 2026 Biannual Threats Report[6] provides further evidence of this displacement towards scams and customer manipulation, identifying nearly €900m in scam-related activity between July and December 2025. Scams were the largest category of consumer payment fraud identified during the period, reinforcing the broader displacement towards manipulation-based fraud.

This evolution has implications beyond direct financial losses. As fraudsters impersonate trusted individuals, businesses and institutions, and use synthetic content to make fraudulent interactions appear legitimate, consumers may find it increasingly difficult to distinguish genuine communications and payment requests from fraud. The 2026 Global Anti-Scam Alliance data found that 28% of online-fraud victims experienced a loss of trust, while 34% changed their online behaviour following the incident. It also found that 42% of scam victims across Europe had been victimised more than once. These findings demonstrate how fraud can cause persistent consumer harm, weaken confidence in digital identities and payment services and create additional friction across the payment journey.

At the same time, the financial services industry has strengthened targeted prevention through sustained investment in technology, intelligence sharing, customer education and collaboration with law enforcement. UK Finance reported that the financial services industry prevented £1.68 billion of unauthorised fraud in 2025, equivalent to 70p in every £1 attempted. The industry-funded UK's Dedicated Card and Payment Crime Unit also prevented £273 million from being stolen and disrupted 157 serious and organised criminals, while the Banking Protocol prevented a further £58.8 million and supported 136 arrests. Intelligence-sharing arrangements enabled the disruption of 12,438 money mules and the identification of more than 2.7 million compromised card numbers, demonstrating the value of combining technology, intelligence and specialist enforcement to prevent fraud and disrupt the criminal networks behind it.

Stronger security controls are producing measurable benefits, even as attack volumes increase. Visa's Spring 2026 biannual threats report noted that it blocked a 13% increase in unique enumeration attacks at network level between July and December 2025, while losses associated with enumeration declined by 16% and device-token fraud declined by 9.6% year on year. These results demonstrate that AI-enabled detection, tokenisation and network-level controls can improve the identification and prevention of attempted fraud, even as criminals increase the speed, volume and sophistication of their attacks.

This dynamic is creating a technology arms race across the payments ecosystem. As payments become faster, more digital and more distributed, fraudsters are increasingly targeting customer behaviour, digital identities, accounts and merchant relationships, reinforcing the need for controls that operate across the full payment journey.



6 Visa Spring 2026 Biannual Threats Report

This report

In this context, Visa commissioned EY to provide an independent, evidence-based, and forward-looking assessment of how fraud across the European and UK payments ecosystem may evolve to 2030.

Building on historical fraud reporting, this report aims to examine how developments in technology, payment methods, criminal operating models, regulation, liability and industry responses could shape future fraud risks and losses.

Approach

To evaluate how fraud across Europe may evolve to 2030, we developed a structured, evidence-based approach that combines historical fraud and payments data with economic, technological, regulatory and societal indicators. The analysis is underpinned by a half-yearly dataset covering 28 jurisdictions from 2016 to 2025, across card payments, credit transfers, e-money payments and cash withdrawals. This evidence base was used to identify the factors associated with fraud outcomes, establish a baseline trajectory to 2030 and assess how these may quantitatively impact fraud losses across these scenarios.

The evidence base draws on the following data types:

1. **Fraud outcomes:** including reported data on fraud value and rates by country and payment channel.
2. **Country payment structures:** including reported data on payment values, channel mix and cross-border payment activity.
3. **Macroeconomic conditions:** including reported data on gross domestic product (GDP) per capita, inflation and unemployment rates by country.
4. **Technology drivers:** Including data on the use of AI and social media by country.
5. **Regulation and prevention measures:** Including data on Strong Customer Authentication (SCA), Verification of Payee (VoP) or Confirmation of Payee (CoP), reimbursement frameworks, contactless limits and information sharing measures.
6. **Behavioural and societal indicators:** Including data on demographic change, and indicators of organised criminal activity by country.



How the analysis was developed:

1	**Built the evidence base**	Consolidated available fraud-loss data and reviewed published evidence on payment trends, fraud typologies, criminal capabilities, regulation and industry controls.
2	**Assessed emerging developments**	Identified and grouped the developments most likely to change the scale, nature or distribution of fraud across Europe and the UK through to 2030.
3	**Constructed future scenarios**	Combined the priority developments into four scenarios that test different interactions between fraud threats and ecosystem responses.
4	**Evaluated scenario impacts**	Undertook econometric analysis to assess how scenarios could evolve through to 2030, relative to the baseline, and to determine the direction and relative scale of change.
5	**Interpreted the findings**	Bringing together the emerging developments and outcomes of the quantitative analysis, a set of actions were developed for consumers, industry participants and policymakers.

Report structure

The report follows the analytical journey highlighted above with **Section 3** examining the changing fraud landscape and the forces reshaping it. **Section 4** translates these developments into a range of future scenarios through quantitative analysis. **Section 5** brings together the key findings and sets out priority actions to strengthen the resilience of the payment ecosystem.

The approach to the econometric modelling, data sources and limitations are set out in the Technical Appendix (Section 6). The scenarios are illustrative, assessed independently and are intended to show direction and relative scale of potential change rather than predict a single outcome.





3 Emerging and future fraud risks

The rapid advancement of AI and automation is driving the industrialisation of fraud, lowering barriers to entry and enabling criminal networks to operate with greater scale, efficiency, and sophistication.

However, the defensive ecosystem is also evolving in response. Significant investments are being made across industry to strengthen fraud prevention, enhance detection capabilities and counter the evolving and sophisticated criminal tactics. Alongside these efforts, industry and regulators are working together through a range of collaborative initiatives to prevent fraud, disrupt criminal activity and improve the recovery of stolen funds.

3.1 | Overview

Advances in AI, the growth of organised crime groups, and the emergence of fraud-as-a-service have enabled fraudsters to operate with greater speed, scale, and sophistication. Fraud is functioning more as a highly organised industry, with fraudsters adapting to improvements in payment security. Strong Customer Authentication (SCA), 3-D Secure and Verification of Payee (VoP) have reduced opportunities for traditional fraud, but criminal activity has now shifted towards customer manipulation, cross-border payment channels and digital assets.

In parallel, a growing proportion of fraud is originating from fraudsters abusing legitimate customer accounts and consumer protection mechanisms through refund abuse, chargeback abuse and other forms of first-party fraud. Generative AI has accelerated this trend by reducing the effort required to create convincing supporting evidence, fabricate documentation, impersonate communications and automate dispute, refund and chargeback requests at scale.



This section examines the key drivers of fraud and how they are likely to shape the fraud landscape through to 2030, with a particular focus on how fraud may materially evolve. We group these in three main themes:

AI and the industrialisation of fraud

- How AI is industrialising fraud, including the emerging technologies that enable fraudsters to conduct more sophisticated attacks more cheaply and at greater scale, while lowering barriers to entry for complex fraud schemes.

Displacement of fraud

- The displacement of fraud towards weaker points in the control environment, as fraudsters adapt and shift tactics in response to strengthened controls and emerging technology.

The evolving payments ecosystem

- The new payment ecosystem and the factors that make fraud more difficult to interrupt, trace, and recover once initiated.

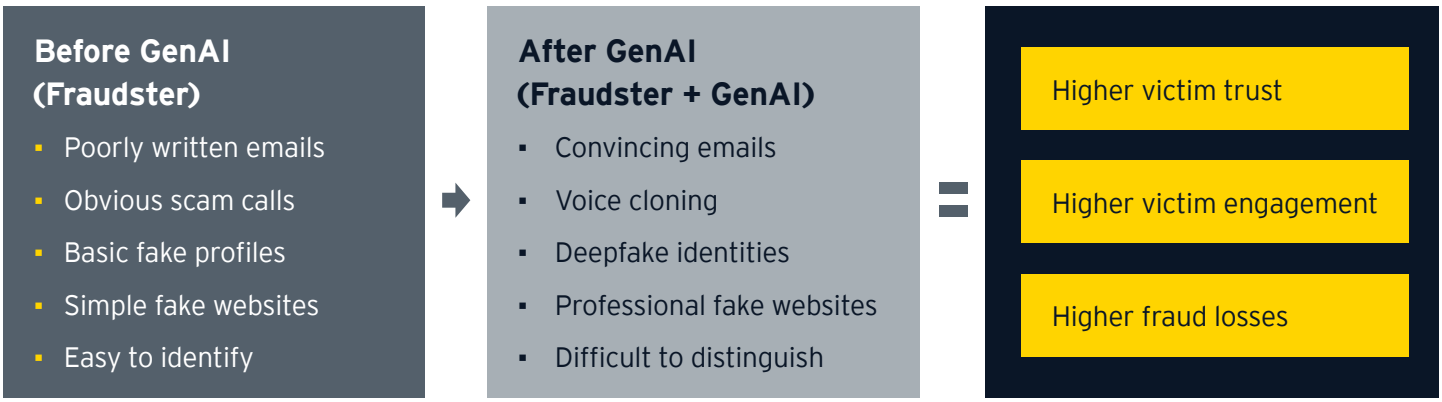
Many emerging fraud risks and typologies cut across the above themes and together form the foundation for the scenarios assessed in Section 4 and the recommendations outlined in Section 5.

3.2 | AI and the industrialisation of fraud

AI has long been a core component of modern fraud prevention. For decades, the payments industry has used predictive models and other advanced analytical techniques to assess risk, identify anomalies and detect potentially fraudulent activity. Today, across the payment journey, the industry uses AI-driven capabilities to analyse behavioural, device and transactional signals at scale, identify suspicious activity, detect evolving fraud patterns and support real-time decisions. At the same time, criminals are using advances in AI and automation to increase the scale and sophistication of attacks and lower barriers to entry. This is not a one-sided development: the same capabilities that allow criminals to automate attacks also enable payment providers to identify suspicious patterns earlier and intervene in real time. The future impact of AI on fraud will therefore depend on how effectively defensive AI is deployed across the ecosystem and combined with human expertise, high-quality data and coordinated action. This section examines how fraudsters are using AI to enhance existing fraud typologies, as well as the implications for future fraud prevention.

a. Generative AI (GenAI) enabled fraud

GenAI has fundamentally changed the way fraudsters conduct scams. Social engineering attacks have also become more convincing as fraudsters use AI to generate realistic emails, websites, scripts, online personas, audio and video content. Where scams could previously be identified through indicators such as poor grammar or inconsistent messaging, GenAI now enables fraudsters to create highly convincing emails, fake profiles, and online personas making fraudulent communications more difficult to distinguish.



b. Frontier AI and large language models (LLMs)

Building on these capabilities, frontier AI models and LLMs are acting as force multipliers for fraud. These technologies enable fraudsters to automate and scale a wide range of activities, including social engineering and malware development. Frontier AI is also expected to accelerate progress towards breaking certain forms of cryptographic encryption, potentially outpacing other emerging technologies such as quantum computing. In addition, LLMs have enabled fraudsters to blend techniques across scam typologies.

c. Enumeration attacks and account testing

Automation is also increasing the scale and efficiency of technical fraud attacks. While enumeration and account-testing attacks are not new, fraudsters are now leveraging bots and automated scripts to systematically test card numbers, expiry dates, and CVVs through low-value transactions, often distributing activity across multiple merchants to evade detection. Once validated, card details can be used for larger purchases, added to digital wallets, or sold on criminal marketplaces.

d. Fraud-as-a-Service

As fraud operations become more sophisticated, criminal ecosystems are now adopting service-based business models. The emergence of fraud-as-a-service and crime-as-a-service models provide fraudsters with special capabilities that can be purchased or rented through specialised criminal marketplaces, significantly reducing the skills, cost, and time required for sophisticated attacks. While these services have traditionally focused on the sale of stolen identity data and attack tooling, stronger identity controls may also drive an increasing demand for specialist services targeting fraudulent credential issuance, wallet recovery abuse, compromised devices, and the recruitment of genuine identity holders to open or operate accounts.

e. Organised criminal specialisation

Ultimately, these developments are driving the growth of highly specialised and industrialised criminal networks, with fraud now being perpetrated at a greater scale by highly organised, transnational networks operating at industrial scale leveraging specialist expertise, global infrastructure, money laundering networks, and criminal service providers.

Prominent examples of organised criminal groups include Southeast Asian scam-compound syndicates specialising in investment and romance scams; West African fraud networks such as Black Axe[7], involved in business email compromise and cyber-enabled financial crimes, North Korean state-sponsored actors, including the Lazarus Group[8] attributed to major banking and cryptocurrency thefts; and English-speaking cybercriminal groups[9] such as Scattered Spider, and LAPSUS$, which are known for social engineering and credential theft.



Overall, AI is transforming fraud from a largely manual activity into a highly scalable and industrialised enterprise, creating the need to strengthen resilience to remain effective in disrupting fraud. In response to this growing threat, the industry has made significant investments in defensive AI capabilities to disrupt fraud. For example, in 2024, Visa announced[10] its acquisition of Featurespace, to strengthen its fraud-detection and risk-scoring capabilities and enhance its use of AI to combat payment fraud. There is evidence that such intervention from the industry is delivering measurable benefits. The Bank of Ireland reported[11] a 30% reduction in attempted payment fraud and a 25% reduction in customer losses following the implementation of AI-led behavioural pattern recognition technology delivered in partnership with Featurespace. Continued investment in AI will be key to ensure that defensive capabilities keep pace with the changing threat landscape.

7 International crackdown on West-African financial crime rings
8 Lazarus Group: Attacks, Tactics, Malware & Defense
9 The COM: Anatomy of an English-Speaking Cybercriminal Ecosystem And The Origins of Scattered Lapsus$ Hunters | CloudSEK
10 https://www.visa.co.uk/about-visa/newsroom/press-releases.3345416.html
11 AI technology sees customer 'payment fraud' losses at Bank of Ireland drop 25% – Bank of Ireland Group Website

3.3 | Displacement of fraud

Fraud displacement is a consequence of effective fraud controls and successful fraud prevention efforts. Regulatory and industry measures such as SCA, VoP, CoP, and other fraud controls have made it difficult for fraudsters to operate through traditional attack vectors making them adapt by targeting different channels, products or customer touchpoints to exploit new vulnerabilities. In this section, we examine key displacement trends that are reshaping the fraud landscape.



a. Account Takeover (ATO)

Across Europe, fraudsters are shifting their tactics and targeting the account login and authentication stage rather than the payment transaction itself. By compromising accounts before transactions are initiated, they can bypass customer trust controls and appear to operate as legitimate users. The reduction in banking ATO losses has coincided with an increase in facility takeover activity across other sectors. The Cifas Fraud Landscape 2026 report[12] indicates that fraudsters are shifting their focus to compromising existing customer accounts across telecommunications, online retail, insurance and other consumer-facing sectors.

b. Credential compromise and identity theft

Building on this trend, credential compromise has evolved from a standalone cybercrime issue into a critical enabler of broader fraud activity. Phishing campaigns, database breaches, infostealer malware and credential marketplaces are supplying organised criminal networks with a continuous stream of compromised accounts and identities. Infostealer malware has emerged as a critical component of this ecosystem, enabling criminals to extract usernames, passwords, browser-stored credentials, and active session cookies directly from compromised devices.

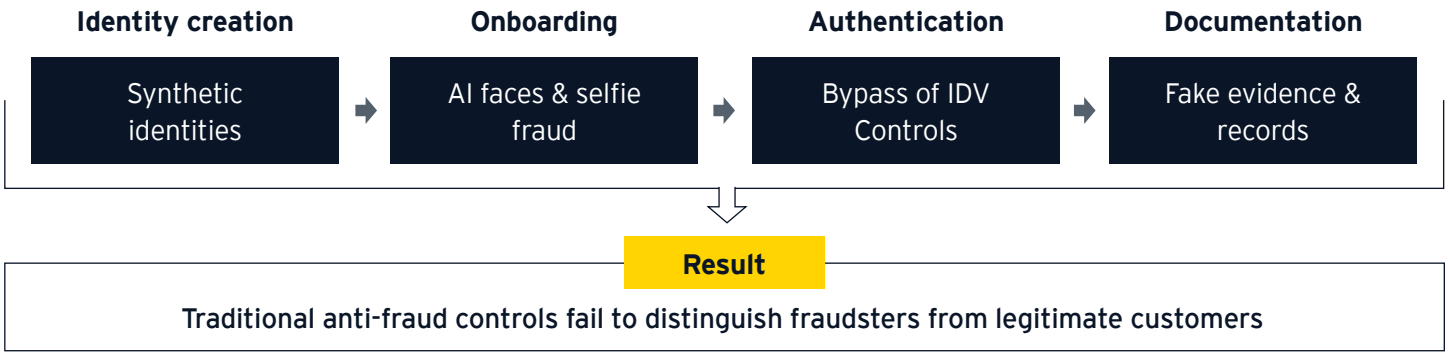
c. Identity and synthetic identity

Identity-enabled fraud encompasses several distinct threats: impersonation using a real person's stolen identity; synthetic identities assembled from fabricated or mixed attributes; and the misuse of genuine identities or legally registered businesses. These threats require different controls. Trusted digital identity credentials can make fabricated identities and document-based impersonation harder to use, provided issuance and verification processes are robust. They do not establish that a genuine customer or business is acting honestly. Merchant and business onboarding must therefore also assess legal existence, beneficial ownership, current authority to act and the nature of the underlying activity. Genuine identity holders may still act as money mules or facilitate fraudulent merchant operations.

12 Fraudscape 2026: Fraud cases hit record highs as criminals adapt and scale | Cifas

d. Deepfakes identity bypass

Closely linked to the rise of synthetic identities is the growth of deepfake-enabled identity fraud. While synthetic identities focus on creating false personas, deepfakes enable fraudsters to make those personas appear genuine during onboarding and authentication processes. Fraudsters are using AI-generated faces, manipulated selfies and synthetic video to attack remote identity proofing, particularly where controls depend on visual evidence or inadequately protected capture channels. As wallet-based identity becomes more widely used, attacks will likely concentrate on initial credential issuance, recovery, alternative onboarding routes and any additional biometric checks.





e. Emerging forms of Authorised Push Payment (APP) fraud

In response to measures such as CoP, enhanced fraud controls and reimbursement requirements, fraudsters are adapting their methods and developing new APP fraud typologies. Some of the emerging examples of scams include:

- **Me-to-me crypto scams** – A me-to-me crypto scam involves victims being manipulated into transferring funds to an account or crypto wallet in their own name before giving the fraudster access to or control of the funds. These scams commonly arise through fraudulent crypto-investment schemes.
- **Gold and precious metal scams** – Fraudsters may persuade victims to convert funds into gold, silver or jewellery and hand them over to a courier under the false pretence of safeguarding assets or assisting an investigation.
- **Whisky and wine cask investment scams** – Whisky and wine cask investment scams involve the sale of illiquid alternative assets using misleading claims about ownership, valuation and returns. Common scam tactics include unverifiable asset ownership or multiple sales of the same cask.

The above emerging scam typologies illustrate how displacement of scams will likely remain a defining feature of the fraud landscape, requiring the industry to continuously adapt its controls and customer protection measures.



f. Growth of first-party fraud

Fraud displacement has also been seen through the growth of first-party fraud, where genuine customers intentionally misrepresent circumstances or misuse consumer protection mechanisms for unwarranted financial gain. As the payment ecosystem strengthens controls against more traditional forms of unauthorised fraud, merchants are reporting an increase in fraud due to customer misconduct. Generative AI has further accelerated this trend by reducing the effort required to create convincing supporting evidence, fabricate documentation and automate dispute, refund and chargeback requests at scale. Common examples of increasing first-party fraud include:

- **Friendly fraud (first-party misuse)** – This involves legitimate customers deliberately misrepresenting a transaction or misusing the dispute or chargeback process to obtain an unwarranted refund or avoid payment after receiving goods or services. This is distinct from genuine consumer disputes, including situations involving legitimate transaction confusion or dissatisfaction.
- **Refund and policy abuse** – This involves the intentional misuse of merchants' refund, return or compensation policies for unwarranted financial gain. Common examples include falsely claiming that goods were not received, returning used or damaged merchandise contrary to applicable policies, manipulating delivery information, or returning incorrect or counterfeit items.

The trend demonstrates exploitation of consumer protection frameworks, creating new challenges for merchants, payment providers and policymakers.

Near Field Communication (NFC) relay attacks

Fraudsters are also adapting to the growing adoption of contactless and mobile payment technologies. A notable example is the emergence of NFC relay attacks, which combine social engineering with the misuse of legitimate payment infrastructure to facilitate fraud. These attacks range from relaying fraudulently provisioned tokens, to using social engineering to convince consumers to install malicious mobile apps and then having the consumer tap their card against the device with the malicious app installed, to hardware shims placed in unattended terminals. The availability of open-source tools, NFC-enabled smartphones, and Malware-as-a-Service offerings has lowered the barriers to entry for fraud, highlighting the growing shift towards social engineering and the abuse of contactless and mobile-payment ecosystems.

Overall, fraud is becoming more adaptive and shifting towards the points of least resistance. Successful fraud prevention will therefore depend on anticipating how fraudsters may redirect their activity towards less-protected channels or vulnerabilities as controls are strengthened, strengthening controls across the end-to-end customer journey, and continuously adapting to emerging attack vectors and technologies.

Combatting and preventing fraud will require layered, adaptive defences across the entire customer journey, combining robust identity assurance, supported by initiatives such as the European Digital Identity Wallet under the revised eIDAS framework, with advanced behavioural analytics, and AI-enabled, context-aware decisioning. At the same time, scam disruption capabilities are enhancing the industry's ability to identify and dismantle fraudulent websites, scam merchants, and other criminal infrastructure at scale, while consumer education and awareness initiatives continue to play a critical role in reducing the effectiveness of social engineering and impersonation attacks. Ultimately, no single control will eliminate fraud. Sustainable progress will depend on continued innovation, investment and cross-sector collaboration, supported by timely intelligence sharing between financial institutions, technology providers, merchants, telecommunications operators and public authorities.

3.4 | The evolving payments ecosystem

The payments ecosystem has evolved, becoming faster and more interconnected, making customer experience more seamless and quick. Transactions can now be completed quickly across large jurisdictions. However, these developments have also made fraud harder to interrupt and recover once initiated as fraudsters are leveraging money mule networks[13] to rapidly move illicit funds through complex transaction chains, making fraud proceeds harder to detect, trace and recover. In this section, we examine factors which have reduced the window for detection, intervention and recovery, requiring greater effort to disrupt the fraud journey.

a. Faster payments

The widespread adoption of real-time payment rails[14] has accelerated the movement of fraud proceeds. The speed and immediacy of these payments can reduce the time available to identify and stop fraudulent transactions, enabling fraudsters to move funds rapidly through mule accounts before intervention is possible. The UK experience illustrates the scale of this challenge. APP scams, which predominantly occur over the Faster Payments network, resulted in £341 million in losses in 2023, according to the Payment Systems Regulator[15] (PSR) data[16]. Following implementation of the APP reforms, independent research[17] showed that APP fraud losses through faster payments declined by approximately 21%. As instant payments continue to grow, fraud prevention and detection capabilities will need to evolve in parallel.

b. Stablecoin fraud

As payment ecosystems evolve, fraudsters are now exploiting stablecoins[18] and other digital assets to facilitate and move illicit funds. Their speed, global accessibility, and ability to transfer value across borders make them attractive tools for both legitimate users and fraudsters. Visa Business and Economic Insights[19] estimates that retail-sized stablecoin transaction volumes grew from approximately €0.45bn in 2019 to €62.7bn in 2025, expanding the channels available for fraud. Fraudsters are using stablecoins in investment scams, fake invoice fraud and wallet compromises, with funds rapidly moved across wallets, blockchains, exchanges and mule networks, making tracing and recovery more challenging.

In parallel, the growth of fraud risks within the digital-asset ecosystem is being accompanied by continued industry investment in monitoring, analytics and compliance capabilities designed to identify and disrupt illicit activity, providing greater visibility of transaction flows and helping to identify suspicious patterns and the movement of illicit funds.

c. Digital wallets

Closely linked to this trend is the growing adoption of digital wallets, which are being embedded across the payments ecosystem. While improving convenience and supporting digital commerce, they also enable fraudulently obtained funds to be moved rapidly between accounts and providers, particularly when combined with instant payments and account-takeover attacks. The speed and interconnected nature of these payment flows can reduce opportunities to detect and disrupt fraud before funds are transferred onwards.

Payment wallets and crypto-asset wallets should be distinguished from European Digital Identity Wallets, whose core role is to hold and present identity data and attestations. Their fraud implications differ: the former may facilitate payment initiation or value transfer, while the latter can strengthen identity assurance and introduce distinct issuance, presentation and recovery risks.

13 **Money mule networks** are individuals or organised groups of individuals who transfer proceeds of fraud through a series of legitimate bank accounts, payment platforms, or cash withdrawals, to conceal the source of illicit proceeds and facilitate the laundering of fraud-related funds.

14 Payment rails refer to the infrastructure that facilitates the movement of funds. Examples include cards, faster payments, SWIFT, real-time payments, digital wallets, stablecoins, and cryptocurrency networks.

15 The UK Government plans to consolidate the PSR's functions within the FCA. Until the necessary legislative changes take effect, the PSR retains its existing responsibilities.

16 APP scams performance report (July 2024)

17 https://www.frontier-economics.com/uk/en/news-and-insights/news/news-article-i22383-app-payment-scam-policies-reducing-fraud/

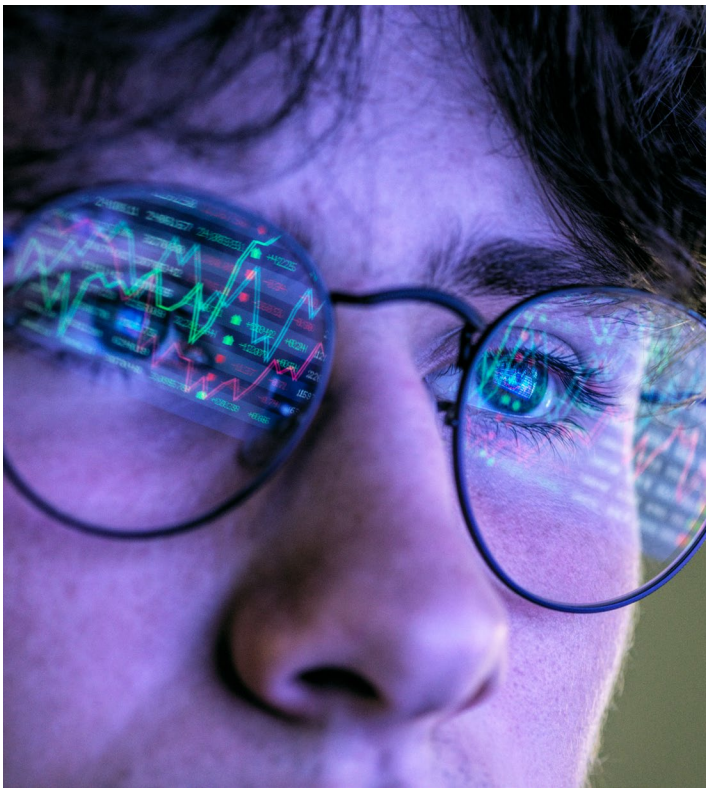
18 Stablecoins are digital currencies designed to maintain a stable value, usually by being pegged to a traditional currency such as the US dollar or euro, or to another asset such as gold.

19 Stablecoins: Reimagining money movement for a digital economy

d. Crypto assets and digital assets

Beyond digital wallets, crypto assets and other digital assets have introduced alternative mechanisms for transferring value outside, and alongside, traditional financial systems. Fraudsters are now exploiting these ecosystems to convert, transfer and layer the proceeds of fraud through multiple wallets, exchanges and blockchain networks, making the tracing of illicit funds more complex.

Overall, the modern payments ecosystem is enabling value to move faster than ever, benefiting consumers and businesses while creating new opportunities for fraudsters to rapidly move and conceal illicit funds. In response to this evolving risk, the industry continues to strengthen security across the payment journey through technologies such as network tokenisation, device binding, behavioural analytics and adaptive authentication, helping to identify suspicious activity and strengthen the protection of legitimate transactions. These advances demonstrate how payment innovation and security can evolve together, enabling faster and more seamless payments while strengthening resilience against fraud. Therefore, effective fraud prevention will depend on maintaining this progress through continued investment in preventative controls and the ability to detect, trace and disrupt fraudulent activity across the end-to-end payment journey.



3.5 | Other emerging fraud risks

While many of the trends discussed so far reflect the evolution and displacement of established fraud typologies, a new generation of risks is beginning to emerge from advances in artificial intelligence (AI), automation, and next-generation computing technologies. These risks are still developing but have the potential to fundamentally reshape the future of fraud. In this section, we examine several emerging threats that could have a significant impact on financial institutions and payment service providers over the coming years.

a. Prompt injection

To begin with, the growing adoption of AI within financial services is creating entirely new attack surfaces for fraudsters. One such threat is prompt injection, where malicious instructions are embedded within messages, documents, webpages, or payment-related data to manipulate the behaviour of AI systems. Financial institutions are an attractive target for fraudsters, especially where AI agents have read/write access to core banking systems, fraud management queues, or payment approval workflows. The attacks cause AI tools to generate misleading outputs, disclose sensitive information, or influence payment-related decisions.

In parallel, the industry is developing and implementing safeguards to reduce exposure to prompt-injection attacks, including strengthening of input handling, controls around AI access to systems and data, and monitoring of AI interactions.

b. Agentic commerce

The emergence of agentic commerce is shifting AI from helping consumers discover and evaluate options to one that can act on their behalf within parameters they define. AI agents may search, compare products, select merchants, choose payment methods and complete purchases based on a user's stated preferences and permissions. As consumers delegate more of these activities, establishing trust, transparency and control becomes increasingly important. New risks may emerge if fraudsters attempt to manipulate the data, instructions or credentials used by AI agents, redirecting transactions towards fraudulent merchants or enabling unauthorised activity. As a result, robust identity verification, authentication, consent management and transaction monitoring will play a critical role in helping ensure agent-led transactions remain secure and trustworthy.

Security and trust by design are therefore fundamental to the development of agentic payment models. Visa's approach, for example, combines tokenised credentials, authenticated payment instructions through Visa Payment Passkeys, agent onboarding and agent identity verification through Visa's Trusted Agent Protocol (TAP), alongside controls that help ensure transactions are authorised and executed within consumer-defined parameters. These safeguards are designed to support transparency, security and consumer control while helping address risks associated with unauthorised transactions, malicious agents and payment credential compromise.

c. Quantum computing

Looking further ahead, quantum computing represents a longer-term but potentially transformative fraud risk. While there is currently limited evidence of its use in facilitating fraud across Europe, the technology has the potential to alter some of the security foundations that underpin modern payment systems. Today's payments ecosystem relies heavily on cryptographic controls to secure authentication, digital signatures, payment messaging and data integrity. As sufficiently powerful quantum computers become commercially viable, some of these protections could become vulnerable, creating new opportunities for fraud.

The emergence of quantum computing has also accelerated industry efforts to strengthen long-term cryptographic resilience. For example, Visa is actively researching quantum-safe payments[20] and has highlighted the need for early preparation for postquantum cryptography, noting that migration could require years of coordinated effort across the payments ecosystem. Visa has established internal milestones to support this transition.



20 preparing-stablecoins-for-quantum-era.pdf

3.6 | The evolving defence ecosystem

While fraudsters continue to innovate and adapt, the defensive ecosystem has also evolved significantly. Across Europe, regulators, payment service providers, and industry bodies have introduced a range of initiatives designed to prevent fraud and disrupt criminal activity. This section examines such initiatives.

a. Regulatory driven defensive ecosystem.

To begin with, regulators across Europe have introduced the following measures aimed at addressing emerging fraud risks and strengthening trust in digital payments:

Regulation	Purpose of the regulation	Fraud risks mitigated
PSD2, PSD3/ Payment Services Regulation (EU)	Introduced and is expected to further develop key measures including SCA, open banking access requirements, enhanced consumer protections, security requirements and fraud information sharing[21] and cross-sector collaboration.	Unauthorised payment fraud, credential theft and account compromise.
Mandatory APP Fraud Reimbursement (UK)	Shifts liability across the payment ecosystem, requiring payment firms to reimburse eligible victims of APP through Faster Payments and CHAPS.	APP and mule account activity.
VoP (EU)	Requiring PSPs to verify whether the beneficiary's name matches the account identifier before a transfer is completed.	Payment redirection fraud, invoice scams and impersonation attacks.
Single Euro Payments Area (SEPA) (EU)	Harmonises euro payments across Europe through common standards and processes.	SEPA enables better fraud intelligence sharing e.g. Fraud Information Distribution Arrangement (FRIDA).
Revised eIDAS framework and European Digital Identity Wallets (EU)	Establishes a framework for trusted identity wallets, person identification data and electronic attestations, supported by security, certification and relying-party requirements.	Document-based impersonation and unauthorised reuse of identity credentials when correctly implemented.
Banque de France OSMP recommandations	Strengthen security on e-commerce with stricter approval strategy for non-3DS, Merchant-Initiated Transaction (MIT), Mail Order/Telephone Order (MOTO).	Unauthorised payment fraud, credential theft and account compromise.

b. Industry/Scheme driven defensive ecosystem

Complementing these regulatory developments has been the industry-driven defensive ecosystem. As traditional credentials such as passwords, PINs and security questions became more vulnerable to theft and social engineering, the industry responded with biometrics, tokenisation, passkeys, device binding and risk-based authentication enabling low-friction authentication while maintaining a seamless customer experience.

21 Article 83a of the current PSR text provides for fraud information-sharing arrangements between PSPs where there are objectively justified reasons to suspect fraudulent behaviour, subject to security, confidentiality and data-protection safeguards. Article 83b complements this by providing for a European Commission-chaired public-private platform to analyse payment fraud trends, share information on mitigation measures, strengthen cross-border and cross-sector cooperation, and advise on measures to combat payment fraud.

c. Cross-sector intelligence sharing

Cross-sector data/intelligence sharing has strengthened fraud prevention and detection by enabling a more connected, intelligence-led approach to identifying and disrupting fraud. The industry, regulators and law enforcement agencies share information on emerging threats, suspicious activity and criminal networks, improving the identification of fraud patterns, mule networks and organised criminal activity. Some of the key European data sharing initiatives include:

- Joint Money Laundering Intelligence Taskforce (JMLIT) – The UK's NCA-led public-private partnership that brings together financial institutions and law enforcement to share intelligence and coordinate action against money laundering and fraud.
- Cifas National Fraud Database – A cross-sector fraud intelligence database which allows member organisations to share confirmed fraud risks and intelligence to disrupt fraud.
- Transaction Monitoring Netherlands (TMNL) – A collaborative initiative established by major Dutch banks to jointly monitor payment transactions and identify potential financial crime risks.
- FIU.net – A decentralised information-sharing network that enables Financial Intelligence Units across Europe to exchange financial crime intelligence and support the identification of cross-border money laundering and fraud.
- FRIDA – A European Payments Council initiative under development to provide a central platform for the secure exchange of fraud-related information between PSPs across SEPA.
- MISP – A European open-source platform that enables payment service providers across SEPA to share fraud, cyber threat and malware intelligence, helping institutions identify emerging threats and strengthen fraud prevention efforts.

The themes explored throughout this chapter highlight a fraud landscape that is shifting to become more dynamic, interconnected, and technology driven. The next section builds on these insights by looking beyond current trends and exploring how fraud may evolve over the coming years.

Case study: Singapore's data sharing success [22]

In 2024 the Monetary Authority of Singapore (MAS) introduced a centralised digital platform, the Collaborative Sharing of Money Laundering/Terrorism Financing Information and Cases (COSMIC).

COSMIC enables financial institutions to securely share information on customers flagged as potential financial crime concerns. Customers are flagged and their information shared based on indicators of serious financial crime.

COSMIC is currently in the initial phase of delivery across six major commercial banks and focuses on three key financial crime risks in commercial banking including misuse of legal persons, misuse of trade finance for illicit purposes and proliferation financing.

In an address to Parliament in August 2026, Alvin Tan the Minister of State for Foreign Affairs and National Development Singapore and board member of the MAS, shared how COSMIC has contributed to disrupting financial crime. Since its implementation COSMIC participant banks have had an increase in Suspicious Transaction Reports (STRs) related to more than 1.6 billion (Singapore dollars) worth of fund transfers. Of the accounts Flagged as suspicious more than 1,000 customer accounts have been closed due to potentially fraudulent activity.

COSMIC was mutually evaluated by the Financial Action Task Force (FATF) and the Asia/Pacific Group on Money Laundering (APG) in 2026. It was recommended that the MAS expand the use of COSMIC to more participants and to cover financial crime risks beyond those currently in focus.

22 COSMIC; Alvin Tan LinkedIn; FATF/APG Mutual Evaluation Report of Singapore – 2026



4 Trajectory of fraud losses to 2030

Fraud losses across Europe could follow different trajectories to 2030 depending on how emerging risks and responses evolve. This section looks at the key risks and opportunities discussed in Section 3 and translates them into scenarios that can be quantitatively assessed. We evaluate how a baseline (where the fraud rate remains relatively similar to today) and four future fraud scenarios could affect fraud losses across Europe to 2030.

The four scenarios are presented as two prevention-led (upside scenarios) and two adverse pathways (downside scenarios):

- Industry no longer prioritises additional prevention, meaning the risks have significant impact on fraud losses:
  1. A technology arms race where fraudsters successfully outpace defences by leveraging AI and technology increasing the number of successful fraud attempts.
  2. Growth in organised crime and fraud-as-a-service furthering the industrialised and globalised nature of fraud increases fraud losses.
- Additional prevention action occurs and fraud losses can be mitigated:
  3. A technology arms race where institutions leverage AI and technology and work collaboratively to reduce fraud losses over time.
  4. Widespread data sharing between stakeholders across the payment ecosystem effectively reduces fraud losses.

Importantly, the analysis shows that the future trajectory of fraud is not predetermined. A baseline view provides the comparison point for each scenario and, if current trends continue without major structural disruption, fraud losses across Europe are estimated to reach around €8 billion by 2030.

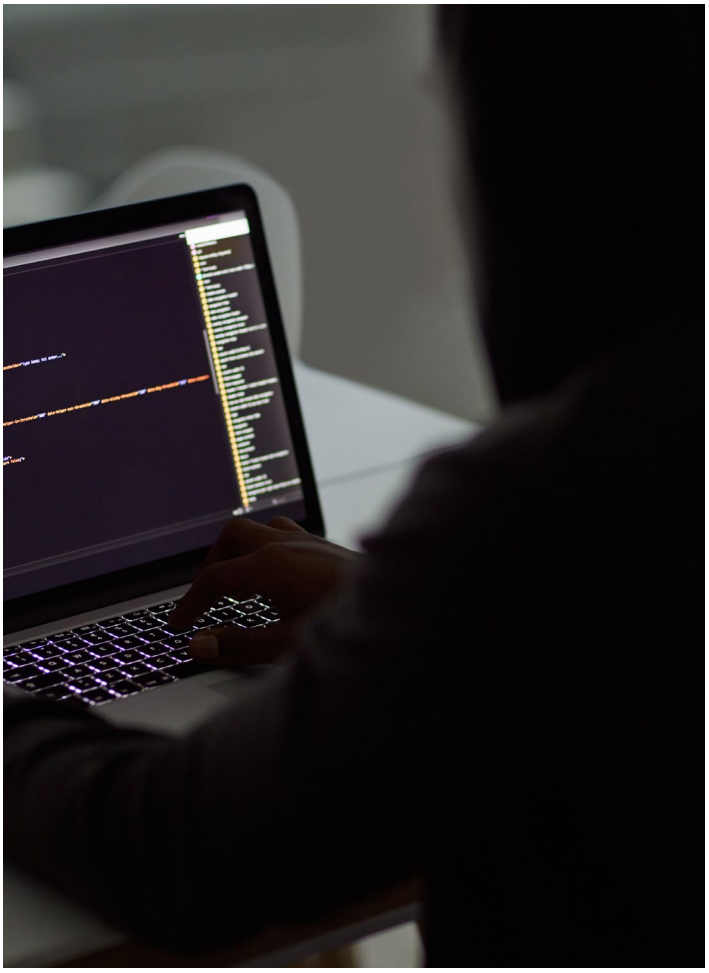
Outcomes could be significantly worse if criminal capabilities develop faster than defences. In the most adverse downside scenario, where technology-enabled criminal capabilities outpace prevention and detection, fraud losses could reach around €12 billion by 2030. A second downside scenario, characterised by increasingly industrialised organised crime and fraud-as-a-service, could see losses reach around €10 billion.

Conversely, continued investment in prevention and effective collaboration could materially improve outcomes. Where technology-enabled defences continue to evolve, fraud losses could be held to around €6 billion by 2030. Under the strongest prevention scenario, widespread data and intelligence sharing across the ecosystem could see annual fraud losses fall to around €5 billion by 2030, 30% below the baseline in 2030, and result in around €6 billion in cumulative fraud losses being avoided over the next four years (when measured against the baseline).

Taken together, the scenarios demonstrate the value of sustained investment in technology, intelligence sharing and coordinated action across the ecosystem in preventing future fraud losses. The scenarios are illustrative, assessed independently and are not predictions of future fraud losses.

4.1 | Overview

This section quantitatively evaluates how themes shaping the future of fraud will impact the trajectory of fraud losses in Europe to 2030. To do this, the interconnected themes discussed in Section 3 are brought together into four scenarios. The expected fraud trajectory under each scenario is assessed and compared against a "baseline" forecast of fraud that represents a continuation of today's trends.



4.2 | Evaluating the risks and opportunities relevant to the future of fraud

Section 3 explored the fraud landscape identifying many current, emerging and future fraud risks that the payment ecosystem faces as it evolves and the scale and sophistication of fraud increases. It also looked at some of the ways in which the industry is adapting and progressing the defensive ecosystem. From this assessment we have shortlisted three themes to be evaluated. These combine fraud risks and defensive opportunities that are likely to shape the future of fraud to 2030:

AI fraud and defence

- Rapid technology growth advancing AI related fraud capabilities is presenting as both a key risk and opportunity for the fraud landscape.

Organised crime and fraud as a service

- Evolving payment methods and increasing cross-border payments overlayed with technology and criminal capability expansion is allowing fraud to become more instant and globalised.

Data enabled defences

- The defence ecosystem is rapidly transforming enabled by a range of initiatives. However, to keep ahead of fraud further advancement is required. Data sharing across all participants is a key opportunity for defence and detection of fraud.

Four scenarios have been developed to explore how fraud losses across Europe could evolve to 2030. These illustrate potential pathways where either no additional prevention action occurs and the risks have a significant impact on fraud losses (downside scenarios 1 and 2) or additional prevention action occurs and fraud losses can be mitigated (upside scenarios 3 and 4).

While in reality these scenarios may occur concurrently and the work already underway across the industry to invest in and innovate defensive capabilities will mitigate some of the impact from these risks, for the purposes of this assessment each scenario provides an independent illustrative view to show the range of impact on fraud losses.

Scenarios under assessment

Downside scenarios

1 Technology arms race where fraudsters outpace defences

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

Influences on fraud trajectory:

- Fraud becomes increasingly automated, scalable and personalised through AI tools.
- Deepfakes and synthetic identities make it harder to distinguish genuine customers from fraudsters.
- Fraudsters increasingly use AI to create convincing scams, impersonations and fraudulent accounts.

2 Organised crime and fraud-as-a-service grows

Fraud is a highly specialised globally connected criminal ecosystem where criminal groups buy technology, victim information, identity creation and laundering capabilities as services.

Influences on fraud trajectory:

- Criminal groups operate increasingly professionalised fraud ecosystems.
- Fraud tools, stolen credentials, synthetic identities and laundering services become widely available for purchase.
- Specialist actors focus on victim targeting, account compromise, identity creation and money movement.
- AI reduces barriers to entry and allows criminal networks to scale rapidly.
- Organised networks become increasingly resilient to enforcement and fraud controls.

Upside scenarios

3 Technology arms race offset by defences

Institutions react and adapt to advancements in technology to offset the ability for fraudsters to exploit technology.

Influences on fraud trajectory:

- AI-enabled detection, stronger behavioural analytics and more complex authentication controls continue to advance and be deployed at scale across the industry allowing institutions to detect fraudulent activity earlier and act in real time.
- Collective action across the industry and Europe to implement advanced defensive capabilities outpace fraudsters.

4 Public and private data sharing is widespread

Banks, PSPs, governments and technology firms share intelligence in near real time, transforming fraud prevention from an institutional challenge into an ecosystem capability

Influences on fraud trajectory:

- Banks, PSPs, governments and technology firms collaborate to identify fraud.
- Shared intelligence improves detection of mule networks, organised crime groups and repeat offenders.
- Fraud signals are increasingly exchanged in real time across institutions.
- Earlier intervention reduces successful fraud and improves recovery outcomes.

Approach to developing and assessing the scenarios

To develop and assess the impact of scenarios on future fraud losses the following approach was undertaken:

Development of future fraud scenarios

The emerging and future fraud risks and potential responses to them provided the context for the development of scenarios that may shape the future of fraud losses to 2030.

Assessment of how fraud evolves under each scenario to 2030

These scenarios were modelled to quantitively evaluate different trajectories of fraud losses against the baseline forecast of fraud representing no-change to the current payment and fraud ecosystem.

Comparison of the future fraud trajectories to the baseline

The baseline of fraud growth to 2030 was compared to the pathways of fraud losses representing the scenarios evaluated. Implications were drawn from the outcomes.

There are many possible future scenarios of how fraud will evolve depending on how the industry, policy and consumers respond to changes in the payment landscape and how fraudsters adapt their capabilities. The scenarios quantified are illustrative of the current and emerging fraud landscape and do not seek to include all potential associated threats and defensive or regulatory responses. Their purpose is to illustrate how sensitive fraud losses are to different threats or how defences can mitigate these losses to inform policymaking, industry plans and consumer behaviours.

4.3 | A baseline of fraud in Europe

To evaluate the impact on the trajectory of fraud losses under differing scenarios, it is important to understand how fraud losses have historically moved across Europe.[23] We have assessed historical reported fraud levels and how they have evolved over time to build a forecast baseline of fraud to 2030.

Recently, total fraud losses have seen a structural shift as fraudsters exploit vulnerabilities in new payment methods and adapt to the introduction of regulations, such as SCA, and defences across the industry. Fraud through credit transfers and authorised fraud is increasing as a proportion of total fraud while fraud through card payments and unauthorised fraud is reducing as a proportion of total fraud (while the total volume and value continue to increase). This illustrates the gradual but continued growth in account-to-account, real time payments and mobile wallets and the introduction of stronger authentication and fraud controls making fraudsters adapt their tactics.

At a country specific level, reported fraud is concentrated in a small number of European markets. The majority of reported fraud losses come from the UK, France, Germany, Spain, Italy and Belgium.

In the baseline, fraud losses are expected to follow the recent trends with credit transfer fraud, followed by card fraud making up most of the fraud losses. E-money fraud will continue to grow while cash fraud may start to see reductions as people continue to evolve their payment behaviours. By 2030, baseline fraud losses are expected to grow to around €8 billion.

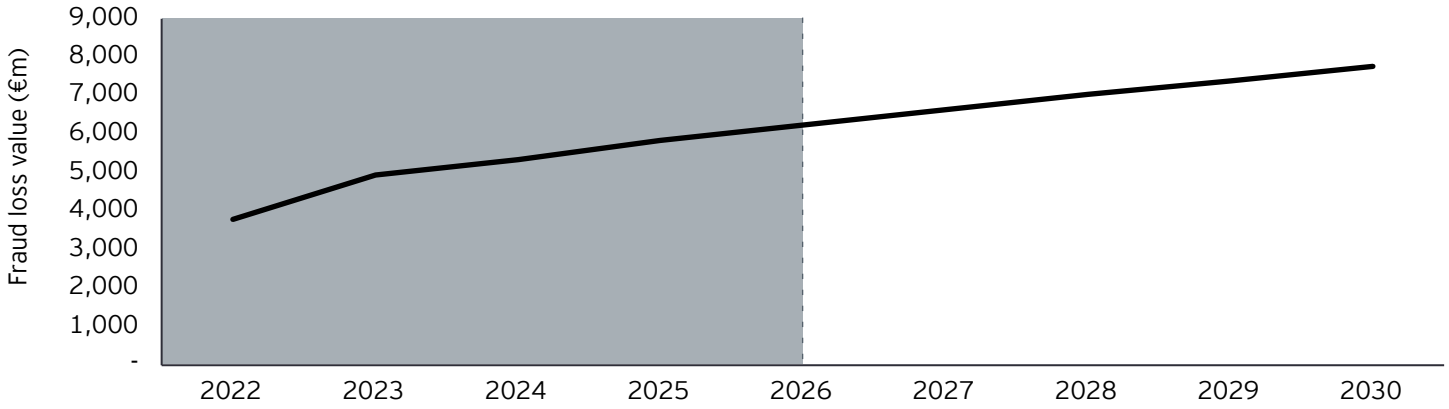
At a country level, it is expected that fraud losses remain concentrated in the major markets. While this has been assumed, fraud losses depend on the scale of national growth in payments and the composition of payments (e.g. growth in faster payments) and any associated regulatory changes that may affect both payments and fraud.

23 Payment channel definitions are based on ECB's data breakdown. They include credit transfers, direct debits, card payments, cash and e-money. Each is defined in the appendix.

Fraud loss data is based primarily on fraud identified and reported by financial institutions and payment service providers and may therefore not capture the entirety of fraud losses. Factors including the sophistication of payment systems (including the level of digitalised banking), fraud exposure, reporting practices and reimbursement frameworks can all contribute to variation in the level of reported fraud across Europe. As a result, reported fraud losses should be treated as a minimum estimate of the actual scale of payment fraud in Europe.[24]

The baseline is shown below.[25]

Europe level fraud loss values (€m) from 2022–2030



4.4 | Assessment of the fraud scenarios

Below each of the downside and upside scenarios are evaluated.[26] The results should not be interpreted as forecasts or expected outcomes, but as illustrations of the potential impact drivers of fraud may have on future fraud losses. Additionally, while presented individually, the scenarios are not mutually exclusive and may occur in tandem so additional fraud losses or outcomes of prevention may occur concurrently.

Downside scenarios

1. A technology arms race where fraudsters outpace defences

This scenario illustrates an adverse pathway where the accelerating adoption of AI to create deepfakes, synthetic identities and automated fraud capabilities coupled with the rise in remotely initiated transactions, may allow the rapid growth and increased sophistication of fraud by criminals. Fraudsters can increase the realism, scale and effectiveness of scam attempts having a significant impact on fraud losses across Europe. Under this scenario, fraudsters exploit technological advances faster than institutions can adapt and therefore fraud could grow considerably.

Outcomes to 2030

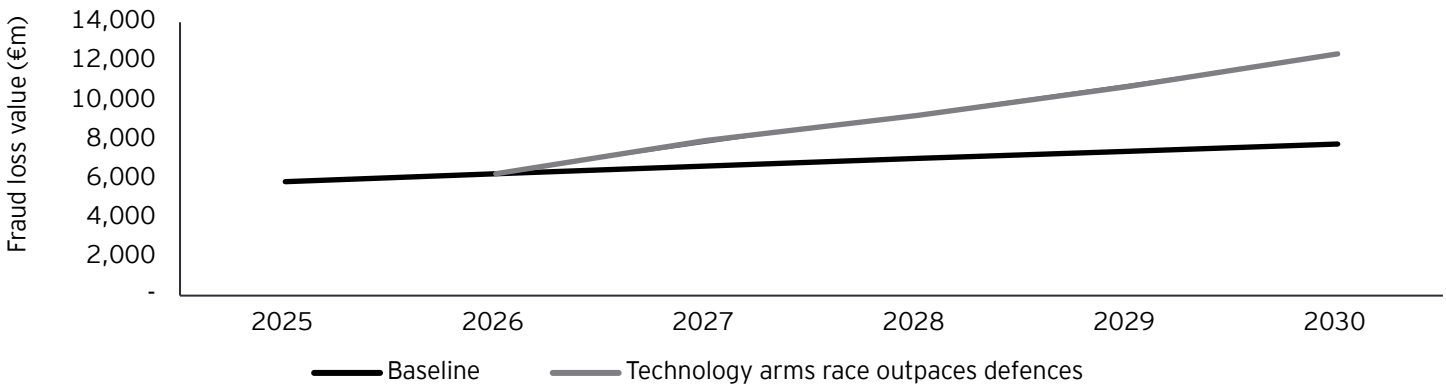
Under this scenario where fraudsters exploit advancements and the industry does not keep up, fraud losses could increase more rapidly and could result in €12 billion in fraud losses in 2030, almost doubling the level of fraud today. Beyond 2030, fraud levels could continue to rise rapidly unless institutions continue to improve their defences by using better authentication, fraud detection systems and sharing fraud intelligence across the industry.

24 UK Finance and ECB and EBA statistics have been used for this baseline analysis as they are the most comprehensive data sets for fraud loss values.

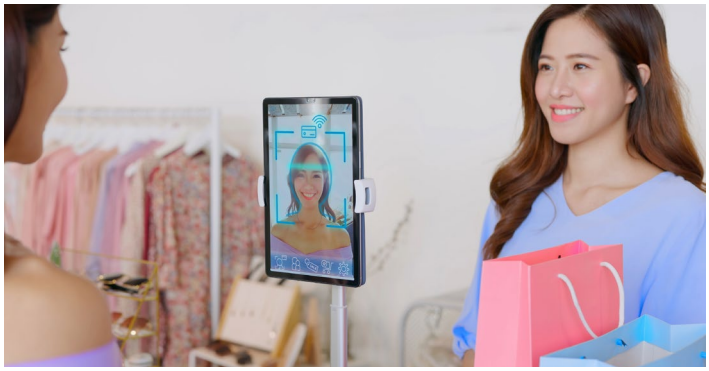
25 Methodology note: The baseline and forecasts do not include direct debit fraud losses, see the technical appendix for further detail on the exclusion and any limitations of the analysis.

26 Figures are rounded. Totals, differences and percentage changes are calculated on unrounded values and may not reconcile exactly with the rounded figures shown.

Europe level fraud loss values (€m) from 2025-2030



Fraudsters can use AI to automate victim targeting, generate more convincing attacks and reduce the cost of conducting fraud at scale. As a result, first party fraud, authorised payment fraud, identity-led fraud and account takeover could represent an increasing proportion of total fraud losses by 2030 under this scenario. Although card fraud remains a significant contributor to overall fraud volumes, growth in losses is likely to mostly be within credit transfers where payments are largely electronic and remotely initiated and social engineering and account compromise play a more prominent role.



2. Organised crime and fraud-as-a-service grow

This scenario assumes that organised criminal networks become more sophisticated and globalised than they are today, making greater use of fraud-as-a-service models, enabling fraud capabilities to be purchased and delivered at scale. These highly specialised and industrialised criminal networks would draw on specialist services and infrastructure including access to victim acquisition services, synthetic identity creation, malware, phishing infrastructure, credential theft and money laundering networks to a greater degree.

Outcomes to 2030

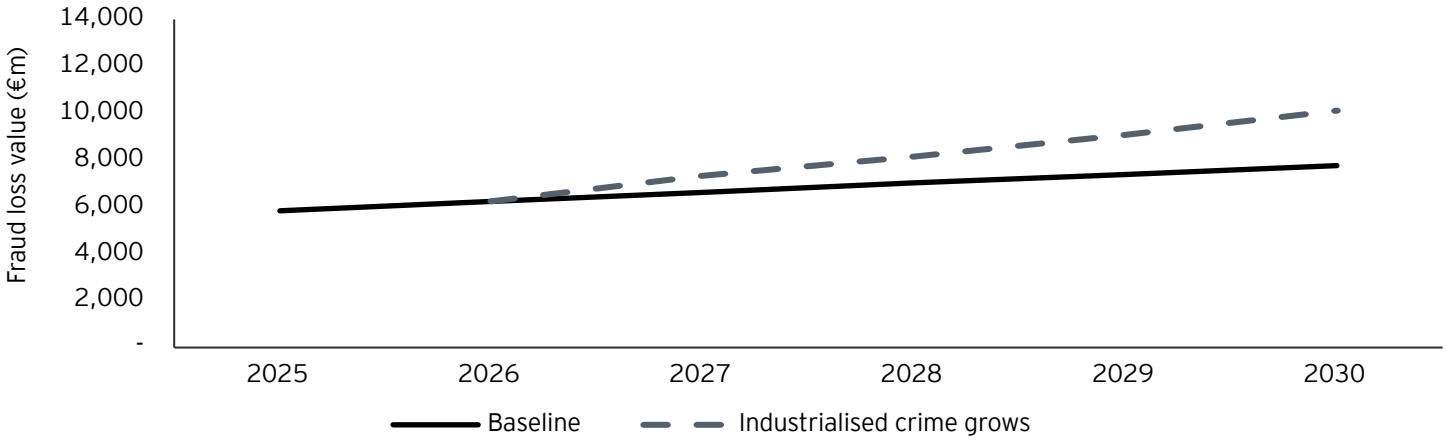
Under this scenario, fraud losses could rise above the baseline forecast as fraud capabilities become more widely available and easier to deploy by criminals. In 2030, fraud could rise to €10 billion, a 30% increase compared with the baseline forecast.

Criminal groups benefit from economies of scale, allowing larger volumes of attacks to be conducted with lower operational effort. Increased attack volumes will contribute to the growth in fraud losses within scam-based, mule-enabled and authorised fraud typologies where they focus on victim targeting, social engineering, identity creation, account compromise and movement of criminal proceeds.

The impact is unlikely to be distributed evenly across Europe. Markets characterised by high payment volumes, high digital adoption and internationally connected payment ecosystems may become increasingly attractive targets for organised criminal activity. Countries with fragmented enforcement capabilities or weaker cross-border coordination could experience greater challenges in disrupting fraud networks and recovering criminal proceeds.

If these trends continued beyond 2030, fraud could become increasingly concentrated among highly organised criminal enterprises capable of operating across multiple jurisdictions and payment systems simultaneously.

Europe level fraud loss values (€m) from 2025-2030



Upside scenarios

3. A technology arms race offset by defences

In a technology arms race, the adoption of AI and automation accelerates with fraudsters using it as an attack mechanism and the industry as a defensive tool. As technology continues its rapid advancement, fraud is becoming increasingly automated, scalable and personalised, enhancing fraudster capability. In parallel, AI is also improving payment security and allowing greater detection of fraud.

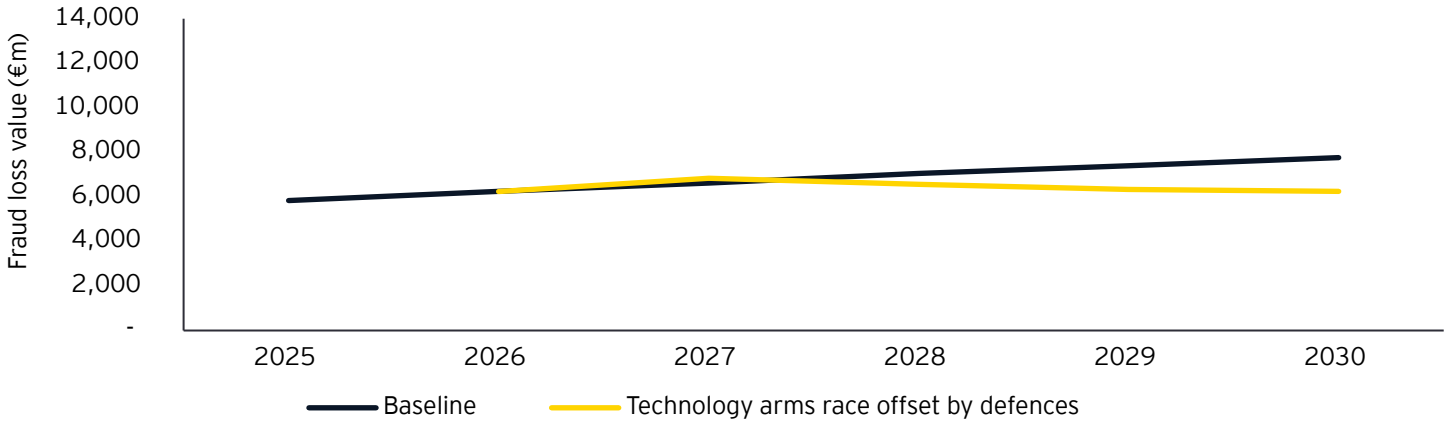
This scenario assesses a future where financial institutions, payment providers, technology firms and other participants across the payment landscape continue to successfully deploy a range of advanced prevention and detection capabilities to stop attacks earlier and mitigate losses, offsetting the emerging threats of AI and other technologies on the resulting fraud risks.

Outcomes to 2030

Over the next 12 months, rapid advancements in AI are expected to outpace the immediate response from industry and regulators, resulting in fraud continuing to grow slightly above the baseline. However, if institutions can continue to roll out improved security measures and controls targeting the capabilities of advancing AI and technology and react swiftly to adapt defences, over time fraud may fall to below the baseline estimate to €6 billion in total fraud losses in 2030, keeping fraud close to current levels. This could result in over €3 billion in fraud losses avoided over the next four years including €2 billion alone in 2030 avoided when compared to the baseline.



Europe level fraud loss values (€m) from 2025–2030



The successful outcomes of the implementation of AI and technologically enhanced defensive capabilities will be dependent on effective integration and the widespread adoption across Europe. For example, within the EU, EU Digital Identity Wallets could reduce the effectiveness of attacks based on stolen identity data, fabricated documents and synthetic media where banks validate credentials and holder proofs correctly. Conversely, uneven adoption, weak recovery processes and less secure alternative journeys could preserve opportunities for impersonation.

Case study: Denmark – AI-enabled fraud detection

Danske Bank has deployed AI and machine-learning capabilities to strengthen real-time fraud detection. The AI-driven fraud platform uses machine learning to analyse large volumes of transaction data in real time, helping the bank move beyond its traditional rules-based approach.

According to Teradata, the implementation increased true-positive fraud detection by 50% while reducing false positives by 60%. More recently, Danske Bank selected Featurespace's adaptive fraud-detection technology to strengthen real-time card-fraud detection, with fraud response times reducing from around 10 minutes to 24 seconds.

4. Public and private data sharing is widespread

Widespread information sharing between banks, payment service providers, governments and enforcement agencies, technology firms and other participants within the payment ecosystem presents a significant opportunity for fraud reduction. This scenario examines how a response to fraud through enhanced collaboration and real-time intelligence exchange, alongside defensive responses, could alter fraud outcomes.

For data sharing to be successful at scale it is assumed that organisations are increasingly required and able to exchange fraud intelligence in near-real-time, supported by improvements in governance, interoperability, data-sharing frameworks and harmonised fraud reporting and taxonomy. As participation expands, fraud signals identified by one participant can be used to strengthen protections across the wider ecosystem, increasing the effectiveness of collective fraud prevention efforts. Enhanced visibility of fraud data, mule networks, suspicious accounts and emerging fraud typologies enables earlier intervention, more effective disruption and faster identification of fraud patterns across institutions.

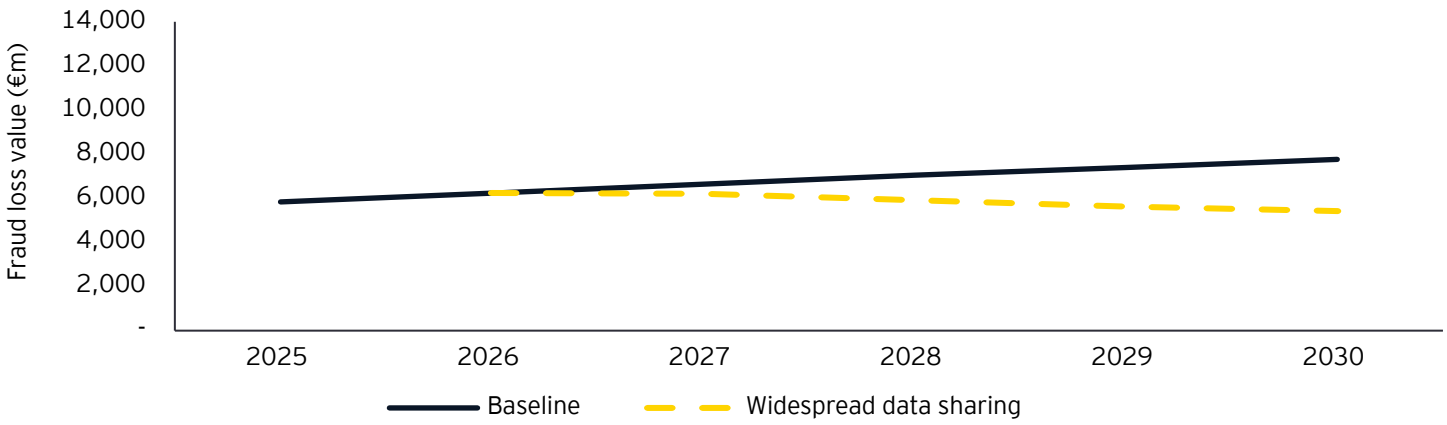
Outcomes to 2030

Widespread collaboration presents a significant opportunity for fraud prevention in Europe. With widespread data sharing, fraud losses may stabilise and reduce when compared to the baseline forecast. In 2030, fraud losses could fall to around €5 billion, a 30% reduction from the baseline in that year. This could result in around €6 billion in fraud losses avoided over the next four years.

The strongest benefits are expected in fraud typologies involving repeated criminal activity, mule account networks and known fraud defence infrastructure (e.g. account limits). Shared data and intelligence may allow institutions to identify patterns in fraud behaviours earlier and intervene before fraud occurs, either prior to account creation or at the time of payment initiation and authorisation.



Europe level fraud loss values (€m) from 2025–2030



The benefits of data sharing are likely to become increasingly significant over time. As more private and public participants contribute data and intelligence and fraud detection capabilities become increasingly interconnected, a more cohesive ecosystem overall can improve fraud prevention performance. While fraudsters continue to adapt and shift tactics, the overall growth trajectory of fraud losses is expected to moderate and begin to decline. Beyond 2030, a mature ecosystem with real-time information sharing and coordinated intervention could increase detection rates further, not only reducing successful attacks by fraudsters but interrupting their ability to adapt to defences and shift their tactics.

The success of this scenario depends on balancing fraud prevention objectives with privacy expectations. Effective data-sharing arrangements will require clear governance frameworks defining lawful purposes, necessary data attributes, access controls and retention periods, while avoiding unnecessary tracking of individuals across services. Maintaining these safeguards will be important to preserving consumer trust and confidence in data-sharing initiatives.

Deep dive: Which countries are driving fraud savings?

Leveraging AI and other emerging technologies can provide an opportunity to reduce fraud losses over time. Countries and institutions that invest more rapidly in digital identity infrastructure and AI-enabled fraud controls and implement collaborative data sharing across the payments ecosystem may experience slower growth or even a reduction in fraud losses than the wider European market.

Across the European markets analysed, France, the UK, Spain and Germany account for some of the largest reported fraud loss totals and therefore represent the greatest opportunity to reduce the overall European fraud burden. As a result, these four countries are the primary drivers of fraud savings in the upside scenarios where additional fraud prevention is implemented. By 2030, these countries may experience significant reductions when compared to the baseline, demonstrating how improvements in the largest markets can have a significant impact when evaluating total European fraud losses.

Compared with the 2030 baseline, these countries could see the following range of fraud loss savings from successfully implementing additional defensive initiatives and cross-industry collaboration[27]:

- France: €220 million to €280 million
- UK: €360 million to €390 million (£310 million to £336 million)[28]
- Spain: €130 million to €150 million
- Germany: €80 million to €140 million

4.5 | Outcomes and implications

This section has evaluated two adverse (downside) and two prevention-led (upside) illustrative scenarios of fraud losses to 2030. These were developed based on key themes shaping the future of fraud losses across Europe to illustrate how fraud losses could respond to different risks and opportunities. The scenarios do not represent actual forecasts rather demonstrates different implications and highlights different priorities for future fraud prevention.

There is around €7 billion difference in fraud losses between the greatest upside scenario where collaboration and data sharing is widespread, and the most adverse downside scenario where fraudsters successfully outpace defences by leveraging AI and technology.

Additionally, when compared to the baseline of fraud (€8 billion by 2030), the upside scenario where collaboration and data sharing is widespread, could result in a cumulation of around €6 billion in fraud losses avoided over the next four years highlighting that data sharing may be a key opportunity for fraud reduction. It is expected that aspects of these scenarios evaluated could occur simultaneously meaning fraud prevention could accelerate further and learnings from each are relevant for today's payment system.



27 All figures are illustrative only and based on scenario forecasts developed as part of this assessment. They do not account for individual country actions that may occur to 2030.

28 Uses the Euro foreign exchange rate per the ECB, 5 October 2026. Euro foreign exchange reference rates



Public and private data sharing is widespread

Widespread data-sharing demonstrates the potential benefits of a system wide defensive response creating a more connected ecosystem.

Widespread intelligence sharing could materially improve the ability of participants to identify emerging threats, detect linked fraud account creation and activity and prevent losses.

€5 billion in fraud losses in 2030, €2 billion less than the baseline.

Technology arms race offset by defences

Rapid technology growth advancing AI related fraud capabilities is presenting as both a key risk but also an opportunity for the fraud landscape.

Where the industry can continue to deploy advanced defensive technologies fraud losses can be identified in real time and avoided in the future.

€6 billion in fraud losses in 2030, €2 billion less than the baseline.

Organised crime and fraud-as-a-service grows

Evolving payment methods and increasing cross-border payments overlayed with technology and criminal capability expansion is allowing fraud to become more instant and globalised.

As fraud becomes more and more cross-border and commercialised organised crime-led fraud may continue to scale faster than efforts to prevent it.

€10 billion in fraud losses in 2030, €2 billion more than the baseline.

Technology arms race where fraudsters outpace defences

As fraudsters gain access to increasingly sophisticated tools enabled by technologies and AI capabilities, traditional controls based on historical patterns may become less effective allowing fraud to grow rapidly.

€12 billion in fraud losses in 2030, €5 billion more than the baseline.

*Figures may not sum due to rounding.

Ways in which the industry can respond to the risks and take advantage of the opportunities

Whether enabled by evolving payment behaviours, AI and other technologies, organised and more globalised criminal networks or fragmented information across institutions, fraud is becoming more scalable, adaptive and difficult to detect. As fraud becomes more global, data-driven and technologically enabled, successful responses are likely to depend on a combination of technological innovation, intelligence sharing and coordinated action across the payment ecosystem. Given the future fraud landscape the industry can respond in ways such as:

- AI-driven fraud detection
- Stronger identity and authentication solutions
- Enhanced real-time decision making
- Maintaining consumer trust in digital payments
- Intelligence-led disruption
- Mule account identification and network disruption
- Cross-border collaboration
- Coordinated enforcement efforts
- Widespread fraud reporting and intelligence sharing
- Common data standards and interoperability
- Privacy and governance frameworks
- Collective fraud prevention capabilities

The following section builds on these findings and the actions identified from each theme. It considers strategic recommendations for industry participants, policymakers and consumers, identifying the key actions that could help strengthen resilience against future fraud risks.



5 Preventing the fraud of the future

The scenarios explored in the last section demonstrate that the future trajectory of fraud is not predetermined. While advances in technology and increasingly sophisticated criminal capabilities present new risks, the analysis also highlights the significant opportunity for the payments ecosystem to strengthen fraud prevention and reduce future losses.

Across Europe, considerable progress has already been made through stronger authentication, improved fraud detection, regulatory interventions and greater industry collaboration. These developments provide a strong foundation on which to build.

Looking ahead, the greatest opportunities lie in harnessing emerging technologies, strengthening identity assurance, improving intelligence sharing and enabling more coordinated intervention across the fraud lifecycle. The effectiveness of these measures will depend not only on individual organisations' capabilities, but also on how successfully the wider ecosystem works together.

This section sets out targeted recommendations for industry participants, policymakers and consumers to strengthen fraud prevention, improve resilience and maintain trust in an increasingly digital payments ecosystem.

5.1 | Overview

The scenario analysis identifies a range of emerging risks and future scenarios that may materialise between now and 2030. These scenarios highlight how rapid technological advancement, the industrialisation of organised crime and fraud-as-a-service, and greater data availability could reshape both fraud threats and fraud prevention across Europe. Our findings show that key implications could include a growing technology arms race between fraudsters and the industry, increasingly scalable and cross-border criminal operations, and the expanding role of data and intelligence sharing in detecting and disrupting fraud. Together, they point to priority areas for action e.g., stronger fraud detection and identity assurance, intelligence-led disruption of mule networks and organised crime, and enhanced data sharing.

This section translates the key priority areas into practical recommendations for industry participants, policymakers and consumers. Collectively, they are intended to mitigate the risks arising from the technology arms race, the growth of organised crime and fraud-as-a-service, and the increasing importance of ecosystem-wide intelligence sharing, while preserving trust, innovation and confidence in the payments ecosystem.

5.2 | Recommendations for industry

For this report, "industry" should be interpreted broadly to include banks, PSPs, card schemes, merchants, acquirers, digital platforms, telecommunications providers, identity providers, crypto-asset businesses and other participants that play a role in customer onboarding, authentication, payment processing, fraud detection and the movement of funds. Whilst technological innovation continues to improve payment speed, convenience and security, it is also providing fraudsters with new opportunities to operate at greater scale and sophistication. In such an operating environment, effective fraud prevention will no longer rely on individual organisations operating in isolation. The industry can therefore improve its resilience against future fraud by potentially taking the following actions:

1. Strengthen detection across the full customer lifecycle.

Developing a broader view of customer activity across the full customer and payment lifecycle by the industry is necessary to identify fraud risks that may not be apparent through transaction monitoring alone. Relevant risk indicators may emerge during onboarding, account recovery, device changes, SIM replacements, beneficiary creation, merchant interactions, wallet enrolment and the movement of funds through receiving accounts.

Individual events may appear legitimate in isolation but become higher risk when viewed together. For example, a recent SIM swap, a new device, an unusual beneficiary, engagement with a high-risk advertisement and the rapid movement of funds through a receiving account may each appear inconclusive on their own. However, when combined, these factors may indicate an elevated risk of fraud.

2. Strengthen identity assurance across onboarding and recovery

Industry participants should consider strengthening identity verification and authentication across the customer lifecycle, including onboarding, account recovery, device replacement and transaction execution. As fraudsters use synthetic identities, deepfakes and AI-enabled impersonation, organisations should adopt layered identity assurance that validates multiple identity attributes and trusted data sources rather than relying on single credentials.

Banks and PSPs should implement clear policies for accepting digital and wallet-based credentials, including checks on issuer trust, validity, cryptographic integrity, revocation status and proof of possession, while ensuring credentials match the customer and transaction. Higher-risk activities such as account recovery, device replacement and account re-binding should be subject to enhanced, risk-based verification and monitoring.

Institutions should continue investing in adaptive authentication, digital identity solutions, biometrics and behavioural analytics to strengthen real-time risk assessment, improve detection of sophisticated impersonation attempts and minimise unnecessary friction for legitimate customers.



3. Prioritise mule-network disruption

Firms should consider treating mule detection as both a fraud and an anti-money laundering intervention. Effective controls may need to identify both individual mule accounts and the networks connecting them. Sending and receiving firms should consider establishing rapid communication and escalation arrangements so that suspicious proceeds can be restricted before they are layered through additional institutions.

Intelligence sharing across banks, payment service providers and other ecosystem participants, where legally permissible, is necessary to identify and disrupt fraud and mule networks that extend beyond the visibility of any single organisation. The success of Europol's European Money Mule Action (EMMA), which coordinates large-scale intelligence sharing and enforcement activity across law-enforcement agencies and thousands of financial institutions, demonstrates the value of collaborative mule-network disruption and coordinated cross-border intervention.

4. Coordinate fraud intelligence and controls at ecosystem level

Participants across the card and non-card payments ecosystem, including merchants, issuers, wallet providers, electronic money institutions, FinTechs, payment processors, digital service providers and telecommunications providers, should continue to strengthen the sharing and integration of fraud intelligence. This should include card-testing, bot, device and merchant intelligence across the network. Fraud attacks may be distributed across multiple participants, channels and merchants making them difficult to identify through controls applied by individual organisations in isolation. Continued collaboration and investment



in advanced detection capabilities will help identify emerging attack patterns quickly and disrupt fraud activity at scale.

5. Prepare for frontier AI and quantum technologies

Firms should consider taking a forward-looking approach to emerging technologies and assess how frontier AI models, autonomous agents and future advances in quantum computing may affect fraud risks in their existing control frameworks. This includes evaluating risks associated with AI-enabled manipulation, autonomous decision-making and emerging threats to digital identity, authentication and cryptographic security. Early planning and ongoing monitoring will help firms strengthen resilience as these technologies mature. Firms should also explore how these technologies can strengthen fraud prevention and detection capabilities, including how they can be used to enhance behavioural analytics, anomaly detection, identity verification and real-time fraud monitoring.

5.3 | Recommendations for policymakers

Policymakers play a critical role in shaping the regulatory, legal and operational frameworks that support fraud prevention across the payments ecosystem. As fraud becomes more technology-driven, cross-border and interconnected, effective responses will depend on balancing innovation, consumer protection and collaboration across industry sectors. Policymakers can therefore take the following actions to help strengthen the resilience of the European payments ecosystem against emerging fraud risks and future threats:

1. Evolve regulatory expectations beyond authentication

Current fraud controls heavily focus on verifying the identity of the payer. Combatting manipulation-based fraud is however, likely to require greater emphasis on

payment context, customer behaviour and receiving-account risk. Effective fraud prevention depends on understanding not only who is making a payment, but also why it is being made, who is receiving it and whether the surrounding circumstances are consistent with legitimate activity.

Regulatory frameworks may consider supporting this shift by encouraging proportionate use of behavioural, device, beneficiary and receiving-account intelligence to identify fraud risks that may not be apparent through authentication controls alone. Regulatory approaches should remain sufficiently flexible and outcomes-focused, enabling firms to adopt risk-based controls that are most effective in their specific operating environments rather than prescribing particular solutions.

2. Enhance existing VoP framework to enable the sharing of more detailed counterparty-risk information

The current European VoP framework focuses primarily on identifying discrepancies between a payee's name and account details before a standard or instant payment is completed. There may be further opportunities to enhance the framework by enabling the secure sharing of richer information about counterparties and risk indicators, to provide customers and PSPs with more meaningful insights. Subject to appropriate legal, privacy and operational safeguards, future approaches could explore how relevant indicators of receiving-account risk may be communicated prior to payment authorisation. Such information could complement existing name-matching controls by helping customers make better-informed payment decisions where the recipient, receiving account or wider payment context presents an elevated risk of fraud.

3. Enable proportionate, intelligence-led friction

Maintaining the benefits of instant payments while allowing proportionate intervention is likely to be necessary to reduce losses where there are credible indicators of customer manipulation or rapid fund dispersal. While instant payments provide significant benefits to consumers and businesses, their speed can reduce the opportunity to investigate suspicious activity, restrict funds or recover fraud proceeds.

Policymakers could therefore consider frameworks that enable targeted, intelligence-led friction in higher-risk circumstances without introducing unnecessary delays into legitimate payments. Depending on the nature and strength of the risk indicators, this could include enhanced warnings, additional verification or other proportionate interventions before funds are transacted and become irrecoverable.

4. Align incentives and responsibilities across the fraud ecosystem

Fraud is an ecosystem-wide issue that can originate through digital platforms and other channels, exploit vulnerabilities across multiple sectors, including telecommunications and payment services, and ultimately result in funds being transferred to mule accounts, crypto-asset exchanges or digital wallets. A clear allocation of responsibilities and incentives across the organisations that influence fraud outcomes is likely to be necessary to achieve sustained prevention, detection and disruption.

Policy frameworks could therefore consider aligning responsibilities and incentives with each participant's ability to prevent, detect, disrupt or respond to fraud. By ensuring that accountability reflects the role each participant plays in the fraud lifecycle, policymakers can encourage proportionate investment across payment service providers, telecommunications companies, digital platforms and other relevant participants, while maintaining consumer protection and avoiding disproportionate reliance on any single sector.

5. Promote harmonised fraud reporting and taxonomy across Europe

Effective policymaking depends on consistent and comparable fraud data. Policymakers should continue efforts to harmonise fraud definitions, reporting requirements and measurement methodologies across jurisdictions and sectors. Improved consistency would enhance understanding of fraud trends, support evidence-based decision making, facilitate cross-border cooperation and allow more effective assessment of the impact of regulatory and industry initiatives.

6. Provide greater regulatory clarity to support fraud intelligence sharing

Policymakers and regulators should consider providing clearer guidance on how fraud intelligence can be shared lawfully, proportionately and securely across institutions, payment channels and sectors. EU data protection requirements allow personal data to be processed for fraud-prevention purposes where an appropriate legal basis and safeguards are in place. Greater regulatory clarity could give organisations greater confidence to collaborate while protecting personal data and supporting more effective fraud detection and disruption.

5.4 | Recommendations for consumers

Digital innovation is delivering significant benefits for consumers across Europe. Instant payments, digital identity solutions, mobile wallets, open banking services and emerging AI-powered tools are making payments faster, more convenient and more personalised. At the same time, fraudsters are using the same technologies to make scams more convincing and harder to detect.

While financial institutions, payment providers, technology firms and policymakers all have important roles to play in preventing fraud, consumers can further strengthen their resilience by adopting a small number of practical steps when faced with unusual requests, unfamiliar investments that may be indicative of potential fraud.

1. Verify unusual requests through a trusted channel

The findings indicate the need for consumers not to rely solely on a familiar voice, photograph, video call, email address or social-media profile as proof of identity. Where someone requests money, sensitive information or urgent action, verification through an independent and previously established channel could provide an additional safeguard.

When using an identity wallet, consumers should check who is requesting information, which attributes will be disclosed and whether the request matches the service they intended to use. Unsolicited requests to activate, recover or use a wallet should be verified through an established channel. Recognition of the requesting organisation does not, by itself, make a payment request safe.

2. Pause and pay attention to typical fraud red flags

Many frauds rely on creating urgency, secrecy or pressure. Fraudsters are shifting from stealing payment credentials to manipulating genuine customers into authorising transactions themselves. They may coach victims on what to say to their bank, instruct them to ignore security warnings or pressure them to override payee verification checks. Pausing and independently verifying unusual payment requests is necessary to protect against APP fraud and other social engineering scams.

Consumers should view payment and security warnings as an opportunity to pause and reassess a situation, particularly where they are asked to override warnings, transfer funds urgently or send money to unfamiliar accounts.

3. Apply enhanced checks to investments and alternative assets

Consumers should exercise additional caution when considering unfamiliar investments, particularly those involving cryptocurrency, stablecoins, high-value physical assets, unfamiliar trading platforms, or investments offering unusually consistent returns. Physical or digital assets should not automatically be regarded as safe simply because they appear tangible, technologically advanced or resilient to inflation. Independent verification of the investment, provider or platform can help reduce exposure to fraud.

4. Act quickly if fraud is suspected and preserve evidence

Consumers should consider contacting their payment provider immediately where they suspect fraud, even if they authorised the transaction themselves. Rapid reporting gives providers a better opportunity to contact receiving institutions, restrict mule accounts and attempt recovery before funds move through additional accounts or jurisdictions. Consumers should consider preserving messages, account details, advertisements, usernames, receipts, transaction references and website addresses.

5. Use available security features

Consumers should enable available security features such as multifactor authentication, biometric authentication and transaction alerts where offered by their financial institution or service provider. These measures can help detect unauthorised activity and reduce the risk of account compromise.

Case studies:



Belgium – Cross-sector collaboration and shared responsibility for tackling online fraud[29]

Belgium is strengthening its response to online fraud through a coordinated approach spanning the banking sector, government and the wider digital ecosystem. The Belgian banking sector's 2026 action plan combines stronger bank-level prevention and detection, enhanced interbank intelligence and data sharing, and increased collaboration with other ecosystem participants, including telecommunications operators and social media platforms. The approach reflects the recognition that online fraud cannot be addressed by banks alone and should, where possible, be disrupted closer to its source.



Europe – Collaborative disruption of money-mule networks[30]

Europol's European Money Mule Action (EMMA) demonstrates the potential impact of coordinated public-private and cross-border intervention. During EMMA 9, law enforcement agencies from 26 countries worked with Europol, Eurojust, INTERPOL and private-sector partners, with 2,822 banks and financial institutions supporting the operation. The initiative identified 10,759 money mules and 474 recruiters, resulting in 1,013 arrests and €32 million in losses being prevented. The initiative demonstrates how public-private information sharing and coordinated cross-border action can support the identification and disruption of money-mule networks.



France – Strengthening identity assurance through SCA and 3-D Secure for remote card payments[31]

France demonstrates how stronger authentication can reduce payment fraud while controls continue to evolve in response to changing fraud patterns. According to the Banque de France, the progressive implementation of Strong Customer Authentication (SCA), supported by 3-D Secure for remote card payments, has reduced fraud rates for remote payments made through 3-D Secure. With fraud remaining structurally higher for remote payments outside 3-D Secure, the French Observatory for the Security of Payment Means (OSMP) has introduced further measures to strengthen the security of these payment journeys.



UK – Cross-sector coordination to prevent and disrupt fraud[32]

The UK Government's Fraud Strategy 2026-2029 sets out a cross-sector approach to tackling fraud, bringing together government, law enforcement, regulators, industry and civil society. Structured around Disrupt, Safeguard and Respond, it focuses on disrupting the tools, platforms and financial flows exploited by fraudsters, strengthening resilience and improving victim support and enforcement. Its emphasis on industry collaboration and tackling fraud closer to its source demonstrates how coordinated action can strengthen prevention across the wider ecosystem.

29 Minister Rob Beenders and Belgian banks step up the fight against online fraud with action plan | Febelfin

30 Paper trail ends in jail time for 1 013 money mules – 2 822 banks and financial institutions join forces with law enforcement agencies in global effort against money laundering | Europol

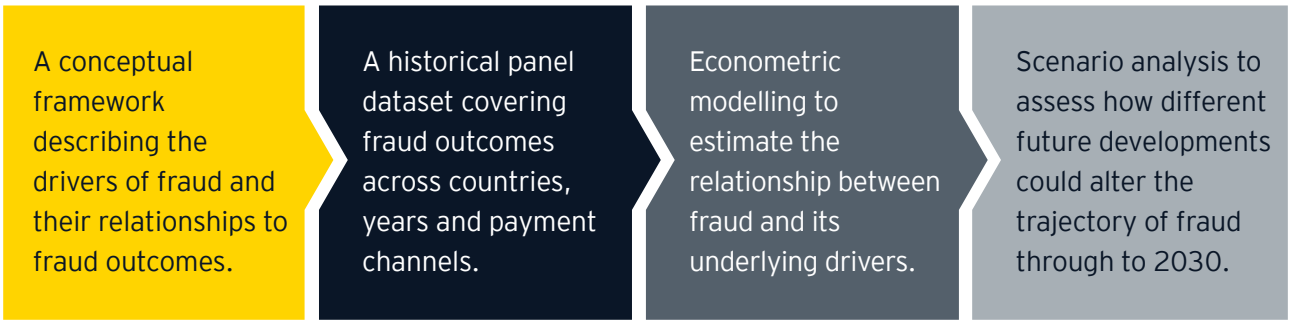
31 250408_OSMP_Fraud_prevention_measures_on_remote_card_payments_outside_3_D_Secure_0.pdf

32 Fraud Strategy 2026 to 2029 – GOV.UK

6 Technical Appendix

6.1 | Overview of the modelling approach

The objective of this assessment is to estimate how fraud across Europe may evolve by 2030 under alternative future scenarios. To do this, a four-staged approach was undertaken:



The approach is intended to quantify the potential direction and scale of change in fraud losses under different future conditions rather than predict a single outcome. The modelling framework therefore combines historical evidence with forward-looking assumptions regarding technological change, regulatory developments, criminal capability and ecosystem responses.

6.2 | Conceptual framework

To understand how the different current, emerging and future drivers of fraud may affect the fraud losses, a framework was developed. The "conceptual framework" illustrates how key drivers are expected to influence behaviours that, in turn, shape fraud outcomes. The conceptual model serves as the foundation for both the econometric analysis and scenario development.

The framework grouped market trends and drivers of fraud into five overarching categories: payment structure drivers, macroeconomic drivers, technology drivers, regulatory drivers and societal drivers. These drivers were then mapped to their intermediate effects, then outcomes and lastly impacts on fraud losses.

Table 1: Conceptual framework categories and example drivers of fraud

Category	Explanation	Example drivers of fraud
Payment structure drivers	Examines how changes in payment methods and payment infrastructure influence fraud trends over time. This includes developments such as real-time payments, open banking and cross-border payments.	▪ Adoption of instant and account-to-account payments ▪ Growth in digital wallets ▪ Open banking adoption ▪ Remote commerce ▪ Cross-border payment activity
Macroeconomic drivers	Explores the extent to which macroeconomic factors such as unemployment, inflation, household or consumer debt and gross domestic product (GDP) per capita influence historical and future fraud trends.	▪ Gross domestic product (GDP) per capita ▪ Inflation ▪ Unemployment ▪ Consumer and household debt
Technology drivers	Assesses how technological developments create fraud risks. This includes, for example, advancements in AI and deepfakes, digital currencies and digital assets.	▪ AI adoption ▪ Deepfakes ▪ Fraud-as-a-service ▪ Digital identity solutions ▪ Defensive fraud technologies
Regulation, prevention and liability drivers	Considers the impact of regulatory changes, fraud prevention measures and liability frameworks on fraud outcomes. This includes the impact of authentication mechanisms, shared ecosystem responsibility and mandatory reimbursement.	▪ SCA requirements ▪ Digital identity frameworks ▪ CoP and similar verification initiatives ▪ Liability and reimbursement frameworks ▪ Information sharing arrangements
Behavioural and societal drivers	Examines how demographic, behavioural and societal factors may influence consumer behaviour, fraud vulnerability and susceptibility to scams. This includes changes in digital literacy, use of digital platforms, consumer trust and population demographics.	▪ Demographic trends ▪ Population age structure ▪ Digital literacy ▪ Social media literacy ▪ Consumer awareness and trust

6.3 | Econometric modelling

Scope and dataset construction

The econometric analysis is based on a panel dataset for 28 jurisdictions, using half-yearly data from 2016 to 2025 across four payment channels. The data draws on various sources, led by the European Central Bank (ECB) and UK Finance, with economic data from Oxford Economics.

Table 2: Modelling framework

Data set	Inclusions
Number of years	2016–2025 historical period, 2026–2030 forecast period
Number of jurisdictions	28 – The 27 EU Member States and the UK
Payment channels	Card payment, credit transfer, e-money payment, cash withdrawals

Fraud outcome data was consolidated from multiple sources and standardised into a consistent structure by country, payment channel and year. Fraud values and transaction values were combined to calculate fraud rates for each observation. Data quality reviews were undertaken to assess coverage, identify outliers and document any limitations or assumptions required where data gaps existed.

Econometric modelling framework

The econometric framework was designed to estimate the relationship between fraud outcomes and their underlying drivers identified in the conceptual framework.

The methodology involved estimating three models:

- Card payment fraud
- Credit transfer fraud
- A combined model including e-money payment fraud and cash withdrawal fraud.

There is a separate model for card payments because it is the payment channel with the highest transaction volumes and one for credit transfers because it is the payment channel with the highest transaction values. The other payment channels were combined into one model. The combined model does not cover direct debits because there is limited historical fraud data.

The primary dependent variable for the card payments and credit transfer models was the fraud value for a given country, payment channel and half year. For the e-money payments and cash withdrawals combined model, the dependent variable was fraud rate because it allows better comparability between two different payment channels.

The card payment fraud and credit transfer fraud models are two-way fixed-effect models with country and time fixed effects, while the combined model is a one-way fixed-effect model with only country fixed effects but includes a time trend variable. The country effects were included to account for persistent differences between jurisdictions, while time effects were used to capture broader market developments affecting all countries simultaneously. All models include at least one explanatory variable from all five driver categories of the conceptual model (see Table 1) however, variables differ across models depending on the strength of the estimated relationships.

Where direct measurement was not possible, proxy variables and composite indices were developed. These indices were designed to capture broader concepts such as regulatory effectiveness and criminal capability. There is one regulation index per payment channel to reflect the fact that regulations affect different payment channels in different ways. The regulation indices account for SCA, VoP/CoP, APP reimbursement (UK only) and contactless payment limits (card payments only). The index is a score that averages the impact of each regulatory instrument on each payment channel. The main variation comes from when the regulations were introduced.

Variables were tested for statistical significance, interactions between drivers and potential non-linear effects.

The modelling process also assessed alternative specifications to ensure the robustness of results and to better reflect the complexity of fraud dynamics. This included testing interactions between key drivers and exploring whether the effects of certain variables strengthen or weaken beyond specific thresholds.

Table 3: Model specifications

Card payment fraud	Credit transfer fraud	E-money payment fraud and cash withdrawal fraud
Dependent variable: ▪ Fraud loss value **Explanatory variables:** ▪ Payment value ▪ GDP per capita ▪ AI use ▪ Percentage of population over 65 ▪ Criminal actor score ▪ Regulatory index.	**Dependent variable:** ▪ Fraud loss value **Explanatory variables:** ▪ Cross-border payments value ▪ Unemployment rate ▪ Inflation rate ▪ Social media use of individuals ▪ AI use ▪ Criminal actor score ▪ Regulatory index.	**Dependent variable:** ▪ Fraud loss rate **Explanatory variables:** ▪ Payment value ▪ Unemployment rate ▪ Inflation rate ▪ AI use ▪ Criminal actor score ▪ Regulatory index.

Baseline forecasting

The baseline forecast provides a view of how fraud may evolve if current trends continue and no major structural disruption occurs.

To model this:

- Future values for explanatory variables were developed using a combination of external forecasts, observed historical trends and published evidence.
- The baseline assumes that payment values will grow at the Compound Annual Growth Rate (CAGR) calculated from 2023-2025 data, although with adjustments to reflect expectations about how the payment mix will change to 2030.
- Macroeconomic drivers of fraud, such as GDP per capita, unemployment and inflation, and the societal drivers of fraud, such as the percentage of the population aged 65 or more, are projected forward based on the latest published forecasts by Oxford Economics, reflecting the current macroeconomic and demographic expectations for each country under assessment.
- The regulation indices are assumed to stay at the 2025 H2 level until 2028 H2 when the outcomes of Payment Services Regulation are expected to start being implemented (excludes UK). All other drivers remain at the 2025 H2 level for the forecast period because there is insufficient published evidence on how they will evolve at the country level to 2030.

The estimated econometric relationships were then applied to these future assumptions to generate annual forecasts of fraud losses through to 2030. The baseline serves as the reference case against which all future scenarios are assessed.

Scenario development and modelling

Scenario analysis was undertaken to assess how different future developments may alter fraud outcomes relative to the baseline forecast.

The scenarios were developed using the conceptual framework and engagement with Visa stakeholders. Each scenario reflects a plausible but uncertain future pathway rather than a prediction.

The scenarios are as follows:

1. A technology arms race where fraudsters successfully outpace defences by leveraging AI and technology and increase successful fraud attempts.
2. Growth in organised crime and fraud-as-a-service furthers the industrialised and globalised nature of fraud increasing fraud losses.
3. A technology arms race where institutions leverage AI and technology to reduce fraud losses over time.
4. Widespread data sharing between stakeholders across the payment ecosystem effectively reduces fraud losses.

For each scenario, selected explanatory variables were adjusted relative to the baseline forecast. These adjustments reflected the scenario narratives and represented either positive or negative shocks to the underlying fraud drivers.

The outputs of each scenario were evaluated against the base case to observe the direction and relative scale of impact. It is noted that the themes explored within each scenario are likely to occur concurrently and are interrelated. However, for the purposes of this analysis, each has been tested as a standalone scenario.

6.4 | Data sources

In preparing this study, EY has drawn on information from publicly available data sources, supplemented by data provided by Visa. The data and sources used are provided in Table 4.

Table 4: Main data sources

Type of data	Data sourced for modelling	Source
Fraud loss	Fraud loss value/rate by payment channel by country	ECB, UK Finance, national banks, Visa
Payment structure drivers	Payment value by payment channel by country	ECB, UK Finance, national banks
	Cross-border payment value by payment channel by country	ECB, BIS
Macroeconomic drivers	GDP per capita by country	Oxford Economics
	Unemployment rate by country	Oxford Economics
	Inflation rate by country	Oxford Economics

Type of data	Data sourced for modelling	Source
Technology drivers	AI use by country: percentage of enterprises with 10 persons employed or more that use at least one type of AI	Eurostat
	Social media use by country: percentage of individuals who used the internet for accessing social networking sites in the last three months	OECD
Regulation, prevention and liability drivers	Strong Customer Authentication: share of SCA transactions (value) by payment channel	ECB
	VoP/CoP introduction date	ECB, Pay.UK
	Authorised Push Payment reimbursement (UK only): percentage returned to victim	UK Finance
	Contactless payment limit by country	Visa news, Mastercard news
Behavioural and societal drivers	Demographic change by country: percentage of population aged 65 or more	Oxford Economics
	Organised crime by country: criminal actor score	Global Organised Crime Index

6.5 | Limitations

As with any long-term forecasting exercise, the analysis is subject to uncertainty.

The future evolution of fraud will depend on technological developments, consumer behaviour, criminal innovation, regulatory responses and broader economic conditions that cannot be predicted with certainty. In addition, data availability varies across countries, payment channels and fraud typologies, requiring the use of assumptions, proxy variables and composite indicators in some areas.

The scenarios presented in this report should therefore be interpreted as illustrations of how fraud may evolve under different future conditions rather than forecasts of what will occur. Their purpose is to provide insight into the drivers most likely to influence fraud outcomes and the relative scale of potential impacts across the European payment ecosystem.

Approach to data limitations

Prior to estimating the models, assumptions were made to improve the publicly sourced datasets. To retain the granularity of the half-yearly fraud loss data, any annual data was converted into half-yearly data.

To fill data gaps, the following approach was taken: where gaps occurred within periods, e.g. 2024 in a dataset covering 2016-2025, the gap was filled by taking the average of values from adjacent periods. Where gaps occurred at the start or end of periods, e.g. 2025 in a dataset which should cover 2016-2025, the gap was filled by carrying forward (or carrying backward

if the gap is at the start) the value from the closest available period. However, there are exceptions to this rule which are outlined below:

- One exception is the criminal actor score from the Global Organised Crime Index, which is only available for 2021-2025. It is unrealistic to assume that the score was at the 2021 level for the whole of 2016-2020 given that the score increased for countries such as the UK, France and Germany between 2021 and 2025. Instead, the criminal actor score was projected back using 2021 data and CAGRs for each country based on the available data.
- Another exception is AI use, which is only available from 2021. In the periods before 2021, the percentage is assumed to be zero for all countries because firms were unlikely to be using AI to any significant degree before 2021. A further assumption for AI use is used to account for the fact that there is no data for the UK. The UK values are assumed to be the same as the values for France, which is economically comparable to the UK.
- A similar approach was taken with social media use for Cyprus and Malta. Ireland is the best comparator country for Malta and Cyprus based on both economic and digitisation conditions, so it was assumed that both countries have the same values as Ireland.

However, even after imposing assumptions, some data gaps remain. The lack of data for certain countries together with the exclusion of direct debits from the analysis results in the models potentially underestimating Europe fraud losses.

6.6 | Payment channel definitions

Table 5: ECB payment channel definitions

Payment channel	Definition
Card payment	Card-based payment transaction means a service based on a payment card scheme's infrastructure and business rules to make a payment transaction by means of any card, telecommunication, digital or IT device or software if this results in a debit or a credit card transaction. Card-based payment transactions exclude transactions based on other kinds of payment services.
Credit transfer	Credit transfer means a payment service for crediting a payee's payment account with a payment transaction or a series of payment transactions from a payer's payment account by the payment service provider which holds the payer's payment account, based on an instruction given by the payer.
E-money payment	Electronic money means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions, and which is accepted by a natural or legal person other than the electronic money issuer.
Cash withdrawals	Cash withdrawals means cash withdrawal at an ATM or at the counter of a PSP using a card with a cash function. It includes cash advances at POS terminals ("cash-back" transactions).
Direct debit (excluded from modelling)	Direct debit means a payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee based on the consent given by the payer to the payee, to the payee's payment service provider or to the payer's own payment service provider.

Table of Abbreviations

Abbreviation	Description
AI	Artificial Intelligence
APP	Authorised Push Payment
ATO	Account Takeover
ATM	Automated Teller Machine
BIS	Bank for International Settlements
CAGR	Compound Annual Growth Rate
CHAPS	Clearing House Automated Payment System
Cifas	Cifas, the UK fraud prevention service and operator of the National Fraud Database
CoP	Confirmation of Payee
COSMIC	Collaborative Sharing of Money Laundering/Terrorism Financing Information and Cases
CVV	Card Verification Value
EBA	European Banking Authority
EBF	European Banking Federation
ECB	European Central Bank
EEA	European Economic Area
eIDAS	Electronic Identification, Authentication and Trust Services
EMMA	European Money Mule Action
EPIF	European Payment Institutions Federation
EU	European Union
EY	Ernst & Young
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FIU.net	Financial Intelligence Unit network
FRIDA	Fraud Information Distribution Arrangement
GASA	Global Anti-Scam Alliance
GDP	Gross Domestic Product
GenAI	Generative Artificial Intelligence

Table of Abbreviations

Abbreviation	Description
IDV	Identity Verification
IT	Information Technology
JMLIT	Joint Money Laundering Intelligence Taskforce
LLM	Large Language Model
MAS	Monetary Authority of Singapore
MISP	Malware Information Sharing Platform
MIT	Merchant-Initiated Transaction
MOTO	Mail Order/Telephone Order
NCA	National Crime Agency
NFC	Near Field Communication
OECD	Organisation for Economic Co-operation and Development
OSMP	Observatoire de la sécurité des moyens de paiement
PIN	Personal Identification Number
POS	Point of Sale
PSD2	Second Payment Services Directive
PSD3	Third Payment Services Directive
PSP	Payment Service Provider
PSR	Payment Systems Regulator
SCA	Strong Customer Authentication
SEPA	Single Euro Payments Area
SIM	Subscriber Identity Module
STR	Suspicious Transaction Report
TMNL	Transaction Monitoring Netherlands
UK	United Kingdom
UKF	UK Finance
USD	United States Dollar
VoP	Verification of Payee

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