# Shaping the Future of Strong Customer Authentication (SCA)

## Modernizing Europe's Approach to Fraud Prevention

PayPal

pa eu
the payments association

Deloitte.

# Thank you note


PayPal

The Payments Association EU would like to express its sincere appreciation to Mathilde Bonneau and Patrick Millais from PayPal for sponsoring this initiative and for their continued commitment to broadening the policy dialogue and promoting collaboration between payment players on issues such as fraud.

---

Deloitte.

We also extend our deepest gratitude to Deloitte, in particular Alexandre Havard, Maxime Gaborieau, and Benjamin Cler, for their expertise and their work in the writing of this report. Their analytical expertise, constructive review, and valuable insights have significantly enhanced the quality and depth of this work.

---

This paper would not have been possible without the contributions of the many members that generously shared their experience and expertise by responding to the questionnaire. We are also thankful to the organizations outside the association that took part in individual interviews and provided their perspectives on the evolving landscape of SCA and fraud.

---

Finally, we would like to acknowledge the outstanding work of Noam Bekhor, Staline Fopa Fomekong, and Baptiste Joachim, young graduates from Solvay Brussels School of Economics and Management. Under the supervision of Youcef Tahari and Tom Koning, they showed exceptional dedication in developing and promoting the questionnaire that served as the foundation of the white paper.

# Contents

# About The Payments Association EU

# Making Payments Work

The Payments Association EU is a business club of decision makers in the payments industry. Our members are the enterprises forming all the components of the payments value chain in the 27 countries of the European Union. Our circle is established as a non-profit association registered in Luxembourg. Our offices are hosted at the Luxembourg House of Financial Technology (LHoFT).

The Purpose of the Association is to facilitate business for its members. PA EU seeks to achieve its objectives by organizing events, managing projects, defending the interests of its members, publishing research documents, and providing training. You will find more details in our brochure.

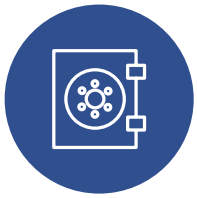
The Payments Association EU, consisting of 100 members from across the payments value chain, including payments schemes, banks and issuers, merchant acquirers, PSPs, retailers, and more.

Collectively, members of the PA EU transact more than 6 trillion € annually and employ more than 300.000 staff, meaning that we now have a significant influence over the industry's future.

### The PA EU provides the payments community with

- A forum in which to learn, collaborate, and do business with contacts you would not otherwise have met.
- A view on pain points that your peers encounter and act upon, such as access to bank accounts, changing industry standards, new regulations, and open banking.
- A perspective that is ahead of the curve, so you can develop products and services in line with what is coming down the road.
- Opportunities to speak to regulators, tap into the heart of central government and engage with authorities to affect change across the wider industry.

## Who should join the Payments Association EU community?


Central Banks


Banks & Issuers

Acquirers & ISOs


Government Bodies


Regulators


FinTechs & PayTechs


Payment Gateways


Retailers & Merchants

TPPs-AISPs PISPs & ASPSPs

Legal & Accounting Firms


Compliance Consultants


Payments Service Providers


Card Schemes


Programme Managers

# Our community

## Our Benefactors

BANKING CIRCLE

Deloitte.

LexisNexis® RISK SOLUTIONS

## Our Patrons

amazon

A&O SHEARMAN

BPC

Brite*

CAB | PAYMENTS EUROPE

COMPLY ADVANTAGE

CompoSecure

enfuce

EQUALS Money

APEX EDB

FIS

Giesecke+Devrient Creating Confidence

kraken

LSEG RISK INTELLIGENCE

payabl.

paymentology

paynt

SCHILTZ & SCHILTZ AVOCATS A LA COUR

sumsub

Swift

TSYS A Global Payments Company

VISA

WORLDLINE

## Our Members

3s.money

airbnb

AlixPartners

ARKEA BANKING SERVICES

BNP PARIBAS

BPCE PAYMENT SERVICES

Chargebacks911

Clear.Bank

convera

dandelion

ebay

ecommbx

epay part of Euronet

epi European Payments Initiative

MAQIT

Fraudio

FTI CONSULTING

IDEMIA SECURE TRANSACTIONS

inswitch

KPMG

LHV

LUXHUB

pwc

MARKET PAY

Modulr

outpayce from AMADEUS

paynetics

Paynovate

PayPal

Up

SELP DIGITAL

SERVIPAY Solutions de paiement

Skaleet

Swissquote

SysPay

tietoevry

Wallester

XMDS

XOAI.A

## Our Scale-Up Members

auric

consalty

FINFLAG SOLUTIONS FOR THE PAYMENT INDUSTRY

iPiD

maksu payments you trust

MetaWallet

NEXTGEN PAYMENT

Ondorse

zwipe

# Why join the Payments Association EU?

If you're going to really prosper in payments, you need access. You need to know the right people. And you need to be on the pitch and make your voice heard.

You also need the freshest news and the latest thinking, and a pool of partners and prospects in which to fish. And you need influence over the future landscape so that when you get there, you thrive.

As a member of the Payments Association EU, you will move your business from reactive to proactive to predictive. From follower to leader. Gaining first-mover advantages or a competitive edge. And you will avoid investing in no-hope technology or risk incurring a regulator's wrath.

## Business Development

Establish new relationships, partnerships, and sales leads while achieving faster time to market, through active participation and engagement in PA EU networking events, projects, activities, and publications.

## Marketing Amplification

Increase your brand awareness, generate sales leads, and maximise your ROI by utilising the PA EU's social media, newsletters, online presence, events, projects, and sponsorship opportunities to increase your reach and reduce spend.

## Collaboration Opportunities

Increase your influence within the industry by collaborating with other buyers, sellers, and partners from across the payments ecosystem to bring about change and direct policy.

## Credibility and Profile

Obtain enhanced credibility, brand awareness, and boost your personal and corporate profile by associating yourself with the PA EU.

## Market Intelligence and Education

Gain a competitive advantage, establish thought leadership, and ensure your team is up to date with priority access to market intelligence, insight, and educational resources. publications.

## Financial Savings

Benefit from the PA' EUs negotiating power and partnerships to maximise the use of your budgets and identify cost savings.

## The Payments Association EU

Thibault de Barsy
Vice-Chairman & General Manager
"The Lhoft", 9 Rue du Laboratoire, 1911 Luxembourg
Phone +352 621 355923
Email thibault.de.barsy@thepaymentsassociation.eu
Website: www.thepaymentsassociation.eu

**Twitter:**
@PAssocEU

**LinkedIn:**
The Payments Association EU

# Executive Summary

Strong Customer Authentication (SCA), introduced in the EU under the second Payment Services Directive (PSD2) to combat payment fraud, has successfully reduced unauthorized account access and established a stronger security baseline for digital payments in Europe.

**Yet these gains have proven partial and short-lived.** As SCA strengthened technical controls, fraudsters adapted - shifting tactics from technical intrusion to human manipulation. Two trends now define the post-SCA fraud landscape:

1. **Exploiting SCA mechanisms:** Attackers use phishing, malware, and data breaches to steal credentials and launch large-scale account takeover attempts. Techniques such as SIM swapping and social engineering compromise one-time passwords (OTPs), undermining the very tools designed to secure transactions.
2. **Authorized payment fraud:** Criminals increasingly deceive customers into approving fraudulent transfers, bypassing SCA entirely. These scams exploit trust and behaviour rather than technology.

While unauthorized fraud has declined, losses have resurfaced through sophisticated social-engineering scams, now the most prevalent form of consumer fraud. Many of these schemes originate outside the financial system - on social media, search engines, telecom networks, and marketplaces - highlighting the need for a cross-sector, coordinated response.

**SCA's success has thus become a double-edged sword: it closed one door but opened others, as fraudsters pivoted to exploit human and systemic weaknesses.** Moreover, stricter authentication requirements have introduced friction in digital commerce, increasing cart abandonment and eroding consumer trust.

**Europe's fight against fraud demands a holistic, multi-layered approach: adaptive regulation, real-time intelligence, cross-sector accountability, strong enforcement, and consumer empowerment. A modernized, intelligence-led approach to fraud prevention will protect consumers, support innovation, and preserve Europe's leadership in digital finance.**

As EU policymakers finalize the fraud prevention framework under the third Payment Services Directive (PSD3) and the Payment Services Regulation (PSR) and consider future fraud prevention initiatives, this vision can be realized through modern, coordinated, and user-centric measures that balance security, innovation, and consumer protection - ensuring Europe's digital economy remains both resilient and globally competitive.

## Recommendations

1

**Future-Proof the Approach to SCA under the PSD3 and PSR.**
SCA has significantly improved payment security but now risks obsolescence if regulation remains tied to static tools such as passwords or SMS codes. The EU should transition toward adaptive, risk-based, and technology-neutral authentication, underpinned by AI-driven intelligence and phishing-resistant methods such as passkeys. A future-proof SCA framework must balance security, usability, and innovation, ensuring proportionality and interoperability across payment methods while avoiding regulatory rigidity.

2

**Build a Layered Fraud-Intelligence Ecosystem, enabled by the PSD3/R.**
The EU should establish a real-time, intelligence-sharing network across the financial sector to enable early detection of emerging threats. Key measures include secure and interoperable data-sharing frameworks, cross-border coordination standards, and financial-sector data hubs - modelled on initiatives like Singapore's Anti-Scam Command Centre - to operationalize collaboration while safeguarding privacy and competition. This will allow the payments ecosystem to shift from reactive defence to proactive, intelligence-led prevention.

3

**Develop a Cross-Sector Strategy that extends beyond the payments sector.**
Fraud journeys span multiple industries, from social media to telecoms and online marketplaces. The EU should adopt a cross-sector accountability model that aligns incentives across all actors in the fraud chain. This requires baseline anti-scam controls for digital platforms, cross-sector intelligence hubs, and accountability across the chain with shared liability frameworks that promote collective deterrence and reduce moral hazard.

4

**Adopt a Whole-of-Government and Cross-Border Response.**
Fraud and scams have become an organized crime enterprise, increasingly transnational and sophisticated, requiring a unified and coordinated public response. The EU should treat fraud prevention as a security priority, aligning financial regulation, cybersecurity, and law enforcement under a single strategic framework. Priority actions include enhancing law-enforcement capability and prosecution, empowering Europol with greater operational authority, and deepening international cooperation to pursue joint investigations and disrupt global fraud networks. Stronger public-sector coordination will ensure consistent enforcement and visible accountability for perpetrators.

5

**Empower and Protect Consumers as Active Partners.**
The most sophisticated defences are only as strong as the individuals they protect. As scams increasingly exploit psychology rather than technology, consumers must be treated as active partners in the EU's fraud-prevention ecosystem. The EU should reinforce shared liability frameworks, promote digital literacy, and scam awareness, and strengthen victim support through trauma-informed law-enforcement training and clear referral pathways. Empowered, informed consumers will form the last and most resilient line of defence.

**The time to act is now - before fraudsters evolve further and the gap between regulation and reality widens.**

# Introduction

The introduction of Strong Customer Authentication (SCA) under the EU's second Payment Services Directive (PSD2) framework has had a significant impact on the payments landscape. By mandating two-factor authentication for electronic transactions, SCA has significantly reduced unauthorized payment fraud, setting a new baseline for digital security across the region.

Fraud rates for transactions authenticated with SCA have declined for the period H1 2022 to H1 2023, according to the 2024 EBA/ECB Report on Payment Fraud. Payments within the EEA that were subject to SCA had lower fraud levels compared to transactions exempt from SCA or conducted outside the EEA. (EBA–ECB Report on Payment Fraud, August 2024)

Industry data supports this trend. Following the introduction of SCA, around 33% of institutions surveyed by the Payment Association EU observed a decrease in unauthorized payment volume and 42% in unauthorized payment value.

Yet this early success came with trade-offs. SCA's added layers of security introduced friction into the customer journey, leading to higher rates of transaction declines and cart abandonment. Survey results reveal that about 31% of respondents reported an increase in abandonment rates. More critically, as consumers adjusted to stronger authentication, criminals adapted faster - developing new methods to circumvent or exploit SCA controls. The result is that fraud has not disappeared; it has shifted form.


**Strong Customer Authentication (SCA)** means authentication based on the use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.

European Parliament and Council of the European Union, 2015. Directive (EU) 2015/2366 on payment services in the internal market (PSD2).

Policymakers often cite SCA as a success story - a proof point that robust authentication reduces fraud. While this remains true for unauthorized payments (e.g., where stolen credentials are used to gain unauthorized access to payment accounts or fraudulently initiate payments), focusing solely on this achievement risks obscuring a more complex picture. Fraudsters have evolved, and new forms of crime now exploit SCA's blind spots.

While SCA has reduced unauthorized fraud, it has inadvertently incentivized a shift toward more complex, sophisticated Modus Operandi (MOs), and deception-based scams. Survey results show a broad rise in authorized fraud typologies between 2020 and 2024, marking a clear shift from technical breaches to socially engineered scams. The rise is especially pronounced for scams that exploit human trust, urgency, and emotional manipulation rather than technical vulnerabilities - such as impersonation scams, financial opportunity scams, and emotional or relationship scams.

Criminals now exploit both technical weaknesses in prescriptive SCA mechanisms and human vulnerabilities through social engineering. The prescriptive nature of SCA rules has, in fact, provided fraudsters with a rulebook to study and exploit, enabling them to anticipate and manipulate authentication patterns and exploit predictable weaknesses. This leads to unauthorized fraud, where passwords and one-time codes are compromised to gain illicit access and execute fraudulent transactions. Meanwhile, fraudsters have shifted towards deception-based scams, manipulating human trust to give rise to authorized payment scams, where customers are deceived into willingly initiating fraudulent payments - effectively bypassing SCA through psychological rather than technical means.

To explore these emerging dynamics in greater depth, the Payments Association EU conducted a data collection exercise among its members, encompassing banks, payment service providers, and technology firms across the region. The findings confirm that while SCA has delivered clear gains in reducing unauthorized fraud, fraud typologies have evolved rapidly, with social engineering and credential theft now accounting for a growing share of losses. Members also highlighted rising operational complexity and customer friction, underscoring the need for a more flexible, risk-based approach to authentication and fraud prevention.

As the EU moves forward with the third Payment Services Directive (PSD3) and the new Payment Services Regulation (PSR), it must recognize these evolving dynamics. Simply reinforcing existing SCA requirements - or layering on more static rules - will not stop modern fraud and may exacerbate consumer friction. Instead, the next phase of Europe's fraud prevention framework should focus on modernizing SCA, embedding cybersecurity best practices, and building cross-sector, intelligence-driven collaboration.

# Scope & Methodology

This section outlines the analytical scope, data collection process, and methodological approach underpinning this paper. It explains how insights were derived and how they reflect the perspectives of key players across the EU payments ecosystem.

The analysis draws on an industry-wide survey conducted by the Payments Association EU (PA EU) among nearly 100 members, representing banks, payment service providers, acquirers, merchants, and technology firms. The 66-question survey covered topics including SCA implementation, fraud trends, user experience, regulatory impacts, and forward-looking recommendations.

**Data Collection Process:**
Data collection ran from July to September 2025, followed by analysis in October. All responses were anonymized and aggregated. Only the PA EU team accessed raw data; neither the sponsor (PayPal) nor the consulting partner (Deloitte) had access to identifiable responses, ensuring analytical independence.

## Survey Topics

### Impacts of SCA

- Implimentation methods
- Fraud Evolution
- Customer experience
- SCA-autherticated transactions
- SCA-exempt transactions

### Unauthorized Fraud

- Fraud types
- Fraud trends
- Fraud rankings

### Authorized Fraud

- Main scam types
- Scam trends
- Prevention measures

### Future of SCA

- New authentication technologies
- Extra fraud controls
- Regulatory impact
- Best practices
- Forward-looking recommendations

**Respondent Profile:**
Respondents included regulated entities and merchant-facing providers across the EU, covering all segments of the payments value chain. Their diverse operational exposure ensured a comprehensive view of authentication and fraud challenges across multiple jurisdictions and business models.

Respondents represented multiple EU jurisdictions and operational markets, reflecting the cross-border nature of modern payments. The diversity of the participant base ensured a balanced understanding of both regulatory implementation experiences and market-driven innovations around SCA.

**Analytical Scope:**
Quantitative findings were enriched with qualitative insights from PA EU working groups, expert panels, and interviews. These discussions linked operational experience with the broader policy implications of PSD3 and PSR. A series of non-anonymized interviews with leading industry experts offered practical insights into authentication, fraud prevention, and regulatory compliance. Their contributions are enclosed at the end of this paper.

> The insights gathered through the Payments Association EU's survey and expert consultations paint a clear picture of a fraud landscape in rapid transition. While SCA has strengthened defences against unauthorized transactions, criminals have adapted their tactics - shifting from technical exploitation to psychological manipulation and system circumvention.

> The following sections analyse these emerging patterns in detail. It explores how fraud typologies have diversified since SCA's implementation and outlines how SCA now fits within a wider, multi-layered fraud-prevention framework, paving the way for a more holistic approach in the EU, under PSD3/R, and more broadly across related policy areas.

## Timeline

**July 1, 2025**
Kick-off of initiative

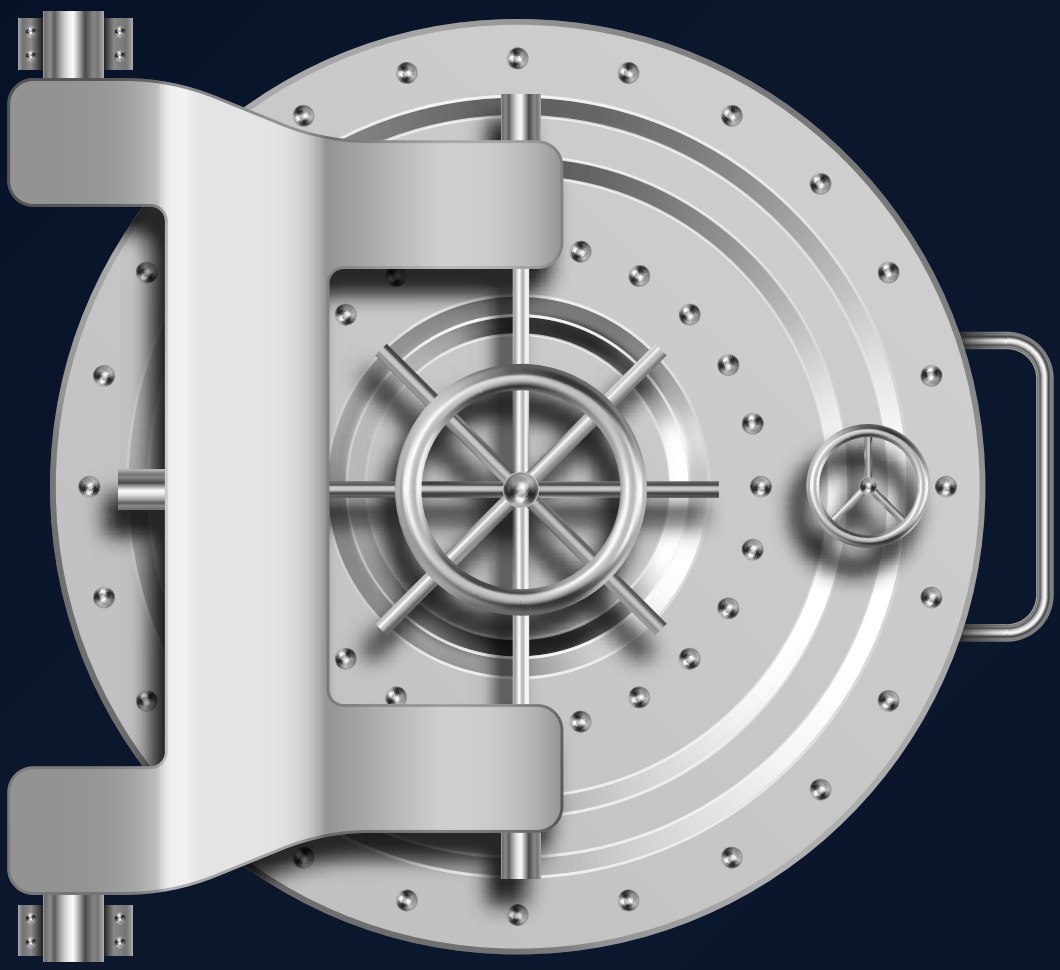
**July 18, 2025**
Survey distributed to stakeholders across the EU payments landscape

**September 30, 2025**
Data collection concluded

**October 1, 2025**
Data analysis and review of findings

**November 1, 2025**
Drafting and design of the paper

**December 11, 2025**
White paper release



Deloitte.

# Shaping the future of SCA

## Key Survey Findings

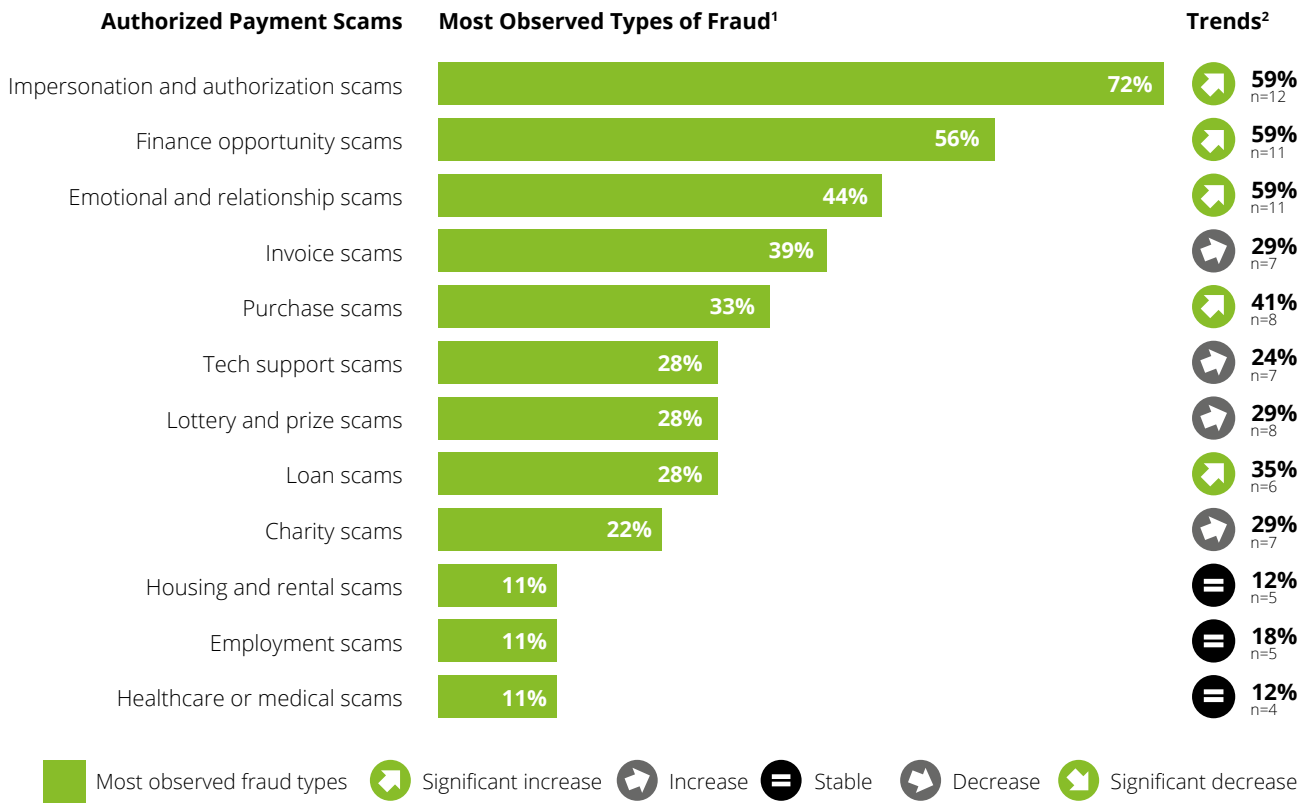
# Overall messages

SCA needs to evolve to address the new types of fraud, improve customer experience and strengthen protection

| Category | Overall Message | Key Points |
|---|---|---|
| OVERALL IMPACT | The introduction of SCA contributed to enhance security and decrease part of fraud | • The volume of unauthorized payment fraud decreased after the introduction of SCA (but new types of fraud emerged)<br>• The volume of authorized payment fraud increased in the past years (and yet some parts are unreported)<br>• Fraudsters are using a vast variety of fraud with new ways to manipulate customers in approving transactions |
| NEW TYPES OF FRAUD | However, new types of fraud emerge with increasingly diverse and more sophisticated methods | • Fraud is becoming increasingly more sophisticated with social engineering and phishing to bypass SCA<br>• New fraud risks are increasing rapidly such as impersonation and authorization scams, financial opportunity scams, etc.<br>• Fraudsters are using new technologies and AI to develop tailored scams at scale exploiting human weaknesses |
| EXPERIENCE IMPACT | SCA negatively impacted customer experience and payment abandonment rate | • SCA-exempted transactions offer a better customer experience<br>• Payment abandonment rate increased since the implementation of SCA |
| CALL FOR ACTION | SCA needs to evolve to address the new types of fraud, improve experience and security | • Security methods need to evolve to remain effective with modern authentication solutions to combat fraud<br>• Current mechanisms in place are not sufficient to protect customers from payment fraud<br>• Actors are using additional tools on top of SCA such as transaction monitoring, fraud scoring and customer education<br>• Fraud occurs upstream in the value chain, so it must be tackled across all sectors, not only at ent stage |
| SUGGESTED CHANGES | SCA should be modernized with biometrics, behavioral and risk-based approach | • In a rapidly evolving fraud landscape, SCA should be dynamic and risk-based considering the context and specific risks<br>• Biometrics and behavioral can be further used for authentication with a combination of other factors<br>• Regulatory framework should support innovative methods allowing to strengthen security<br>• Modern authentication solutions such as passkeys allow to improve both customer experience and security |

# Authorized payment fraud

New types of authorized payment fraud are rising and becoming increasingly more sophisticated

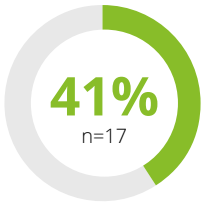



**Key Points**

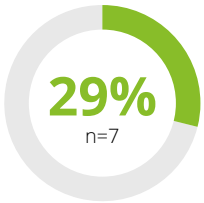
**SCA effectiveness remains limited with numerous fraud**

**New types of fraud are emerging with increasing sophistication**

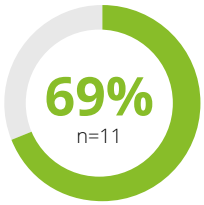
**Changes in SCA should allow to improve experience and protection**



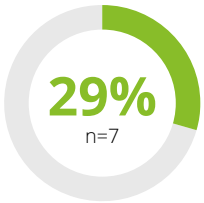

of respondents mentioned that the impact of authorized payment fraud is underestimated across the industry



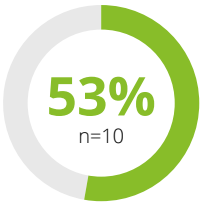

of respondents mentioned a decreased volume of authorized payment fraud since the introduction of SCA




of respondents put in place measures against APP (customer education, notification, verification of payee, manual controls)




of respondents mentioned a decrease in first-party abuse since SCA came into force




of respondents mentioned that current mechanisms in place are not sufficient to protect customers from payment fraud

n= number of respondents, excluding no answers

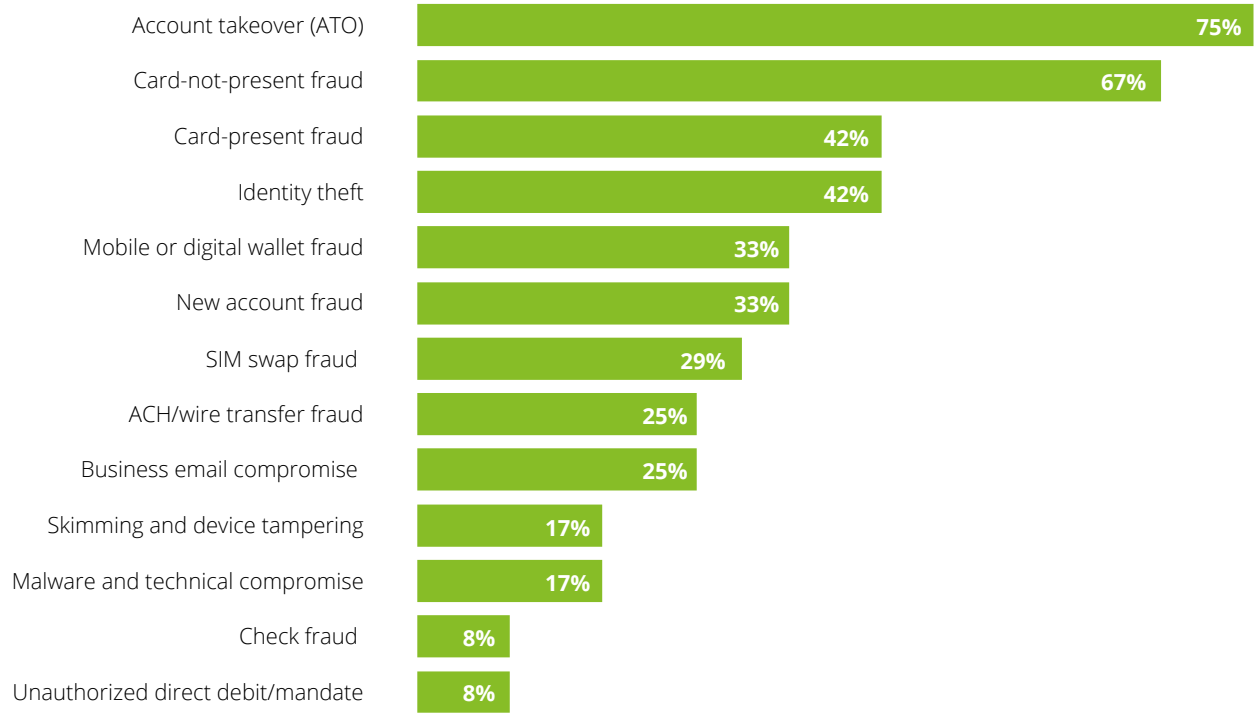
1. Percentage of respondents answering "Yes" to the question "Which types of authorized payment fraud scenarios have you observed?" (n=18, excluding no answers)

2. Percentage of respondent answering "Increase" to the question "Between 2020 and 2024, please indicate whether each scenario type has increased, decreased, or remained the same" (excluding no answers)

# Unauthorized payment fraud

Unauthorized payment fraud decreased after SCA rollout both in terms of volume and value

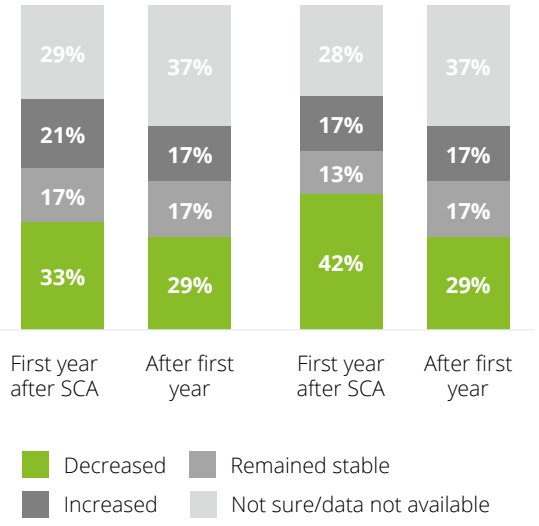
**Unauthorized Payment Scams** — **Most Observed Types of Fraud[1]**




**Key Points**

- **SCA contributed to decrease a part of unauthorized payment fraud**
- **Unauthorized payment fraud decreased after SCA rollout (both in terms of volume and value)**
- **However, the impact remained limited with only 29% of respondents mentioning a decrease after the first year**
- **The fraud rates of SCA transactions is lower than for SCA-exempted transactions**

**Volume of fraud evolution[2]** — **Value of fraud evolution[3]**



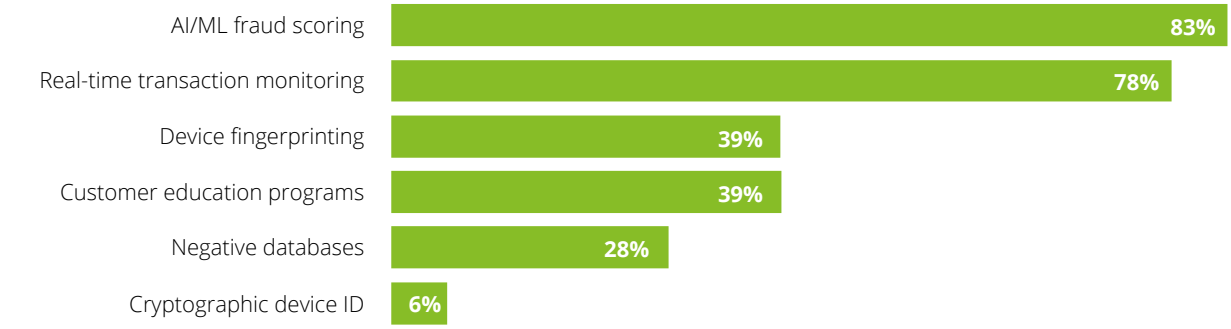

1.Percentage of respondents answering yes to the question "What are the types of unauthorized payment fraud your organization has observed?" (n=24, excluding no answers)
2.Percentage of respondents answering the question: "How did unauthorized fraud volume change in the first year and after the first year of SCA implementation?" (n=24, excluding no answers)
3.Percentage of respondents answering the question: "How did unauthorized fraud value change in the first year and after the first year of SCA implementation?" (n=24, excluding no answers)

# Future of SCA

The future of SCA is shaped by new technologies and regulatory changes

## Additional measures[1]

Actors put in place additional fraud prevention measures on top of SCA




## New authentication technologies[2]

New authentication technologies can be used to improve customer experience and security

### Biometrics and Behavioral

Use more behavioral biometrics with advanced device ID and digital trust

### Risk Based Approach

Combine risk-based authentication and SCA to counteract fraud risk

### Passkey

Allow password-less login (e.g. with passkey standard FIDO2/WebAuthn)

### Digital Identity

Leverage the European digital identity wallet (cf. eIDAS2)

## SUGGESTED REGULATORY CHANGES[3]

Regulatory framework should evolve to allow innovative methods to increase customer protection, experience and security

### PSD3/PSR

- Adjust SCA requirements in PSD3/PSR to strengthen protection

### Customer Protection

- Strengthen customer protection
- Conduct real investigation/prosecution of scammers

### Collaboration and Data Sharing

- Create consortiums for data and knowledge sharing
- Share additional data about payer (incl. device fingerprints)
- Use data to increase efficacy of ML fraud model

### Multi-Factor

- Keep combination of different factors (inherence, possession, knowledge)

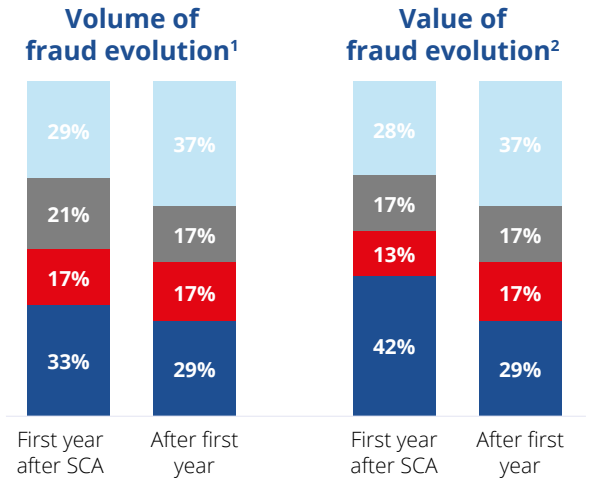
1. Percentage of respondents answering yes to the question "Did you put in place additional fraud prevention measures on top of SCA?" (n=18, excluding no answers)
2. cf. question "Are you considering new authentication technologies (e.g. passwordless login, behavioral biometrics, etc.)? If yes, can you elaborate?"
3. cf. question "What regulatory changes or additions would you suggest to strengthen fraud protection frameworks?"

CHAPTER 1

# The Evolving Fraud Landscape Under SCA

## Initial Impact: A Short-Term Win Against Unauthorized Fraud

The full enforcement of SCA produced clear and immediate results. Many payment providers reported a reduction in unauthorized payment fraud: 33% of surveyed institutions saw a decline in the volume of unauthorized payments, while 42% observed a decrease in value.




1.Percentage of respondents answering the question: "How did unauthorized fraud volume change in the first year and after the first year of SCA implementation?" (n=24, excluding no answers)

2.Percentage of respondents answering the question: "How did unauthorized fraud value change in the first year and after the first year of SCA implementation?" (n=24, excluding no answers)

However, these gains soon plateaued as fraudsters adapted, targeting areas outside the scope of SCA or exploiting weaknesses in its implementation. 34% of survey respondents saw either stable or increases in both value and volume in subsequent years, while only 29% of respondents mention a decrease after the first year.

This trend extends beyond the EU. According to UK Finance's 2025 Annual Fraud Report, unauthorized fraud losses rose to £722 million, while confirmed cases increased by 14%, reaching approximately 3.13 million in 2024. (UK Finance, Annual Fraud Report 2025, June 2025).

> Collectively, these findings highlight a maturing threat environment in which initial security gains have given way to new and more complex forms of attack. Insights from the PA Europe survey point to several defining shifts in the post-SCA fraud landscape.

## When Security Depends on the Customer: Concentration Risks in SCA

While SCA has reduced unauthorized fraud, it has also concentrated authentication practices around the customer - creating new vulnerabilities. Fraudsters have shifted their focus toward schemes that exploit customers directly, aiming to harvest credentials such as passwords or one-time passcodes (OTPs).

Survey results show that phishable authentication dominate the European market: 70% of respondents reported offering password + SMS OTP combinations, while PIN and passwords are used across 4 of the 6 combinations surveyed.

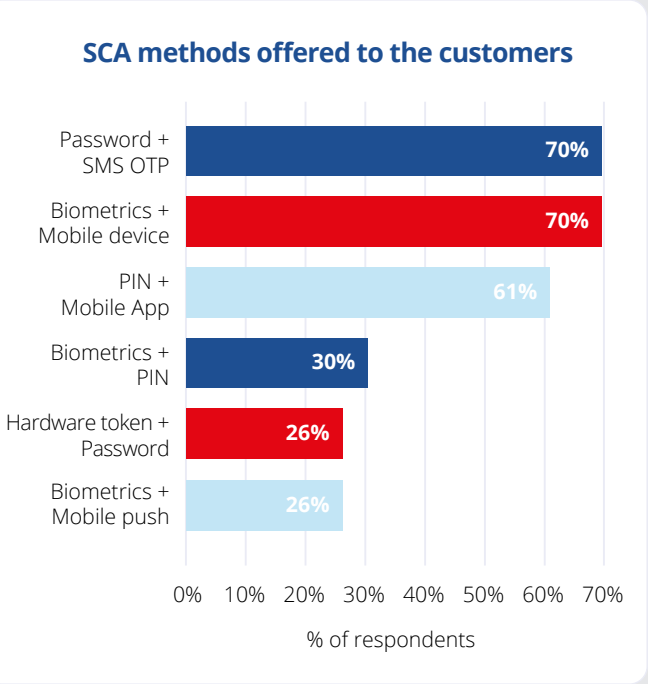
**"The implementation of SCA has significantly strengthened security while keeping customer experience within acceptable parameters, despite some added friction. This achievement marks an important milestone in our journey. However, to progress toward more sophisticated and innovative approaches, it is essential to consolidate processes and establish a solid foundation that supports future transformation, ensuring both protection and convenience for our customers."**

João Leote | Manager | Digital Transformation, Operations & Business Efficiency
**Banco BPI**

These approaches share a critical weakness - they rely on active user input that can be phished or socially engineered, such as typing passwords or one-time-codes. As a result, fraudsters increasingly deploy social engineering and deception tactics to trick users into revealing their credentials, bypassing the strongest technical barriers.

The survey also shows that 70% of respondents offer SCA combinations using biometrics and mobile-based possession factors, highlighting the growth of alternative, data-driven methods to secure transactions. These approaches have the benefit of being more resistant to phishing attacks.

When looking at whether these SCA methods were used heavily or only occasionally, the survey reveals similar trends. A significant 83% of respondents indicated that the password + SMS OTP combination was occasionally to heavily used by their customers, mirroring the uptake of biometric authentication combined with a mobile device–based possession factor. PIN-based methods also remain prevalent, with 70% of respondents reporting frequent use of PIN + mobile app combinations, and 48% indicating the use of PIN + biometric authentication.



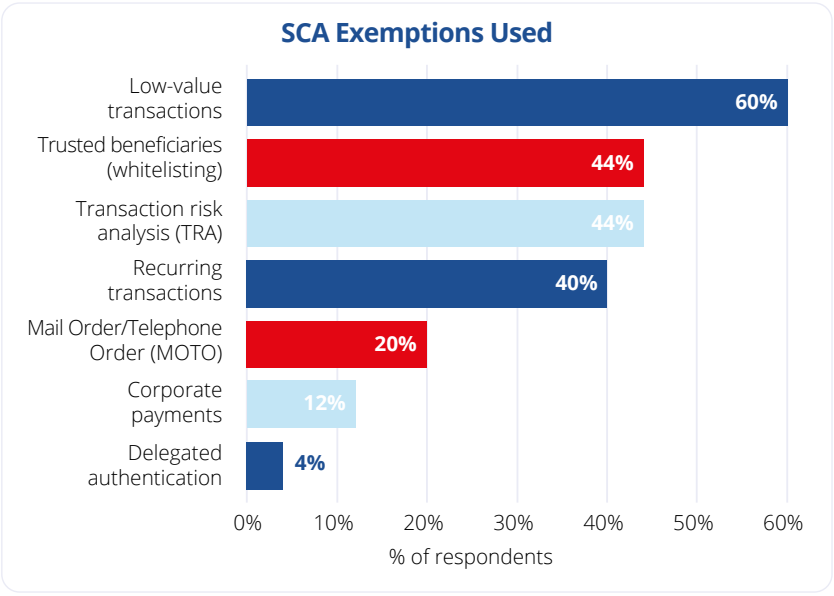

## SCA's Impact on the Customer Experience

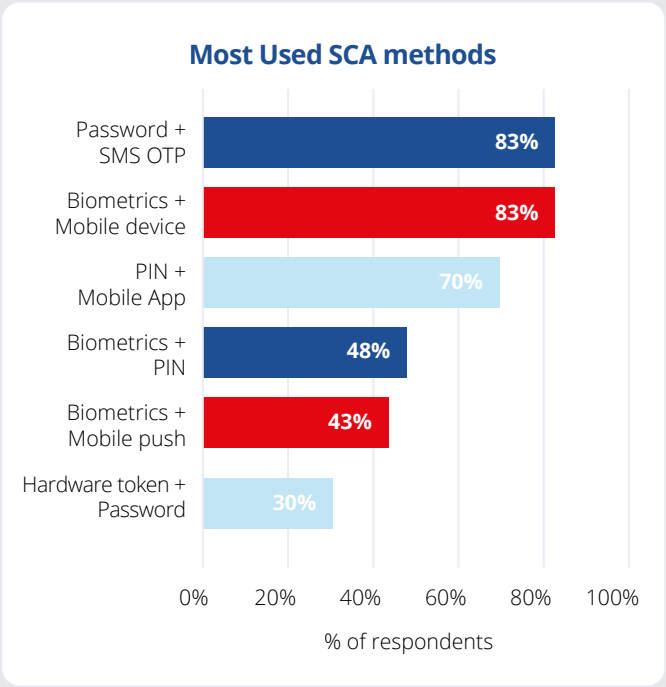
The introduction of SCA has reshaped the customer experience across digital payments, balancing stronger security with varying levels of friction. Survey results show that SCA exemptions have been key to preserving convenience and reducing authentication fatigue, particularly where risk-based strategies are applied effectively.

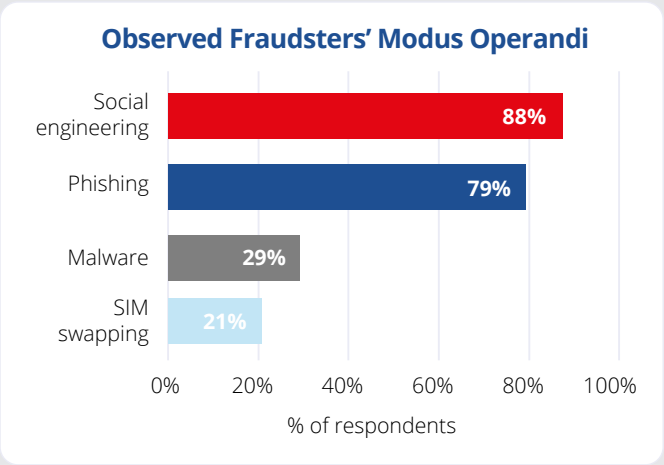
- 36% of respondents reported that exempted transactions offer a significantly better customer experience, with another 12% noting a slight improvement.
- The low-value exemption is the most widely applied (by 60% of respondents), reflecting its practicality for every day, low-risk payments.
- Trusted beneficiaries (used by 44% of respondents) and transaction risk analysis (TRA) (deployed by 44% of respondents) are increasingly used, signalling a shift toward more dynamic, intelligence-based authentication.
- 40% of respondents apply exemptions for recurring payments such as subscriptions and utility bills, highlighting efforts to maintain convenience for routine transactions.

However, data also suggests that fraudsters are increasingly targeting static exemptions, where controls are predictable or insufficiently adaptive, resulting in higher fraud rates compared with fully authenticated transactions.

This reinforces that the impact of SCA on user experience and security depends on how exemptions are defined and implemented: when controls are dynamic and data-driven, they enhance usability without exposing new vulnerabilities; when they remain rigid, friction may decrease but risk rises. Across the industry, consensus is emerging that adaptive, risk-based authentication flows are the most effective way to achieve both security and simplicity.





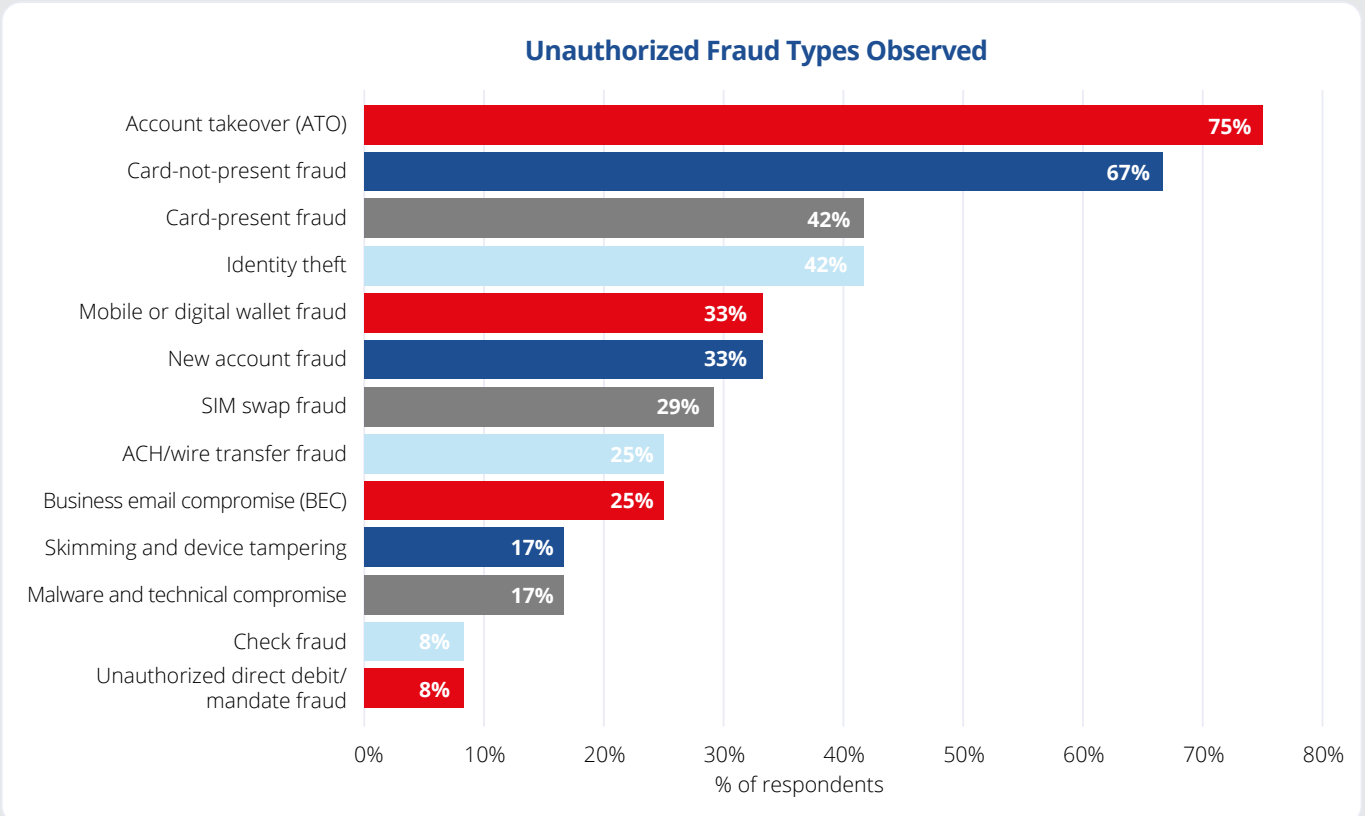




## Persistence of Credential Theft and Account Takeover

Despite widespread SCA adoption, credential theft remains pervasive. Fraudsters continue to exploit human vulnerabilities rather than technical flaws. Social engineering and phishing are the most common techniques for bypassing SCA controls, cited by 87.5% and 79.2% of respondents, respectively.

By contrast, more technical approaches such as malware (29.2%) and SIM swapping (20.8%) are less frequently reported - cybersecurity intelligence suggests that both are becoming more sophisticated and harder to detect. SIM swap attacks, for instance, enable criminals to redirect OTP to their own mobile phone, while malware can extract authentication tokens in real time.

The effects of these tactics are evident in downstream fraud trends. Account Takeover (ATO) and Card-Not-Present (CNP) fraud remain the most prevalent, reported by 75% and 67% of respondents. Other significant categories include identity theft and card-present fraud (reported by 42% of respondents), as well as mobile wallet and new account fraud (33%). Even multi-factor-protected channels are proving susceptible.

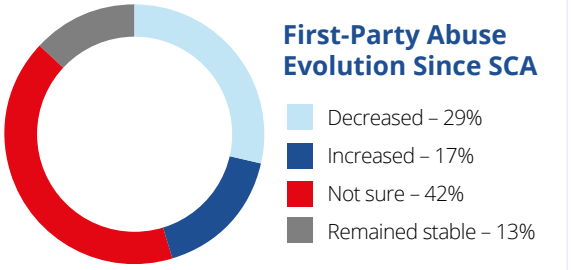


Over half (53%) of respondents believe current SCA mechanisms are insufficient to fully protect users, citing persistent exploitation of technical and procedural gaps. This sentiment reflects a broader shift toward fewer but more sophisticated attacks, with higher-value losses per incident - signalling the evolution from opportunistic fraud to targeted, high-impact intrusions.

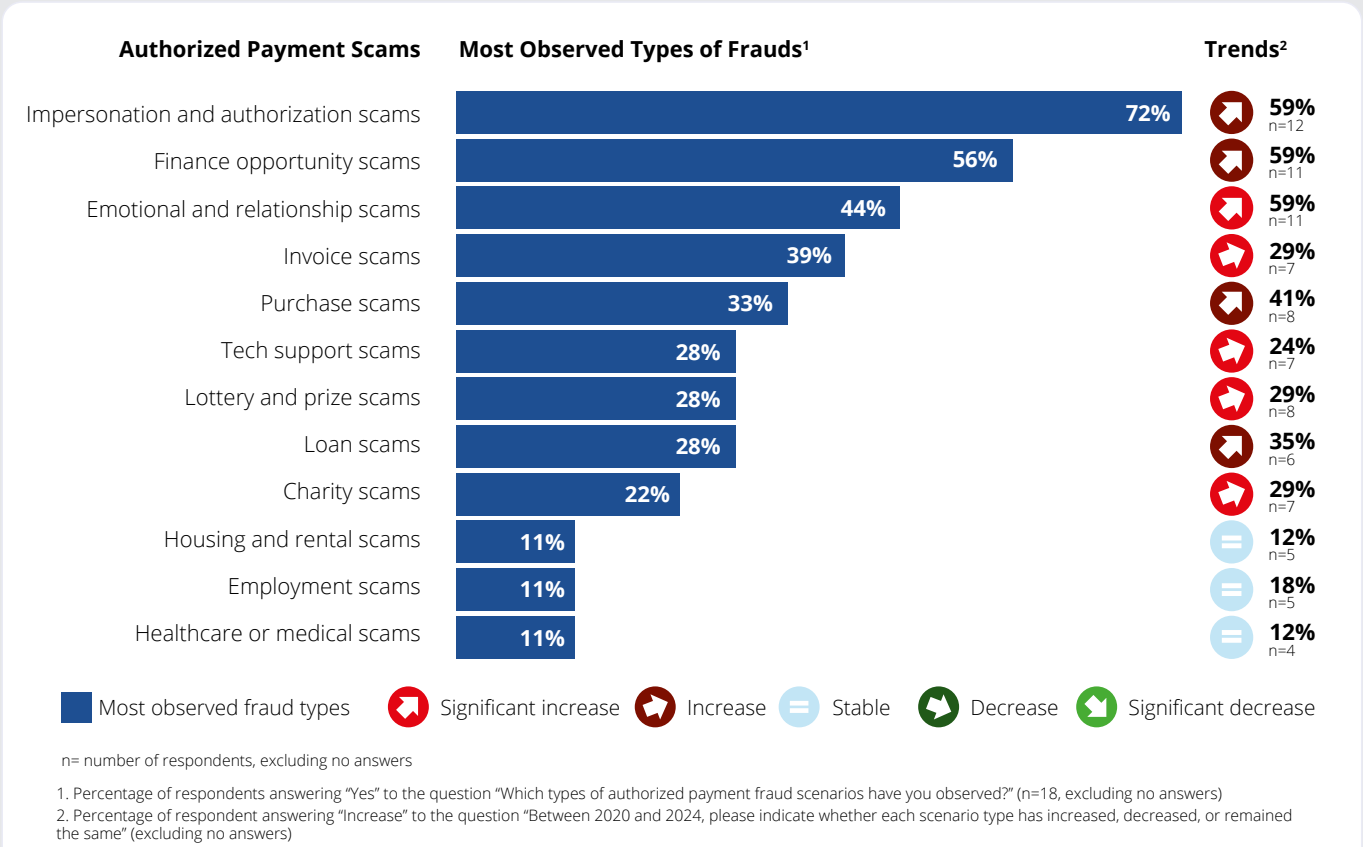
## Understanding First-Party Abuse

First-party abuse refers to cases where a legitimate customer intentionally misuses their own account or payment credentials to commit fraud against a business or institution - for example, by making purchases with no intent to pay, falsely disputing legitimate transactions ("friendly fraud"), or exploiting refund and chargeback processes for personal gain. This can also include collusion cases, where the consumer and merchant are working together to commit fraud against the payment provider. Unlike external attacks, these incidents originate from the account holder, making them difficult to detect, classify, and prosecute.

While SCA has proven effective in reducing unauthorized fraud, its impact on first party fraud is less clear-cut. Among surveyed institutions, 29% reported a decrease in first-party abuse since SCA implementation, suggesting that stronger authentication and monitoring may have deterred some opportunistic misuse. However, 16.7% observed an increase, and the largest share (41.7%) were unsure, highlighting the industry's ongoing challenge in identifying and attributing such cases.




Because first-party abuse involves legitimate credentials and authorized transactions, it often falls into a regulatory grey area between consumer protection and fraud prevention. As authentication strengthens, behavioural analytics, data sharing, and clearer liability standards will be essential to help PSPs and regulators distinguish genuine victims from deliberate misuse - ensuring that fraud prevention frameworks remain both fair and effective.




n= number of respondents, excluding no answers

1. Percentage of respondents answering "Yes" to the question "Which types of authorized payment fraud scenarios have you observed?" (n=18, excluding no answers)
2. Percentage of respondent answering "Increase" to the question "Between 2020 and 2024, please indicate whether each scenario type has increased, decreased, or remained the same" (excluding no answers)

## Surge in Social Engineering and Authorized Fraud

Criminals increasingly recognize that deceiving a human is easier than defeating an algorithm. The result has been an explosion in authorized payment fraud - including impersonation, investment, and romance scams. 59% of respondents reported increases in these scam types since 2020, with many noting that transactions pass SCA successfully because they are initiated by genuine customers.

As a result, authorized payment fraud falls outside traditional SCA safeguards. 41% of respondents believe the impact of authorized fraud is underestimated across the industry, underscoring the need for new frameworks that address the behavioural and psychological dimensions of financial crime.

## Technology-Enabled Fraud in a Connected Ecosystem

The rapid evolution of digital technologies and artificial intelligence (AI) is reshaping the fraud landscape. While AI itself is not malicious, it is increasingly weaponized by organized criminal groups to automate, scale, and personalize attacks. AI-driven tools can mimic legitimate user behaviour, craft highly convincing communications, and generate synthetic identities and deepfakes, blurring the line between genuine and fraudulent interactions.

Modern fraud networks operate with industrial efficiency, combining automation, large-scale data breaches, and AI-powered analytics. Bots conduct credential-stuffing and brute-force attacks, while generative AI systems produce linguistically tailored phishing campaigns that exploit psychological and behavioural cues to deceive consumers and institutions alike.

At the same time, fraud is no longer confined to the financial sector. It now thrives across a digitally connected ecosystem spanning social media platforms, online marketplaces, telecom providers, and messaging apps. Criminals exploit these channels to manipulate consumers long before payment occurs, fusing social engineering with technical intrusion - for example, harvesting credentials through phishing and then deploying remote-access malware or session hijacking tools to complete fraudulent transactions in real time.

This convergence of technology, automation, and human manipulation marks a decisive shift toward adaptive, intelligence-driven fraud, against which static controls are increasingly ineffective. Fraud in the post-SCA era has become a complex, human-centric challenge: while traditional unauthorized fraud has declined, social engineering, AI-driven deception, and organized crime networks have created a more diffuse and resilient threat environment. Addressing this evolution requires a new generation of fraud prevention - one built on intelligence, adaptability, and cross-sector coordination, capable of responding to both technological innovation and the psychological dimensions of modern crime.

CHAPTER 2

# Beyond SCA: Building a Multi-Layered Fraud Prevention Framework

SCA remains a cornerstone of payment security, but it represents only one layer in a broader defence strategy. Leading payment service providers recognize that no single control can fully prevent modern fraud. A multi-layered, risk-based approach - combining advanced technology, analytics, and enhanced consumer awareness - is now standard practice across the payments ecosystem.

Survey findings from the Payments Association EU highlight this evolution: 70% of respondents reported deploying additional fraud prevention measures beyond SCA and traditional static controls – such as AI-powered transaction monitoring, device fingerprinting, and customer awareness initiatives. Respondents are also actively exploring next-generation authentication technologies designed to enhance security while maintaining a seamless customer experience.

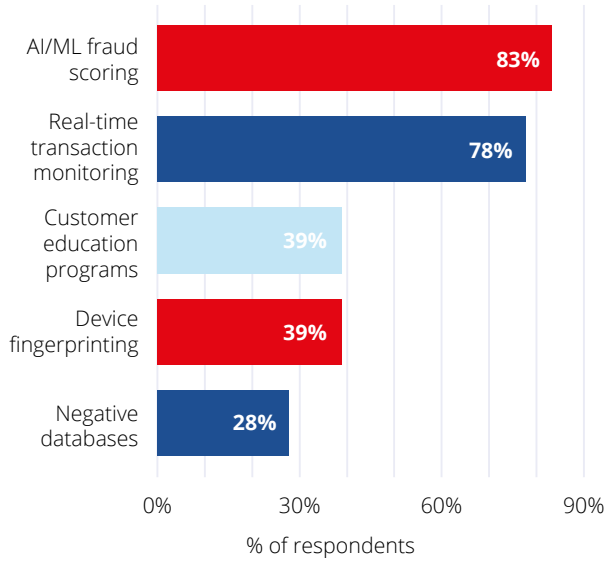
## Measures Beyond SCA: Continuous and Intelligence-Led Defence

### AI powered Transaction Risk Monitoring

AI has become central to modern fraud prevention. According to Survey results, 83% of respondents use AI or machine learning (ML)–based fraud scoring, and 78% deploy real-time transaction monitoring as part of their fraud defence strategies.

Transaction monitoring has become a foundational control across the payments ecosystem. PSPs now assess each transaction - and increasingly, each customer interaction - in real time using advanced AI/ML models that analyse hundreds of dynamic attributes, including geolocation data, behavioural patterns, device identifiers, and historical fraud indicators. This fusion of transactional and behavioural analytics enables systems to detect not only suspicious payments but also unusual user behaviour that may signal emerging threats. When anomalies are detected, systems can respond instantly by flagging, holding, or declining transactions, or by triggering additional authentication steps.

Adaptive AI/ML models continuously refine their understanding of evolving risk patterns, identifying typologies such as AI-driven attacks, synthetic identity fraud, and behavioural manipulation. Together, transaction and behavioural analytics form the intelligence backbone of modern fraud detection - delivering continuous, adaptive protection that evolves as fast as the threats themselves.




### New authentication technologies

New authentication technologies can be used to improve customer experience and security

**Biometrics and Behavioral**
Use more behavioral biometrics with advanced device ID and digital trust

**Risk Based Approach**
Combine risk-based authentication and SCA to counteract fraud risk

**Passkey**
Allow password-less login (e.g. with passkey standard FIDO2/WebAuthn)

**Digital Identity**
Leverage the European digital identity wallet (cf. eIDAS2)

> **Worldline provides a multi-layered, AI-driven fraud prevention solution that brings together technology, data, and authentication under one roof. This includes AI-driven analytics and hybrid detection, combining rules with machine learning to analyze billions of transactions and detect anomalies instantly; as well as Risk-based authentication, Device and behavioral intelligence, and Cross-channel fraud visibility. The impact is measurable and proven: AI-driven fraud detection improvements deliver up to a 30% uplift, 50M+ yearly transactions secured, and 3× fewer false positives than the industry average."**
>
> Colombe Hérault | Authentication & Identification Portfolio Business Manager
> João Courinha | Senior Global Product Manager
> **Worldline**

## Device Fingerprinting and Cryptographic Device Identifiers

Device intelligence is emerging as a complementary layer to AI-based monitoring. By uniquely identifying and binding transactions to trusted devices, PSPs can significantly reduce impersonation and account takeover risks.

According to the PA Europe Survey (Summer 2025), 39% of respondents use device fingerprinting, while 6% have implemented cryptographic device identifiers.

- Device fingerprinting builds a unique, privacy-preserving profile based on multiple attributes - such as browser configuration, operating system, and network metadata - helping detect anomalies such as logins from manipulated or unfamiliar devices.
- Cryptographic device identifiers (or secure device binding) go a step further by using hardware-backed cryptographic keys to authenticate transactions. Each transaction is cryptographically signed by a trusted device, ensuring it cannot be replicated or intercepted.

When combined with AI-driven monitoring and behavioural signals - supported by liveness detection and spoof-resistance - device intelligence enables continuous, context-aware risk monitoring that protects against fraud well beyond static, one-time checks.

## Customer Education and Real-Time Alerts

Technology alone cannot stop fraud and scams; consumer awareness at the point of risk remains essential. According to the PA Europe Survey, 39% of respondents have implemented customer-awareness initiatives as part of their fraud-prevention strategies.

Leveraging AI/ML technologies, many PSPs now integrate real-time, just-in-time scam warnings within the payment flow, alerting users to potential deception when initiating high-risk transfers or interacting with unfamiliar payees. For example, PayPal's AI-powered scam alert system leverages its risk-monitoring capabilities to issue contextual, non-disruptive warnings, helping customers recognize suspicious activity before confirming a transaction.

While education alone cannot eliminate scams, it strengthens the first line of defence - the customer. Proactive, contextual communication empowers users to make safer choices and reduces vulnerability to authorized payment fraud, where manipulation rather than system compromise is the primary threat.

Beyond immediate alerts, ongoing education and awareness programs build long-term resilience. In-app prompts, public campaigns, and continuous communication help customers recognize evolving threats - from impersonation to deepfake-enabled deception - and identify red flags early. A more informed and vigilant customer not only reduces individual losses but also strengthens trust and integrity across the payments ecosystem.

> **Scams increasingly rely on impersonation tactics, with fraudsters posing as trusted organizations such as banks, government bodies, or well-known service providers. This evolution calls for new, more adaptive detection and prevention strategies, including behavioral analytics, real-time risk assessment, customer education, and closer collaboration across the financial ecosystem to effectively combat these emerging threats."**
>
> Georgios Tangilis | Fraud Lead
> **payabl.**

## Next-Generation Authentication: Evolving SCA Itself

As fraudsters evolve, so too must authentication. The same technologies that underpin advanced fraud prevention - AI, device intelligence, and behavioural analytics - are now driving the next generation of authentication technologies.

Future authentication methods will be phishing-resistant by design, leveraging biometric and behavioural signals alongside cryptographic device binding to deliver both enhanced security and a frictionless user experience.

### Behavioural Biometrics and Continuous Authentication

Behavioural biometrics, once primarily used for fraud detection, are maturing into a critical contextual risk signal within next-generation authentication frameworks. These technologies authenticate users based on unique behavioural signatures (such as typing cadence, mouse movement, device handling, or gesture dynamics) that are extremely difficult to replicate or steal.

When combined with other authentication factors, behavioural biometrics provide continuous, passive validation of user legitimacy throughout a session. Unlike static passwords or one-time codes, they offer persistent, invisible security that strengthens authentication while maintaining a frictionless user experience.

In parallel, PSPs are increasingly implementing continuous authentication - systems that operate invisibly in the background to monitor user interactions in real time. This enables adaptive, context-aware validation without interrupting legitimate activity. When integrated with AI-driven anomaly detection, these capabilities provide a powerful second line of defence against both account takeover and authorized payment fraud.

### Flexible, Risk-Based Authentication Flows

Modern fraud defence increasingly relies on risk-based authentication - dynamically adjusting the strength of controls according to assessed transaction risk. RBA allows PSPs to tailor authentication in proportion to the likelihood of fraud, achieving both robust protection and a frictionless user experience. When high-risk indicators emerge - such as anomalies in device behaviour, location, or transaction patterns - systems can instantly trigger stronger measures to ensure security.

This proportionality principle - calibrating authentication to the level of risk - ensures that defences remain effective while preserving a smooth user experience. It also supports a more sustainable fraud management model by focusing resources where they have the greatest impact.

> **"This risk-based approach centers on device cryptographic proof as the foundation of authentication. Public–private key pairs are permanently embedded in user devices, serving as a possession factor, similar to how car keys authenticate ownership of an expensive car. Geographical location changes are acceptable when the device itself can be proven legitimate. A high-risk situation might arise when multiple risk signals occur together, for example, a new location, a new device, and a new merchant, triggering the question: "Why would these three things happen simultaneously?"**
>
> Gerhard Oosthuizen | Chief Technology Officer
> **Entersekt**

By integrating real-time analytics, behavioural biometrics, and contextual device intelligence, PSPs can deliver adaptive authentication journeys that evolve alongside threat landscapes.

### Digital Identity

The evolution of authentication is closely linked to the rise of digital identity frameworks such as the European Digital Identity (EUDI) Wallet. Integrating verified digital identities into payment authentication can deliver stronger security and seamless payment experiences.

This convergence streamlines KYC and AML processes by enabling reusable identity verification, reducing the need for customers to repeatedly prove their identity across institutions. The EUDI Wallet's privacy-preserving design allows individuals to selectively disclose only the attributes required for a transaction (such as age) without exposing full identity documents. This selective disclosure aligns with Europe's data protection principles while enabling seamless cross-border payments and strengthening fraud prevention through trusted, interoperable credentials.

By combining digital identity with next-generation authentication, the EU can establish a unified trust framework that enhances security, usability, and confidence across the digital payments ecosystem.

## Phishing-resistant authentication

Phishing-resistant authentication is a security method that binds authentication credentials to a specific legitimate website domain or mobile app, making it impossible for attackers to use them on fake sites.

Unlike passwords or OTPs that work anywhere they're entered or used, phishing-resistant methods:

- Verify site or app authenticity before authenticating - stopping attacks at the source
- Fail automatically if the user lands on a fake or spoofed site
- Cannot be replayed or reused by attackers - no shared secrets exposed
- Remove human error - users no longer need to detect phishing attempts themselves

The importance of phishing-resistant authentication is reflected in recent cybersecurity guidance across Europe. The ENISA Technical Implementation Guidance issued under the NIS2 Directive explicitly recommends the use of phishing-resistant multi-factor authentication (MFA), with FIDO passkeys recognized as a strong form of MFA. Similarly, the German Cybersecurity Centre (BSI) and the Dutch National Cyber Security Centre (NCSC) both advocate the use of passkeys and other secure, passwordless authentication methods to strengthen resilience against phishing and credential theft.

## Phishing-Resistant Authentication

Phishing-resistant authentication represents a fundamental shift in how authentication is performed - moving from credentials that can be stolen or intercepted to cryptographic proofs that cannot. Unlike traditional methods where users transmit secrets (passwords, SMS OTPs) that attackers can intercept, phishing-resistant systems bind cryptographic keys to specific websites or mobile applications. This origin binding means a credential created for one domain (e.g. paypal.com) simply cannot be used on a fake domain that mimics the original (e.g. paypa1.com) - the authentication ceremony will not proceed, regardless of how convincing the fake site appears.

Passkeys (FIDO2/WebAuthn) exemplify this approach. When a user authenticates, the browser or operating system verifies the site's domain before the credential can be invoked - meaning a phishing page cannot trigger authentication even if the user is deceived. Based on asymmetric cryptography with private keys stored in secure hardware and unlocked through biometrics (e.g., fingerprint or facial recognition), passkeys inherently combine two factors - possession and inherence. When passkeys are synchronized across a user's trusted devices, end-to-end encryption ensures that only the user's devices can decrypt the private keys, making passkeys tamper-proof, confidential, and resistant to unauthorized access.

Crucially, phishing-resistant authentication also reduces cognitive load on customers by removing the need to remember passwords or interpret complex login prompts. This simplicity enhances security awareness - customers are better able to recognize genuine warnings and are less vulnerable to authorized payment fraud, where deception rather than technology is the attack vector.

CHAPTER 3

# Rethinking Regulation: Toward a Future-Proof and Holistic Approach

The PSD3 and PSR package offers policymakers a pivotal opportunity to modernize authentication, strengthen cross-sector collaboration, and align incentives to protect consumers without stifling innovation or competitiveness. Yet this alone is not enough: action beyond payments is essential, requiring a cross-sector, whole-of-government strategy that unites all stakeholders, including consumers, behind a shared goal of reducing fraud.

Drawing on insights from the Payments Association EU survey and member engagement, this paper proposes five key policy recommendations to strengthen Europe's fight against fraud.

## 1. Future-Proof the Approach to SCA

Since its introduction, SCA has delivered measurable improvements in payment security. However, the framework now risks stagnation if regulation continues to anchor the industry to outdated tools such as passwords and SMS one-time passcodes (OTPs). As this paper has shown, these methods have become increasingly vulnerable to phishing, SIM swapping, and credential theft, while fraudsters evolve faster than compliance cycles can adapt.

To remain effective, SCA must evolve in step with the threat landscape, embracing innovation, adaptability, and continuous improvement. Policymakers and regulators should move beyond static, prescriptive requirements toward adaptive, risk-based, outcome-driven, and technology-neutral frameworks. This would empower PSPs to deploy phishing-resistant methods - such as passkeys - in combination with contextual, AI-driven risk assessments.

The future of SCA lies in creating a dynamic, principles-based framework that balances innovation, accountability, and regulatory clarity. The goal under PSD3/R is not only to preserve the security gains achieved under PSD2 but also to future-proof authentication against the accelerating pace of technological change.

> **"The survey clearly shows that Strong Customer Authentication (SCA) has significantly enhanced payment security and reduced unauthorized fraud. However, this progress has also resulted in an increase in authorized payment fraud and the emergence of more sophisticated threats, such as impersonation and AI-based scams. It is evident that malicious actors are always one step ahead of those attempting to prevent, detect, and deter fraud or related crimes, and this challenge will persist. Our future success relies on the creativity of the good guys, their ability to collaborate—including between public-public, public-private, and private-private sectors—and the deployment of appropriate tools. These may include innovative analytics techniques, training, new technical solutions, and a variety of other approaches. There is no single 'cure-all' solution; only a combination of methods can offer some remedies."**
>
> Indrek Tibar | Head of AML
> **Wallester**

**Key Recommendations for the PSD3/R and the subsequent Regulatory Standards on SCA developed by the European Banking Authority (EBA):**

- **Balance Security, Convenience, and Competitiveness.** Fraud prevention must coexist with accessibility and ease of use. Overly complex authentication undermines adoption and trust. The PSR should pursue dual objectives - reducing fraud while enhancing usability - to strengthen consumer confidence and support EU competitiveness.

- **Prioritize Authentication Strength and Phishing Resistance.** SCA requirements should assess the effectiveness of the overall authentication process rather than the category of factors used. Cryptographic authentication bound to specific origins - such as passkeys -provides stronger assurance than knowledge-based credentials by preventing credential theft by design. Therefore, phishing-resistant methods should be promoted as a core EU principle.
- **Align Authentication Rules with State-of-the-Art Cybersecurity Practices.** SCA requirements must evolve in line with modern cybersecurity guidance across Europe. Recent ENISA recommendations explicitly prioritize phishing-resistant multi-factor authentication, embedding these standards into the EU payments framework will strengthen resilience against phishing, credential theft, and emerging attack vectors, while ensuring consistency with the broader European cybersecurity agenda.
- **Advance Risk-Based, Intelligence-Led Authentication.** The PSR should recognize AI and machine learning as enablers of adaptive, real-time fraud prevention. Static, rules-based controls must evolve into dynamic frameworks that respond to live risk signals. To strengthen resilience, static measures that can be learned and manipulated by fraudsters over time should be complemented with dynamic risk-sensitive controls that adapt their detection models to counter emerging attack patterns.
- **Harmonize and Enhance Risk-Based Exemptions.** Ensure consistent, risk-based application of exemptions such as Transaction Risk Analysis (TRA), Trusted Beneficiary, and Delegated Authentication across Member States. Continued use and refinement of these exemptions will enable proportionate, intelligence-led risk management and ensure parity between card and non-card payment methods.
- **Foster Outcome-Based, Technology-Neutral, Regulation.** Governance should emphasize accountability and performance rather than prescribing tools. The PSR and EBA standards should remain technology-neutral - avoiding rigid, static, mandates - and instead, focus on transparency, measurable outcomes, and continuous improvement through supervisory oversight.

> By embedding these principles, the PSD3/R can modernize the approach to SCA, moving beyond a "one-size-fits-all" model toward a flexible, contextual, and intelligence-driven framework. Empowering firms to innovate - and holding them accountable for secure, adaptive authentication - will ensure Europe's payments ecosystem remains secure, proportionate, and globally competitive in the era of AI-enabled threats and generative fraud.

> Yet even the most advanced authentication cannot, by itself, address the broader ecosystem risks that drive today's fraud. A coordinated intelligence-sharing model is the necessary next step.

## 2. Beyond SCA: Build a Layered Fraud Intelligence Ecosystem

Authentication is critical, but SCA alone cannot address the full spectrum of modern fraud. Today's attacks increasingly rely on social engineering, impersonation, and deception - exploiting human trust rather than technical weaknesses. To achieve true ecosystem resilience, the EU must enable, through PSD3/R and through further initiatives, a layered, intelligence-led defence that brings together banks, fintechs, payment service providers, and merchants under a unified framework for real-time data sharing and collaboration.

A structured, privacy-preserving fraud intelligence ecosystem would significantly strengthen the EU's collective ability to detect and prevent emerging fraud typologies before losses occur. Coordinated intelligence-sharing - rather than isolated institutional responses - allows threats to be identified and disrupted earlier in the fraud chain. This collaborative approach transforms fraud prevention from a series of individual defences into a connected, proactive network.

### Key Recommendations:

- **Enable Secure and Interoperable Data Sharing Across the Fraud Ecosystem.** Facilitate proportionate, privacy-compliant data sharing between PSPs, merchants, banks and fintechs through a clear legal framework. Shared access to key transactional and behavioural insights would improve collective fraud detection, enhance risk models, and enable earlier identification of threats while maintaining strong privacy and competition safeguards.
- **Establish Financial-Sector Data Hubs for Real-Time Fraud Collaboration.** Create trusted, real-time data-sharing hubs to connect banks, PSPs, fintechs, and merchants. These hubs should enable continuous exchange of transaction-level intelligence and behavioural indicators to detect emerging fraud typologies early and coordinate swift responses. Operated under clear governance and supervisory oversight, they would serve as the operational backbone for collective defence within the financial sector while ensuring full compliance with EU data-protection and competition rules.
- **Strengthen Cross-Border Intelligence Sharing and Coordination.** Enable seamless exchange of verified fraud intelligence across Member States, by strengthening Europol's leading role in aggregating, analysing, and distributing cross-border threat information. This framework should facilitate real-time collaboration between national authorities and financial institutions. Introducing safe-harbour provisions would allow institutions to share threat indicators responsibly and confidently, balancing data protection with collective security. A coordinated EU-wide approach - anchored by Europol's operational and analytical capabilities - will ensure that cross-border fraud threats are identified and contained before they escalate.

By enabling secure data flows across merchants, payment providers, and public authorities, the EU can move from fragmented, reactive defences toward a connected, intelligence-led model of fraud prevention. Enhanced collaboration will allow threats to be detected earlier, countermeasures to be deployed faster, and organized networks to be disrupted more effectively - reinforcing consumer protection and strengthening the resilience of Europe's digital payments ecosystem.

This section focused on strengthening intelligence exchange within the payments ecosystem - among banks, PSPs, fintechs, and merchants - as the foundation for broader cross-sector collaboration. Building on this foundation, the next priority is to extend coordination beyond payments to all sectors involved in the scam lifecycle.

## 3. Beyond Payments: The Need for a Cross-Sector Fraud Strategy

Fraud journeys today often begin long before any payment takes place - on social media platforms, search engines, telecom networks, or online marketplaces - and conclude only when the victim initiates a transfer within the financial system. A holistic model of intelligence sharing is therefore essential to close these gaps, connecting data across the entire digital ecosystem while upholding strict privacy and competition safeguards. Combating these complex, cross-channel, threats requires a coordinated, ecosystem-wide strategy that brings all relevant sectors into a shared framework of accountability.

Fraud prevention will only succeed if incentives are aligned across the entire ecosystem. Current reimbursement schemes may protect consumers in the short term but risk sustaining criminal incentives by making scams profitable. A one-sided approach that places the full burden on payment providers creates moral hazard and fails to address the root causes of fraud.

The EU Commission should therefore adopt a Cross-Sector Fraud Strategy that brings together all sectors along the fraud chain - including telecom providers, social media, messaging services, online marketplaces, and advertising networks - under a shared responsibility model. Each actor should be accountable for mitigating risks within its domain, supported by enhanced collaboration, intelligence sharing, and proactive risk management.

### Key Recommendations:

- **Cross-Sector Control Frameworks.** Require technology platforms, telecom providers, and marketplaces to implement baseline anti-scam controls such as advertiser verification, rapid removal of fraudulent content, and SIM-swap protections. The European Commission should convene a cross-industry fraud task force to coordinate these efforts and define consistent best practices.
- **Develop Cross-Sector Intelligence Hubs for Systemic Threat Analysis.** Promote EU-wide intelligence hubs that aggregate, and correlate verified data from multiple sectors - finance, telecoms, social media, marketplaces, and technology platforms. These hubs should map scam networks, trace cross-channel fraud journeys, and distribute actionable alerts across industries. Such hubs would enable earlier disruption of cross-sector scams and reinforce accountability across the entire digital ecosystem.
- **Accountability Across the Chain. Extend due diligence and anti-fraud expectations beyond the financial sector.** Each participant would be responsible for preventing fraud within its sphere of influence and for contributing to restitution when its controls fail. A cross-sector, shared-accountability model promotes collective deterrence rather than blame-shifting. This balanced approach fosters proactive prevention over reactive compensation, strengthening trust, transparency, and resilience across Europe's digital economy.

Cross-sector collaboration can address many vulnerabilities within the digital economy, but it cannot dismantle the organized criminal networks operating behind them. To translate private-sector cooperation into systemic deterrence, the EU must also mobilize public authorities and law-enforcement agencies through a whole-of-government, cross-border strategy.

## 4. Adopt a Whole-of-Government and Cross-Border Response

The private sector cannot fight fraud alone. Given the transnational nature of scams and organized criminal networks, a coordinated public response is essential. Fraud and scams are increasingly orchestrated by sophisticated groups operating across jurisdictions and exploiting digital platforms beyond the EU's borders. Addressing these threats requires a whole-of-government strategy - one that brings together financial regulation, law enforcement, cybersecurity, and diplomatic action to disrupt criminal operations before they reach consumers.

The EU should complement its cross-sector fraud strategy with enhanced law enforcement and prosecution capabilities, ensuring that criminal actors face consistent deterrence and accountability. Fraud prevention must be treated not only as a compliance obligation for industry, but as a national and European security priority, requiring strategic coordination between public authorities, regulators, and private-sector partners.

### Key Recommendations:

- **Coordinate Across Policy Domains.** Align anti-fraud initiatives with the EU's broader digital, financial, and cybersecurity agendas, ensuring that frameworks such as PSD3/PSR, the Digital Services Act (DSA), the NIS2 Directive, or the Digital Operational Resilience Act (DORA) reinforce one another. A coordinated approach will close systemic gaps, strengthen consumer protection, and promote a consistent standard of trust and security across the digital economy.

- **Strengthen National Law Enforcement Capability and Prosecution of Fraud Networks.** Invest in resources, technical tools, and specialized training to improve Member State capacity to detect, investigate, and dismantle organized fraud networks. Enhanced domestic capability - supported by streamlined judicial cooperation - will ensure timely prosecution, stronger deterrence, and visible accountability for perpetrators.
- **Promote Robust International Cooperation and External Enforcement.** Deepen collaboration with non-EU partners on joint investigations, intelligence sharing, and cross-border enforcement actions. The EU should also apply diplomatic and regulatory pressure on jurisdictions that function as safe havens for cyber-enabled fraud, money mule networks, or large-scale scam operations - ensuring that EU efforts are supported by a credible global enforcement posture.
- **Empower Europol as the Strategic Anchor of the EU's Anti-Fraud Ecosystem.** Expand Europol's mandate and operational authority to coordinate EU-wide fraud and scam prevention through a dedicated intelligence and response hub, modelled on successful examples such as Singapore's Anti-Scam Command Centre. This structure would integrate real-time information exchange, cross-sector collaboration, and operational tasking across Member States, while operating under a clear statutory framework for data sharing, accountability, and privacy protection.

> By coordinating public authorities and industry partners, the EU can tackle scams at their source, dismantle criminal infrastructure, and prevent the misuse of legitimate digital platforms for fraudulent activity. A unified national, EU and international strategy will strengthen Europe's ability to detect, deter, and disrupt organized fraud, protecting consumers and reinforcing trust in the digital economy.

> While enhanced enforcement and international cooperation are vital to disrupt organized fraud networks, lasting success requires engaging the public as part of the solution. The next step is to empower consumers with the knowledge, tools, and confidence to detect deception and function as the first line of defence in Europe's fraud ecosystem.

## 5. Empower and Protect Consumers as Active Partners

Consumers remain the final and most critical line of defence against fraud. As scams increasingly rely on psychological manipulation rather than technical intrusion, empowering individuals through education, awareness, and clear protections is essential. Fraud prevention must therefore treat consumers not only as potential victims to be reimbursed but as active participants in a shared security ecosystem.

Building on an ambitious EU Commission 2030 Consumer Agenda, the EU should promote a coordinated public–private strategy to strengthen consumer protection, awareness, and accountability. This includes ensuring that customers receive clear, consistent information about fraud risks while maintaining proportionate liability standards - recognizing that true protection requires both responsible industry behaviour and informed consumer action.

These consumer-level measures complement the institutional and cross-sector frameworks described in earlier sections, ensuring that protection is consistent from system to individual.

### Key Recommendations:

- **Strengthen Consumer Protection and Accountability.** Clarify shared liability in fraud cases to ensure balanced responsibility. Consumers should be protected from sophisticated deception, but gross negligence - such as ignoring verified warnings or bypassing security checks - should carry proportionate consequences.
- **Enhance Consumer Awareness and Education.** Support coordinated industry and public initiatives that promote digital literacy and awareness of social engineering tactics. Consistent messaging across banks, PSPs, telecom providers, and digital platforms can help consumers recognize manipulation early and make safer decisions.
- **Strengthen Victim Support.** Law enforcement should receive specialized training in victim engagement and fraud awareness to ensure sensitive handling of cases, effective escalation, and consistent communication. Improved coordination and victim-centred practices will help restore trust, accelerate recovery, and generate valuable intelligence to prevent future harm.

> By fostering a culture of shared vigilance, Europe can build a more informed, resilient, and fraud-aware public - one capable of recognizing manipulation, resisting deception, and contributing to collective protection. Empowered consumers, working in partnership with industry and public authorities, represent the strongest foundation for trust and security in the digital payments ecosystem.

# Conclusion

The fight against fraud in Europe stands at an inflection point. PSD2's Strong Customer Authentication (SCA) was a landmark step in securing online payments, dramatically reducing unauthorized fraud, and establishing Europe as a global leader in payment security. Yet, as this paper has shown, the fraud landscape has evolved faster than regulation. Criminals have shifted from stealing credentials to manipulating consumers, exploiting psychological, procedural, and technological blind spots that SCA alone cannot close.

The data is clear: socially engineered and authorized payment fraud now dominate, enabled by the very success of SCA in blocking traditional attacks. Fraudsters exploit the seams between financial, digital, and telecom ecosystems - where accountability is diffused and defences are fragmented. The result is a system that looks safer on paper yet leaves consumers more exposed to deception in practice.

PSD3 and the PSR provide a once-in-a-decade opportunity to rethink Europe's fraud prevention architecture. The goal should not be to discard SCA, but to modernize it and integrate it within a broader, adaptive framework – one that reflects the realities of today's threats and the technologies available to counter them. The cost of incremental change is steep: continued consumer harm, eroding trust in digital payments, and constrained innovation. The alternative is a bold, future-oriented framework that makes Europe both secure and frictionless by design.

Taken together, the five policy priorities outlined in this paper form a comprehensive blueprint for next-generation fraud prevention - one that extends beyond PSD3 and the PSR into interconnected policy areas spanning financial, digital, law-enforcement, governmental, and consumer-protection domains.

> Implementing these measures would create an adaptive, intelligence-led ecosystem where every actor - public or private, digital, or financial - plays an active role in detection, prevention, and accountability. The message is simple: fraud prevention is not a banking issue - it is an ecosystem issue, and it requires ecosystem solutions.

> If implemented appropriately, PSD3 and PSR can be a first step in achieving this. They can deliver outcome-based, innovation-friendly regulation that empowers providers to deploy the best available security methods while preserving a seamless user experience. They can embed cybersecurity best practices into payments law, align incentives across sectors, and restore consumer trust in digital transactions.y acting decisively, the EU can once again lead the world in secure, trusted, and competitive digital payments - proving that strong protection and user-friendly innovation are not opposing goals, but two sides of the same European advantage.

1

## Future-Proof SCA

Ensure authentication evolves in step with emerging threats and technologies, enabling adaptive, phishing-resistant, and intelligence-led methods.

2

## Collaborative Fraud Intelligence

Build real-time, privacy-respectful data-sharing frameworks to detect and disrupt fraud collectively across banks, fintechs, PSPs and merchants, and across borders.

3

## Cross-Sector Coordination

Recognize that the responsibility for fraud and scam prevention now lies beyond payments to digital platforms, telecom providers, and online marketplaces.

4

## Whole-of-Government Action

Treat fraud as a security and law enforcement priority, coordinating financial, cyber, and diplomatic tools to tackle scams at their source.

5

## Consumer Empowerment and Protection

Strengthen public awareness, digital literacy, and victim support to ensure citizens are informed, supported, and resilient.

# Strong Customer Authentication (SCA): is it still strong enough?

**Benjamin Cler**
Director | Cloud & Engineering

## Introduction: the promise and the limits of Strong Customer Authentication (SCA)

Strong Customer Authentication (SCA) was one of the most visible and impactful requirements introduced by the PSD2 directive. It marked a decisive shift in the way the European Union approached payment security; moving from a reactive model to a proactive standard built on clear principles: verify who you are with at least two independent factors. The goal was simple: reduce fraud and restore trust in the growing world of digital commerce.

And it worked. Since its rollout, SCA has helped to significantly reduce fraud on card-not-present transactions[1] and provided a harmonised security baseline across the EU. Consumers are more protected. Payment providers have clearer rules to follow. The system is stronger.

But SCA, as powerful as it is, wasn't designed for today's fraud landscape. The methods attackers use have changed, shifting from purely technical exploits to targeting human behaviour. Social engineering, identity theft, fake websites and hijacked recovery flows now bypass the protections SCA was meant to offer. And while the principle of SCA remains sound, the ways it is implemented, often still reliant on SMS OTPs or static credentials, are no longer enough.

As new authentication methods emerge and fraud becomes more intelligent, we must ask a simple question: is SCA still strong enough in a world of AI-driven fraud and passwordless ecosystems?

## SCA today: a solid but aging foundation

The strength of SCA lies in its simplicity. It is built on three clear types of authentication factors: something the user knows, something they have, and something they are. By requiring two independent factors, the regulation established a flexible and future-proof framework. In principle, this approach is still entirely valid.

The issue lies in how it has been put into practice. When PSD2 was adopted in 2018, most implementations of SCA were based on the technologies available at the time. SMS one-time passwords, static PINs, and fingerprint-based authentication became the standard. While effective initially, these methods were not designed to withstand the sophisticated fraud tactics we see today. Attackers have shifted their focus from bypassing authentication directly to exploiting context, timing, and human behaviour. This includes techniques such as social engineering, phishing, and impersonation to trick users into approving fraudulent transactions or revealing credentials.

### What is a Passkey?

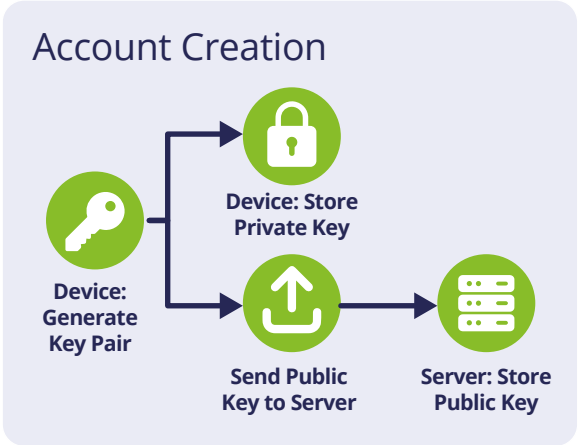
A passkey is a digital credential, based on public-key cryptography, that replaces a traditional password.

It consists of a unique cryptographic key pair: a public key, which is registered with the website or service, and a private key, which is stored securely on the user's device (such as a phone or computer) and never leaves it.

No separate application is needed; the technology is built directly into the device's operating system (e.g. iOS or Android) or password manager (e.g. 1Password, Dashlane or LastPass).

To log in, the user simply approves the authentication request using their standard device unlock method - such as facial recognition, a fingerprint scan, or their device PIN. This action proves possession of the private key without the key itself (or any other secret) ever being transmitted.

Because no password exists to be phished, shared, or stolen, this method is inherently resistant to the social engineering and credential theft attacks that target traditional authentication.




1 2024 Report on payment fraud | EBA

Deloitte.

In many cases, SCA is now reduced to a compliance exercise rather than a dynamic part of the fraud prevention strategy. The framework is right – but execution needs to evolve to match the threat landscape.[2]

## The rise of passwordless and new identity models

While SCA remains conceptually strong, the technological landscape around it has moved forward. New methods of authentication have emerged that improve both security and user experience. These innovations do not replace the core principles of SCA but rather offer more robust and seamless ways to apply them.

One of the most significant advancements is the adoption of passkeys (see the box "What is a Passkey?" for more details). These passwordless credentials[3] combine something the user has (their device) with something they are (biometric recognition). The result is a phishing-resistant, frictionless experience that meets SCA requirements while reducing the reliance on outdated tools like SMS codes.

At the same time, Europe is preparing for the rollout of eIDAS 2 and the EU Digital Identity Wallet[4], which aim to provide individuals and organisations with portable, high-assurance digital identities. These wallets will enable secure authentication across borders and sectors, laying the foundation for trusted interactions beyond payments.

These developments demonstrate that SCA does not need to be replaced or rewritten. Its flexibility allows it to absorb and integrate modern solutions. However, as authentication becomes more advanced, the weakest point in the chain shifts elsewhere.

Recovery (the process of regaining access when a device is lost or credentials are reset) has become the new entry point for fraud. No matter how secure the login method, if recovery is poorly protected, the system remains vulnerable. Ensuring that recovery processes are held to the same standards as authentication is now essential.

## Recovery: the hidden weak link

As authentication methods become more sophisticated, fraudsters increasingly look for vulnerabilities elsewhere. One of the most exploited and least regulated areas is account recovery. This is where users regain access after losing a device, forgetting credentials, or being locked out. Unfortunately, it is also where attackers often find their way in.

Rather than cracking passwords or intercepting codes, criminals now impersonate victims and exploit gaps in helpdesk procedures or recovery flows. Many social engineering attacks begin with a simple request for assistance: a fake lost phone, a forgotten login, a change of device – and end with a fraudster successfully re-enrolling a new device or resetting credentials.

In many organisations, recovery still relies on weak verification methods, such as email links or SMS messages, without context-aware checks or behavioural risk analysis. These methods fall far short of the security standards applied during initial authentication.

Recovery must become iron-clad. This means integrating it into the broader identity lifecycle, using verified digital identities, strong device binding, and layered verification. It also means ensuring that every recovery action is logged, monitored, and subjected to the same level of scrutiny as a high-risk transaction.

To close this gap, regulators and issuers should treat recovery not as a support function, but as a critical security control. As authentication strengthens, recovery must keep pace.

## Beyond SCA: toward continuous and adaptive authentication

SCA provides a solid foundation, but it was never intended to be the sole defence against fraud. On its own, it is static: it authenticates at specific moments, such as login or payment confirmation, and assumes those moments are enough to establish trust. In today's environment, that is no longer sufficient.

Fraud is dynamic. Attackers exploit context, timing, and user behaviour. To respond, organisations must go beyond binary checks and move toward adaptive authentication – a model that adjusts the level of scrutiny based on real-time risk[5].

This is where AI-powered fraud engines play a critical role. By continuously assessing user behaviour, device integrity, and transaction context, these systems can identify anomalies and trigger additional security measures only when needed. This helps balance security and user experience, reducing unnecessary friction for legitimate users.

Importantly, the security perimeter is expanding. It is no longer just banks and payment providers defending against fraud. Devices and browsers are now active participants. For example, Google Chrome's Enhanced Protection[6], powered by Gemini, can detect scams and fake websites in real time, offering users a new line of defence before a transaction even begins.

This shift highlights a key trend: security is becoming distributed. Trust is no longer established at a single checkpoint, but maintained continuously across the entire journey, with multiple actors contributing: issuers, identity providers, device manufacturers, and browsers.

2 Payments and digital assets | Deloitte UK

3 Passkeys: Passwordless Authentication | FIDO Alliance

4 EU Digital Identity Wallet Home | EU Digital Identity Wallet

5 Payments and digital assets | Deloitte UK

6 Protection from Online Scams & Fraud | Google Safety Center

Deloitte.

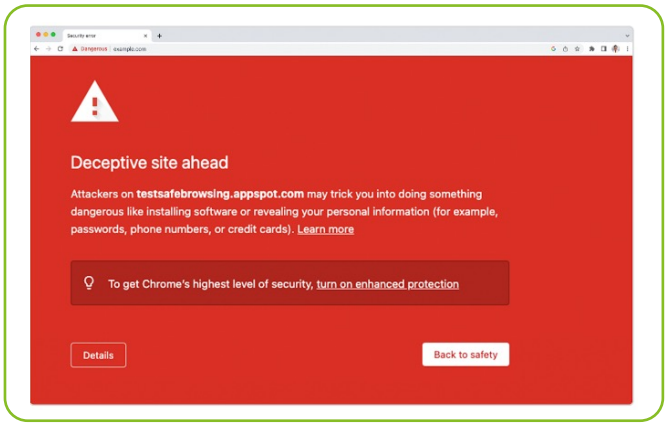



*Figure 2 - Google Chrome's fraud prevention screen*

As this model evolves, it is essential to design with users in mind. Adaptive authentication must not only be secure, but also inclusive. It should work reliably across devices, age groups, and levels of digital literacy. Achieving this balance requires thoughtful user experience design and a clear commitment to accessibility.

Finally, regulation has a role to play – not in limiting innovation, but in enabling it. SCA must remain a baseline, but organisations should be encouraged to go further when new technologies offer better outcomes for both security and users.

## A shared responsibility: the role of Regulators and the Market

The future of authentication cannot be shaped by individual actors alone. It requires coordination between financial institutions, technology providers, and regulators. While many organisations already recognise the need to evolve, some will only move when required to do so. This is why regulation must continue to play a proactive role; not only in enforcing baseline standards, but in encouraging the adoption of stronger, more modern solutions across the board.

The upcoming PSD3 and Payment Services Regulation (PSR), alongside eIDAS 2, present a timely opportunity to update and harmonise expectations. These frameworks can provide clear guidance on emerging authentication models, recovery procedures, and interoperability, helping the market move at a consistent pace[7].

But regulation alone is not enough. Collaboration across the ecosystem is essential. Fraud does not respect organisational boundaries, and attackers will always seek out the weakest link. Only by working together, across sectors and borders, can we create a coherent and resilient model of trust that keeps pace with evolving threats.

## Looking forward: quantum resilience and future challenges

While most of today's authentication challenges stem from evolving fraud techniques and inconsistent implementation, the horizon holds deeper, structural shifts. One of the most significant is the arrival of quantum computing.

Quantum capabilities may still be several years away from practical impact, but when they arrive, they will disrupt the foundations of current cryptographic algorithms. Many of the secure communication protocols used in today's authentication systems could become vulnerable to quantum-enabled attacks[8].

This is why forward-looking organisations are beginning to explore post-quantum cryptography, a new class of algorithms designed to withstand quantum threats. In parallel, there is growing interest in privacy-preserving technologies, such as zero-knowledge proofs[9], which allow trust to be established without revealing unnecessary data.

In this context, the next generation of SCA will need to be more than strong. It must be resilient, adaptable, and capable of evolving alongside the technologies that support it. That means embedding agility into identity frameworks, investing in crypto-agile architectures, and ensuring that authentication systems can incorporate new standards as they mature.

Ultimately, the goal is not just to protect passwords or devices, but to build sustainable trust that can endure even in a radically different digital landscape.

## Conclusion: keep SCA evolving

Strong Customer Authentication remains a cornerstone of secure digital payments. Its principles are sound, its impact is proven, and its flexibility gives it the potential to evolve. But security is not static. As fraud becomes more sophisticated and technologies advance, authentication must keep moving forward.

SCA alone is no longer enough. It must be complemented by adaptive risk analysis, hardened recovery, and a broader trust ecosystem that includes browsers, devices, and identity providers. The emergence of passwordless methods, digital identity wallets, and AI-driven detection signals a clear direction for the future.

Regulators, too, have a vital role to play, not just in enforcing compliance, but in enabling progress. By setting clear expectations and harmonising standards, they can help the market move faster and more consistently.

Europe has already led the way once with SCA. It can do so again by embracing a smarter, more collaborative, and future-ready model of digital trust. Because in cybersecurity, the greatest risk is standing still.

7 Shedding light on PSD3/PSR | Deloitte Luxembourg

8 Welcome to the post-quantum era: challenges and strategies for cybersecurity | Orange Cyberdefense

9 The next generation of data-sharing in financial services

Deloitte.

WORLDLINE

# On-the-Ground Interview

## A view on SCA and fraud

**Colombe Hérault**
Authentication & Identification
Portfolio Business Manager

**João Courinha**
Senior Global Product Manager

In this interview, PA EU engages in a conversation with Colombe Hérault, Authentication & Identification Portfolio Business Manager, and João Courinha, Senior Global Product Manager, both from Worldline. With over 18 years of experience in the payments innovation field, Colombe leverages her strong technical understanding and innovative management skills to define and develop new products that comply with regulatory requirements and adapt to the complexities of the payment landscape, drawing on emerging trends in digital identity, artificial intelligence, and new payment solutions. João is a Senior Global Product Manager for Worldline's fraud management solutions; drawing from his years in the financial sector, he develops fraud solutions that focus on current fraud trends, leveraging AI for real-time and near real-time monitoring across issuing, acquiring, and account payments.

### What is the main focus of Worldline in terms of products and fraud? Are there differences across European countries?

Worldline's main focus is to secure digital payments while keeping the customer experience seamless. We provide anti-fraud software and services for financial institutions, payment processors, and merchants, with a strong emphasis on card and payment fraud protection. Our main products center on authentication, digital identity, and of course, fraud. Our solutions enable our clients to prevent, detect, and respond to fraud across all payment channels, from card transactions to instant payments and e-commerce flows.

Worldline's approach covers a wide spectrum of fraud typologies, including impersonation and phishing attacks, account takeover (ATO), authorized push payment (APP) fraud, romance scams, synthetic identity fraud, and merchant fraud (and not only).

Across Europe, our strategy remains unified but tailored to local regulations and payment behaviors. Differences arise mainly from PSD2/SCA interpretation by national regulators, local payment rails, and the way consumers and fraudsters interact within each ecosystem. For example, in the Nordics, where instant and account-to-account payments are widespread, the main risks are authorised push payment (APP) and social-engineering fraud.

The Netherlands faces growing helpdesk, impersonation, and QR-phishing scams, while the UK and Ireland show similar patterns of APP and impersonation attacks due to the expansion of real-time payments.

In Southern Europe, where card payments and e-commerce remain dominant, card-not-present and merchant fraud are most common.

Meanwhile, Central and Eastern Europe continues to experience mainly card and phishing scams, reflecting the rapid rise of online and mobile banking. These variations show that while fraud patterns differ across regions, the underlying need for adaptive, data-driven protection is universal — and this is precisely where Worldline's Fraud Management and Authentication solutions deliver the strongest impact.

## What are the key measures currently implemented by Worldline to combat payment fraud? Which measures were the most effective?

Worldline provides a multi-layered, AI-driven fraud prevention solution that brings together technology, data, and authentication under one roof.

Key measures include:

- For the banks & merchants, reduce the Direct To Authorisation use cases (MIT, TO, Oneleg transactions) & push 3DS.
- AI-driven analytics and hybrid detection: combining rules with machine learning to analyze billions of transactions and detect anomalies instantly.
- Risk-based authentication: applying SCA intelligently, only when risk is high — ensuring security without unnecessary friction.
- Device and behavioral intelligence: using over risk indicators to identify suspicious activity.
- Cross-channel fraud visibility: connecting card, account, and merchant data to prevent fraud across the customer journey.
- Regulatory alignment and privacy by design: ensuring compliance with PSD2, SCA, and local banking rules while safeguarding customer data.

The impact is measurable and proven: over 15 billion transactions analyzed yearly with our Fraud solution, AI-driven fraud detection improvements deliver up to a 30% uplift, 50M+ yearly transactions secured, 3× fewer false positives than the industry average.

Among these, the most effective measures have been the AI-powered hybrid detection engine and risk-based authentication. Together, they deliver the highest fraud prevention performance by combining real-time decisioning with a frictionless user experience. AI enhances accuracy and speed, detecting new and subtle fraud patterns, while adaptive authentication ensures legitimate customers can transact smoothly.

## Which emerging types of fraud concern you the most ? Do they belong more to authorized or unauthorized payment fraud?

The most concerning emerging fraud types are primarily authorized payment frauds, where genuine customers are manipulated into authorizing fraudulent transactions. These represent the fastest-growing threat vector across our European markets.

Based on our experience in France and broader European operations, we observe that Merchant Initiated Transactions (MIT) show significantly higher fraud rates compared to transactions using 3D Secure authentication. This pattern led French regulator OSMP to implement new rules in 2024/2025 specifically targeting MIT in Direct To Authorization (DTA), one-leg, and MOTO transactions.

The implementation of MIT within 3DS frameworks has proven highly effective, demonstrating substantial fraud reduction. This validates our approach that proper authentication flows remain the most effective defense against evolving fraud tactics, particularly in authorized push payment scenarios.

## What do you think about the current effectiveness of SCA and how do you assess it?

SCA has proven effective as a foundational security measure, but its implementation varies significantly across European markets, creating both opportunities and challenges.

However, current SCA faces limitations in cross-channel fraud detection and user experience friction. The most successful implementations combine SCA with advanced fraud detection systems that analyze behavioral patterns, device intelligence, and transaction context. Our data shows that hybrid approaches using AI-enhanced risk assessment with adaptive SCA deliver up to 30% better fraud.

The regulatory framework provides a solid foundation, but technological evolution — particularly artificial intelligence — offers opportunities to enhance both security and customer experience.

## How do you see fraud evolving in the coming years? How would it impact Worldline?

Fraud evolution will be driven by three key factors: technological advancement, regulatory changes, and expanding payment ecosystems.

We anticipate sophisticated AI-powered attacks targeting multiple payment rails simultaneously, with fraudsters leveraging machine learning to evade traditional detection systems. Social engineering attacks will become more personalized using data from various sources, while synthetic identity fraud will grow as digital onboarding expands.

The expansion beyond traditional card payments to instant payments, Central Bank Digital Currencies (CBDCs), and account-to-account transfers will create new attack vectors. Fraudsters will increasingly target the authentication process itself, attempting to compromise biometric systems and exploit vulnerabilities in emerging technologies.

For Worldline, this evolution represents both challenge and opportunity. Our multi-layered, AI-driven approach positions us well to address emerging threats. We're investing in cross-channel fraud detection, behavioral analytics, and adaptive authentication to stay ahead of evolving attack methods. The key impact will be our ability to provide comprehensive fraud protection across all payment rails and customer interaction points.

## What are the most critical challenges and opportunities for Worldline regarding fraud and SCA?

**Challenges:**

- Emerging authentication schemes: New payment scheme competitors implementing Delegated Authentication programs that could fragment the authentication landscape and create security gaps.
- Technology adoption barriers: FIDO authentication adoption faces regulatory compliance challenges, requiring careful navigation between enhanced security and PSD2 requirements.
- Integration complexity: EU Digital Identity Wallet (EUDIW) authentication flows risk disrupting established payment processes, requiring significant technical adaptation.

**Opportunities:**

- Regulatory alignment: New regulations, particularly in France, reducing Direct To Authorization usage in favor of 3DS authentication, directly supporting our fraud reduction capabilities.
- Market expansion: Growing demand for comprehensive fraud solutions across all payment rails creates opportunities for our multi-channel approach.
- Technology leadership: Our AI-driven detection capabilities and extensive transaction analysis experience position us to lead in next-generation fraud prevention.

## Which technologies are most promising to combat payment fraud?

The most promising technologies combine artificial intelligence, behavioral analytics, and advanced authentication methods into integrated fraud prevention ecosystems.

Artificial Intelligence and Machine Learning:

- Real-time AI Scoring: Capability to score transactions in real-time and prevent fraud.
- Adaptive Learning: AI models that continuously retrain and adapt to emerging fraud patterns using automated model training and transfer learning strategies.
- Behavioral Analytics: AI-powered analysis of user behavior patterns to distinguish legitimate from fraudulent activities without disrupting genuine transactions.
- Device Fingerprinting.
- Device identification solutions integrated in fraud platforms with the capability to track device trustworthiness, detect spoofed device fingerprints, and identify replay/bot attacks.
- Collection of fraud indicators: Detection signals including hardware details, browser data, and geographic information.
- Advanced holistic Data Analytics: Combination of multiple data sources from several payment rails and payment journey, for enhanced risk assessment. Cross-channel data correlation for detecting sophisticated fraud schemes.
- In depth portfolio monitoring: Predictive analytics using large historical transaction databases and complex pattern recognition.
- Biometric Authentication: Integration of physiological and behavioral biometrics for strong customer authentication (SCA) compliance with support tor standards from EMVCo, FIDO Alliance, EUID.
- Consortium Intelligence: Unified fraud intelligence networks sharing threat data across merchants and issuers. Real-time information exchange for proactive threat identification. Global fraud pattern recognition leveraging collective intelligence.

Production AI Models:

- 8+ AI models currently running in production across Central and northern Europe.
- Models that can serve both bank-specific and country-specific fraud detection needs.
- Technologies deployed include Neural Networks with multiple architectures and XGBoost models.

Real-time scoring Technology:

- Real-time AI scoring solution deployed across payment processing pipelines.
- Real-time AI Scoring: Worldline's Instant Score technology uses advanced machine learning to provide real-time fraud scoring with up to 30% improvement in detection rates while reducing false positives.
- Adaptive Learning: Our AI models can be continuously retrained to adapt to emerging fraud patterns using automated model training and transfer learning strategies.
- Behavioral Analytics: AI-powered analysis of user behavior patterns to distinguish legitimate from fraudulent activities without disrupting genuine transactions.
- Supports plug-and-play deployment on Worldline's private cloud or other public cloud providers.

Advanced AI Applications:

- Generative AI for dynamic rule creation and maintenance.
- Clustering models using K-Means unsupervised learning to minimize false positive ratesIdentity Behavioral Analysis providing real-time machine learning analysis across transaction networks.
- Using Gen AI as a complement to VoP algorithms to produce more reliable results.

## How is AI changing the game for attackers and defenders? Did you deploy AI-driven fraud solutions ?

Based on Worldline's large fraud management experience, where our human analysts conduct in-depth investigations of AI-flagged transactions through sophisticated case management systems and validate machine learning models using a rigorous "4 eyes principle," we've proven that combining human expertise with artificial intelligence not only reduces false positive ratios through monthly governance reviews and contextual decision-making, but also creates a feedback loop that continuously improves our AI models' accuracy —demonstrating that human oversight transforms AI from a standalone detection tool into a strategic fraud prevention ecosystem that adapts and evolves with emerging threats.

## How should SCA adapt to improve customer experience and increase protection?

Our perspective varies depending on the stakeholder viewpoint:

- From a Fraud Service Provider perspective: The current PSD2 framework provides a solid foundation. However, FIDO authentication integration represents the most significant opportunity — enabling enhanced security and user experience while maintaining regulatory compliance. This would require either regulatory adaptation or technological advancement to bridge current PSD2 compliance gaps.
- From a Merchant perspective: The regulatory framework should enable more frictionless, merchant-led authentication options, particularly for Secure Payment Confirmation (SPC) implementations. This would improve customer experience while maintaining security standards.

## If you could change three elements in the regulatory framework, what would you change/remove/add?

**It depends on the perspective:**

- For a company like ours, providing Fraud services, in particular ACS service, the current regulation is adequate. Nevertheless, as said earlier, solutions need to evolve, both in terms of UX and security thus it could be interesting to see how Fido will improve SCA experience (as no need to switch to another device for authentication) but Fido as of today is not compliant with PSD2. It could be interesting to see if there could be a change of regulation or advancements in technology that could make FIDO PSD2 compliant.
- for Merchants : the regulation could open doors to more frictionless & SPC merchant led.

## Way forward

The future of SCA is likely to be tied with improving the UX to the extreme. Meaning that the end goal would be to be able to authenticate the user without them noticing they are being authenticated, through behavioral authentication for example. User adoption will still rely on trust, and that would be the biggest challenge: how can a user still trust the operation they are authenticating is safe and secured if they don't even feel they're being authenticated? Building a user experience around this is key and one of Worldline's next challenges.

Fraud solutions are going to integrate more and more data (device data, white and black lists, cross channel data), collected throughout transactions, at many customer interaction points. Fraud has to be implemented:

- On all payment rails, not only card payments but also Account to account, CBDC, etc.
- In many different use-cases: payments for sure but also in other sensitive activities: add a new beneficiary, raise a threshold, etc.

Using proven technologies (such as rules) but also develop new AI models, under the supervision of experts, Fraud solutions are going to have a more holistic approach.

SCA & Fraud will also have to evolve with the new payment means, such as Agentic Payment. Delegating an AI agent to perform a purchase on your behalf comes with a new authentication & fraud framework that needs to be defined. Still, with usability, trust and clarity for the end-user.

Swissquote

# On-the-Ground Interview

## A view on SCA and fraud

**Cédric Devigne**
Chief Information Security Officer

Cédric serves as Chief Information Security Officer at Swissquote Bank Europe in Luxembourg, where he leads the bank's information security strategy and compliance programs. With a background in ethical hacking and penetration testing, he has spent the past decade transitioning from hands-on technical work to governance and strategic risk management. He currently oversees ISO 27001 implementation, DORA alignment, and the institution's broader cybersecurity and audit framework.

Swissquote Bank Europe is Luxembourg's leading online bank for investors and has been at the forefront of digital investing for over 20 years. Swissquote Bank Europe combines the trust and security of a Luxembourg bank with the ease of use and transparent pricing that are traditionally the reserve of fintechs. The Swissquote Group employs more than 1,000 people globally, with 35% working in technology roles. With over 600,000 clients worldwide and over €80 billion in client assets, the bank offers a wide range of digitally enabled banking and investing solutions to private, professional and institutional clients. Based in investor-friendly, AAA-rated Luxembourg, Swissquote Bank Europe has full bank status and is regulated by the CSSF under the oversight of the European Central Bank.

### What are the key measures implemented by Swissquote to combat payment fraud?

At Swissquote, we're developing a comprehensive fraud prevention initiative in collaboration with Swissquote Switzerland and Yuh that goes beyond traditional SCA requirements. Our approach centers on metadata intelligence and behavioral analytics rather than solely relying on authentication friction.

The initiative includes:

- Device fingerprinting and IP tracking to establish baseline patterns and detect anomalies.
- Transaction amount profiling with intelligent thresholds that trigger alerts for unusual patterns.
- Zero-trust architecture that evaluates risk based on contextual attributes rather than applying blanket authentication requirements.

The plan is to move from "authentication as a gate" to "authentication as a dynamic response." We authenticate when risk signals warrant it, not simply because a regulation mandates it.

## What emerging types of fraud are of greatest concern to Swissquote?

Authorized payment fraud is unequivocally our primary concern. While SCA has been remarkably successful at reducing unauthorized fraud, it has inadvertently created a false sense of security among customers. The "I authenticated, therefore it's safe" mindset makes social engineering attacks devastatingly effective.

We're particularly concerned about scammers targeting vulnerable populations, elderly customers, non-tech-savvy users, and those under psychological pressure.

These attacks exploit the human layer, which no amount of strong authentication can protect against. The sophistication of AI-driven impersonation scams has accelerated this problem significantly.

## What do you think about the current effectiveness of SCA, and how do you assess it?

SCA has been a success story for what it was designed to do: reduce unauthorized payment fraud. However, it's simultaneously created new vulnerabilities and degraded the customer experience in ways that are becoming untenable.

The fundamental challenge is that current SCA implementation treats all transactions with equal suspicion. A customer making their 500th payment to the same beneficiary faces the same authentication burden as someone making a first-time high-risk transfer. This creates friction fatigue, leading to both payment abandonment and, paradoxically, reduced vigilance when customers do authenticate.

## Which technologies are most promising to combat payment fraud?

The future lies in behavioral biometrics, contextualintelligence, and risk-based adaptive authentication.

Specifically:

- Behavioral biometrics that analyze typing patterns, mouse movements, and device interaction to detect account takeovers.
- Metadata correlation across device, location, time-of-day, and historical patterns.
- Real-time risk scoring that adjusts authentication requirements dynamically.

Regarding passkeys and FIDO2, we've conducted extensive testing and found them to be a mixed bag. While they improve security posture, they don't meaningfully enhance user experience; in fact, initial setup can be quite complex for non-technical users. They solve the password problem but don't address the fundamental issue of adaptive security.

In the end, at Swissquote Luxembourg, we are only using them for specific internal use cases.

## How should SCA adapt to improve customer experience and increase protection?

SCA must evolve from static strong authentication to dynamic, attribute-based trust evaluation.

The goal should be to make authentication invisible when risk is low and proportionate when risk is elevated.

This means:

- Risk-based exemptions that are genuinely intelligent, not just transaction-value thresholds.
- Continuous authentication through behavioral biometrics rather than periodic friction points.
- Context-aware authentication that considers device trust, location familiarity, beneficiary history, and transaction patterns.

The philosophy should shift from "secure the transaction" to "secure the customer journey." We need to move beyond MFA as a checkbox requirement and toward zero-trust frameworks that evaluate dozens of attributes in real-time.

## If you could change three elements in the regulatory framework, what would you change?

1. Authority-led standardization initiatives
   Rather than each institution experimenting independently, regulators should facilitate cross-industry working groups to establish behavioral biometric standards, risk-scoring frameworks, and data-sharing protocols. We're currently learning through expensive trial and error, industry-wide collaboration would accelerate progress significantly.
2. Risk-based authentication flexibility Expand regulatory acceptance of dynamic authentication that adjusts based on comprehensive risk profiles. Current frameworks are too prescriptive about "when" to authenticate rather than "whether" authentication adds meaningful security value.
3. Safe harbor provisions for shared fraud intelligence Create legal frameworks that explicitly permit real-time fraud pattern sharing across institutions without running afoul of data protection regulations. Fraud is a cross-industry problem that requires cross-industry solutions, but current legal uncertainty creates paralysis. We have currently started to experiment with such solutions in collaboration with some of our crypto competitors.

## How important are cross-industry collaboration and data sharing in combating fraud? What forms of collaboration would you like to see?

Cross-industry collaboration isn't just important, it's essential and currently our biggest gap.

Fraudsters operate across institutions; our defenses should too.

Specifically, we need:

- Real-time fraud pattern databases that allow institutions to query: "Has this device/IP/account pattern been flagged elsewhere?".
- Standardized risk signals so that behavioral biometric vendors and authentication platforms speak a common language.
- Payment association leadership in facilitating these initiatives, as they have a neutral positioning to drive consensus.

The technology exists. What we lack is the regulatory framework and industry coordination to implement it at scale.

## What is your vision for the future of SCA? How would a next-gen authentication model look like?

Next-generation authentication should be invisible, continuous, and intelligent. The user should rarely be aware that authentication is happening.

This model would:

- Continuously evaluate trust through behavioral biometrics, device intelligence, and contextual signals.
- Authenticate adaptively, applying friction only when risk warrants it.
- Learn and evolve, using AI to identify emerging fraud patterns and adjust risk models in real-time.
- Collaborate across institutions, leveraging shared intelligence while respecting privacy.

In practice, this means a customer with an established trust profile, making a routine payment, experiences no authentication friction, while an anomalous transaction from an untrusted device triggers proportionate verification. Security becomes an intelligent layer rather than a gate. The irony is that better security should mean less visible authentication, not more. We're working toward that future at Swissquote.

payabl.

# On-the-Ground Interview

## A view on SCA and fraud

**Georgios Tangilis**
Fraud Lead

Georgios was born and raised in Greece and has a background in engineering and consulting. He built his foundational knowledge of the fintech industry and fraud prevention while working in the Netherlands, where he gained hands-on experience in global payments and risk management. He recently moved to Cyprus to lead the fraud team at payabl., focusing on building a scalable fraud prevention framework aimed at improving approval rates, reducing fraud, and leveraging AI/ML-driven decisioning.

Money is always in motion. It powers every decision and opportunity in your business. At payabl., we help you take control of this movement, transforming it into money flow that drives growth. We connect payments and business accounts in one platform, giving you complete visibility and the tools to navigate any complexity.

### SCA has strengthened security and reduced unauthorized payment fraud. However, authorized payment fraud increased, and new, more sophisticated fraud types, including impersonation and AI-driven scams, are rapidly emerging

SCA has significantly strengthened payment security and reduced unauthorized fraud by making it much harder for criminals to complete transactions without the cardholder's authentication. This has been a major step forward in protecting consumers and restoring trust in digital payments. However, we're now observing a clear shift toward authorized payment fraud, where customers are manipulated into approving transactions themselves.

These scams increasingly rely on impersonation tactics, with fraudsters posing as trusted organizations such as banks, government bodies, or well-known service providers. By establishing credibility and urgency, they trick victims into making payments or sharing sensitive information. The challenge has deepened with the rise of AI-driven schemes that leverage technologies such as voice cloning, deepfakes, and automated social engineering to create highly personalized and convincing interactions at scale.

In parallel, romance and investment fraud have surged, exploiting victims' emotional vulnerability and trust.

Fraudsters build long-term relationships online before persuading individuals to transfer money or invest in fictitious opportunities.

As a result, the fraud landscape is shifting from technical exploitation to psychological and social manipulation.

This evolution calls for new, more adaptive detection and prevention strategies, including behavioral analytics, real-time risk assessment, customer education, and closer collaboration across the financial ecosystem to effectively combat these emerging threats while maintaining a seamless user experience.

At payabl., we utilise not only static rules but also a Machine Learning/AI model powered by Sift, which could give us an edge in reducing fraud while increasing approval rates. Additionally, we built a new risk engine, which already shows less fraud, faster authentication, and increasing authorisation rates.

## Customer experience has declined, with higher payment abandonment since SCA implementation

From a fraud prevention standpoint, the implementation of Strong Customer Authentication (SCA) under PSD2 has been a significant success in reducing unauthorized transactions and strengthening overall payment security. However, from an operational and customer experience perspective, it has introduced new challenges that have directly affected conversion rates and payment abandonment.

Since SCA became mandatory, we have observed a noticeable increase in friction during the checkout process. Additional authentication steps, such as OTPs, app approvals, or biometric verification, have disrupted the seamless experience customers were accustomed to. Even small interruptions in the payment journey can have a disproportionate impact on conversion, especially in e-commerce and mobile environments where user attention is limited and expectations for speed are high.

While consumers generally recognize the value of enhanced security, many still perceive SCA as confusing or risky. In cases where authentication methods fail due to expired sessions, poor mobile network coverage, or lack of familiarity with the bank's authentication app, transactions are often abandoned altogether. For merchants, this translates into lost sales and lower authorization success rates, even when legitimate customers are attempting to pay.

In essence, SCA has made payments safer but also more fragile in terms of customer experience. As fraudsters evolve, so must our authentication strategies toward smarter, adaptive models that preserve the intent of SCA while minimizing friction for genuine customers. This is what we do at payabl. and hopefully, the whole industry, from issuers to acquirers, should also move towards this direction.

The next phase of payment security must therefore focus not only on stopping fraud but also on rebuilding the simplicity and trust that drive customer loyalty.

## Current fraud prevention measures are insufficient, requiring modern, adaptive authentication solutions

As fraud patterns evolve, it has become increasingly clear that old fraud prevention measures, while effective in their time, are no longer sufficient to counter today's sophisticated threats. Traditional approaches, heavily reliant on passwords, SMS one-time codes, and static authentication flows, are proving inadequate against modern fraud techniques that exploit both technology and human psychology.

Fraudsters have adapted rapidly to post-SCA environments. While Strong Customer Authentication has reduced unauthorized fraud, it has not eliminated the problem; it has simply shifted it. We are now facing a surge in social engineering, authorized push payment scams, and AI-driven impersonation attacks, where the customer is manipulated into authenticating fraudulent transactions themselves. In this landscape, static security methods provide limited protection because they fail to assess context, intent, and behavioral patterns in real time.

To stay ahead in the industry, at payable., we move towards adaptive, intelligence-driven authentication models. At payabl., we believe the future of fraud prevention lies in flexibility and intelligence, not just compliance. Our fraud controls are evolving from rigid rule-based systems to adaptive ecosystems that can learn, predict, and respond in real time to emerging threats. By embracing AI/ML models and similar modern standards, the payments industry can reduce fraud exposure, improve user trust, and restore the frictionless experience that digital commerce was built on.

In short, to protect tomorrow's payments, we must modernize authentication today, making it stronger, smarter, and seamless.

## SCA must evolve through biometric, behavioral, and risk-based approaches to balance security and user experience

As fraud tactics evolve, SCA must also advance beyond static two-factor methods. The next stage of Strong Customer Authentication should leverage biometric, behavioral, and risk-based approaches to maintain security without compromising user experience.

Behavioral analytics takes this further by introducing a continuous, invisible layer of defense. By analyzing subtle user patterns such as typing rhythm, device motion, touchscreen pressure, or mouse movements, systems can identify anomalies that signal potential fraud, even when credentials appear legitimate. This approach helps detect impersonation or AI-assisted scams early, before the transaction is completed.

In parallel, Risk-Based Authentication (RBA) introduces flexibility by adapting the authentication challenge based on transaction context. Low-risk activities, such as repeat purchases from trusted devices, can proceed seamlessly, while higher-risk scenarios trigger stronger verification steps. This dynamic decision-making maintains strong protection while minimizing unnecessary friction for genuine customers.

This layered, adaptive framework represents the natural evolution of SCA, one that blends security, intelligence, and user experience.

At payabl., we are continuously moving in this direction, investing in technologies that deliver security, speed, and trust for both merchants and end customers. By adopting biometric, behavioral, and risk-based standards, now and in the future, we aim to help our partners reduce fraud exposure while ensuring that every transaction remains both safe and effortless.

entersekt

# On-the-Ground Interview

## A view on SCA and fraud

**Gerhard Oosthuizen**
Chief Technology Officer

As CTO at Entersekt, Gerhard is responsible for leading innovation, research, and global strategic initiatives. He has over 25 years fintech experience in banking payments and digital channels. During this time, he has conceptualized and delivered payment and authentication solutions across the world. He has been with Entersekt for more than 12 years, and also spent 12 years at Mosaic Software (now part of ACI). Current focus areas are protecting Faster Payments from Social engineering and exploring how digital identity will impact the banking industry.

Entersekt, The Financial Authentication Company, provides financial institutions with digital banking fraud prevention and payment security solutions through its cross-channel, Context Aware™ Authentication platform that secures digital transactions and optimizes user experiences.

Founded in 2010, Entersekt serves financial institutions around the world, and holds 120+ patents for its security innovations. In 2023, Entersekt acquired the Modirum 3-D Secure software business from Modirum, a security technology firm based in Helsinki, Finland, positioning Entersekt as a global industry leader in authentication solutions for financial services. Entersekt processes 7.5bn+ transactions for 250m+ cardholders and 450,000+ merchants from nearly 900 banks in 70+ countries. Backed by companies like Silicon Valley-based Accel-KKR, one of the world's top private equity firms, Entersekt continues to expand its footprint across key regions.

### Fraud Trends

An observed trend is the increase in social engineering attacks that exploit emotional triggers. Fraudsters deliberately target the amygdala, the so-called "lizard brain", using primal emotions such as fear, anger, or sexual cues to bypass rational thought. These manipulations lead to irrational decision-making, allowing even well-educated and intelligent users to fall for phishing attempts, particularly when they are having a bad day or are emotionally compromised.

### Regional Fraud Prevention Philosophies

The U.S. approach follows a "do not challenge" philosophy, aiming to minimize friction and preserve user experience.

This strategy prioritizes convenience over security measures. In contrast, Europe operates in a heavily regulated environment that requires frequent customer challenges. Institutions are often compelled to justify or remove challenges to reduce customer burden, creating operational tension and compliance pressure. South Africa largely follows the European model. There is growing recognition that simply asking customers what they want to do is no longer an effective strategy, as users can easily be deceived into believing they are communicating with legitimate parties. Regulations, therefore, need to be rewritten to reflect the realities of social engineering. A fundamentally different approach to fraud prevention is required.

## Advanced Technology Solutions and Biometric Analysis

There are three main categories of biometric authentication: on-device, server-side, and behavioral biometrics.

- **On-Device Biometrics**

  Technologies such as Touch ID, Face ID, and Windows fingerprint scanning can provide two-factor authentication using cryptographic signatures. iPhones are noted for having three advanced sensors compared to traditional 2D cameras. A key requirement is the ability to detect changes in biometric profiles, such as added or removed fingerprints or altered facial features. Attackers could potentially register their own biometrics on compromised devices. Once verified, on-device biometrics become primarily a convenience factor for customers.

- **Server-Side Biometrics**

  Server-based face recognition and voice authentication are becoming increasingly problematic due to advances in AI and deep-fake technologies.

  Voice authentication, for example, has already been compromised, as Sam Altman warned, with many known cases where victims were conned in live video calls with fake people. Such methods are only viable when combined with other additional signals such as trusted device verification. Used in isolation, they represent a "slippery slope" in authentication security.

- **Behavioral Biometrics**

  Behavioral patterns, such as keystroke dynamics, require high entropy derived from repetitive typing behavior. However, auto-fill and password managers like Chrome's have significantly reduced opportunities for pattern collection. Historical deployments achieved only about a 30% capture success rate.

  Behavioral biometrics for anomaly detection can contribute to anomaly detection, for example, identifying whether information was typed or copied and pasted, or if a form was filled in faster than the norm. This technique is particularly effective in detecting fraud operations, such as call centers filling multiple forms rapidly. Post-authentication value, however, remains minimal due to the robustness of modern device security. Behavioral analytics shows promise, since it tracks more typical behavior as to the device types and locations and times where clients interact, and their frequency of interacting.

## Contextual Risk-Based Authentication Strategy

This risk-based approach centers on device cryptographic proof as the foundation of authentication. Public–private key pairs are permanently embedded in user devices, serving as a possession factor, similar to how car keys authenticate ownership of an expensive car. Geographical location changes are acceptable when the device itself can be proven legitimate. A high-risk situation might arise when multiple risk signals occur together, for example, a new location, a new device, and a new merchant, triggering the question: "Why would these three things happen simultaneously?"

Risk-Based Challenge Escalation

- Standard scenarios: Regular Strong Customer Authentication (SCA) pop-up approvals.
- Suspicious device pairing: Proximity-based authentication challenges.
- Suspected social engineering: Selfie verification on the original communication channel (not the victim's phone) or cross-channel verification through QR code scanning.

Authentication does not end once the user approves a transaction. There is a use for bi-directional signal collection and continuous evaluation after approval.

Additional signals can still trigger flags or delays, allowing early detection of fraudulent behavior during the scanning phase.

## SCA Implementation Challenges and Success Metrics

### Common Implementation Failures

- Banks are new to SCA processes and are not managing the registration processes
- Improper fallback procedures
- SMS OTP's present various challenges
  - Phishable, and since clients focus on code, they don't read the message
  - Fails if the DB contains Outdated or incorrect customer phon e numbers (or landline numbers)
  - MNO's delivery times are fraudulent
- Explore SCA procedures optimized for high success. Prefer On-device 2FA, rather than OOB (since that can also be spoofed.

**Defence in depth**

SCA mechanism should be selected based on risk conditions and behavioral analytics.The type of authentication can be changed to protect clients from attacks (e.g., protect against social engineering) or to improve acceptance rates.

**Customer Perception and Behavior**

Many customers expect to always see an SCA. They perceive authentication challenges as a "safety blanket," giving reassurance that their bank actively monitors transactions. Conversely, when friction is absent, customers may contact the bank's call center out of concern for potential fraud.

**PSD3 Enhancements**

The upcoming PSD3 regulations aim to reduce unnecessary friction while maintaining strong authentication. Key improvements include exemptions for recurring payments and merchant-initiated transactions, leading to a more seamless and secure user experience when implemented correctly.

## Comprehensive Regulatory Recommendations Framework

Four-pillar approach for advancing fraud prevention practices.

1. **Adaptive Authentication Philosophy**

   Adopt a risk-based, single-factor authentication model for low-risk activities. For instance, a weekly food delivery from a trusted device to a home address may only require possession of verification. Authentication should be contextual rather than applying blanket two-factor requirements in every scenario.

2. **Holistic Customer View Integration**

   The current siloed approach creates vulnerabilities as fragmented across multiple domains, with separate fraud systems for login authentication, push payments, and card payments, creating exploitable vulnerabilities. A typical attack chain might involve a password reset, device registration, and subsequent fraudulent card payment. There is a need for integrated fraud detection across all customer touchpoints to close these systemic gaps.

3. **Cross-Institution Pattern Recognition**

   Fraud detection should extend beyond individual institutions. A consortium-based detection network would allow banks to identify abnormal activity collectively. For example, a £100,000 deposit into an account that historically never exceeds £1,000 should trigger a review. The system should support anonymized signal sharing that preserves customer privacy while defining what data can or cannot be exchanged between institutions. And systemic attacks across various banks (e.g, based on a card breach) can be picked up more easily.

4. **eIDAS 2 and PSD3 Integration Strategy**

Digital identity frameworks primarily confirm "Is it you now?" but remain vulnerable to social engineering, where customers may willingly share identity data when deceived. Future regulations must maintain transaction-specific dynamic linking requirements and preserve strong customer authentication foundations. Digital identity should complement, not replace, established payment security mechanisms.

# Disclaimer

The interviews referenced in this report, as well as the selection of interviewees, were conducted and determined solely by the Payments Association EU. The perspectives shared reflect the expertise and experience of the participants and do not represent an official endorsement by any external institution, including those who may be part of, or contribute to, the project.

# Glossary

**Term**

1. **Credit Institution / Bank**

   A licensed financial institution authorized to receive deposits, grant loans, and provide a broad range of regulated banking services under EU law.

2. **Payment Institution (PI)**

   A Payment Institution (PI) is a type of financial institution authorized to provide various payment services under the regulatory framework established by the Payment Services Directive (PSD3) in the European Union.

3. **Electronic Money Institution (EMI)**

   A regulated institution authorized to issue electronic money (e-wallets, prepaid cards) and provide payment services, with strict safeguarding of customer funds.

4. **Account Information Service Provider (AISP)**

   A PSD2-licensed provider that aggregates and displays customers' account information from multiple banks, without handling or storing funds.

5. **Payment Initiation Service Provider (PISP)**

   A PSD2-licensed provider that enables online payments directly from a bank account to a merchant, acting as a third-party initiator but not holding customer funds.

6. **Phishing**

   A fraud technique using deceptive communications (e-mail, SMS, calls) to trick users into sharing personal data, credentials, or payment information.

7. **SIM swapping**

   A form of identity fraud where criminals transfer a victim's mobile number to a SIM they control, allowing them to intercept authentication messages.

8. **Malware**

   Malicious software designed to infiltrate devices, steal information, monitor activity, or manipulate transactions without the user's knowledge.

9. **Social engineering**

   Manipulation of individuals into performing actions or revealing confidential information, exploiting trust rather than technical vulnerabilities.

10. **Unauthorized payment fraud**

    Unauthorized Payment Fraud" refers to fraud when a fraudster gains unauthorized access to the account or payment credentials. For example, a fraudster gains access to your payment account or credit card information and makes payments that you are not aware of and did not authorize.

**Categories as defined in the questionnaire:**

- Card-present fraud (e.g. physical card stolen, counterfeited)
- Card-not-present fraud (e.g. remote use of stolen card data)
- Skimming and device tampering (e.g. use of illegal devices on ATMs or payment terminals to capture card data)
- Account takeover (ATO) (e.g. fraudster gains access to user's account)
- ACH/wire transfer fraud (e.g. unauthorized electronic transfers initiated after account compromise)
- Check fraud (e.g. forged, altered, or stolen checks used for payments or withdrawals)Check fraud (e.g. forged, altered, or stolen checks used for payments or withdrawals)
- Mobile or digital wallet fraud (e.g. unauthorized access/ enrollment of a new device, exploitation of app security flaws)
- Identity theft (e.g. using stolen personal information to open new accounts or access existing ones without authorization)
- New account fraud (e.g. fraudulent accounts created with stolen or fake identities to perform unauthorized transactions)
- Business email compromise (BEC) (e.g. fraudulent payment requests sent by impersonating senior staff or vendors)
- Malware and technical compromise (e.g. installation of malicious software to capture login/payment information for illicit use)
- SIM swap fraud (e.g. fraudsters transfer a victim's number to a new SIM to intercept authentication codes and access accounts)
- Unauthorized direct debit/mandate fraud (e.g. creation or alteration of bank mandates to debit victims' accounts without consent)

11. **Strong Customer Authentication under PSD2**

    'Strong customer authentication' means an authentication based on the use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the

breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.

**12. First-party abuse**

First-party abuse (or first-party fraud) refers to a situation where the customer intentionally commits fraud against a business or institution. This can also include collusion cases, where the consumer and merchant are working together to commit fraud against the payment provider.

**13. Authorized payment fraud**

"Authorized Payment Fraud" refers to a transaction initiated and authorized by the legitimate account holder that has been tricked, deceived or manipulated by a fraudster.

The payment is "authorized", the customer has willingly approved the transaction and SCA has been successfully completed. But authorization is obtained by deception or manipulation. For example, the fraudster convinces the customer to send money to a fake account or transfer funds under false pretenses (like a fake invoice, impersonation, or investment scam). This is different from unauthorized fraud, where payments happen without the customer's consent or knowledge (e.g. stolen card details used fraudulently).

**Categories as defined in the questionnaire:**

- Impersonation and authorization scams (e.g., Fraudster poses as a bank employee, police officer, government official, or company executive)
- Emotional and relationship scams (e.g., Scammer builds a false emotional relationship and requests money for emergencies, travel, etc.)
- Financial opportunity scams (e.g., Victim is lured into fraudulent crypto, property, or business schemes)
- Invoice scams (e.g., Fraudster sends a fake or altered invoice pretending to be a trusted supplier)
- Tech support scams (e.g., Fraudster claims to be from a software/telecom firm and instructs a payment for "services" or "repairs")
- Lottery and prize scams (e.g., Victim is told they've won a prize but must pay a release fee or taxes)
- Loan scams (e.g., Victim is tricked into applying for a fake loan, pays upfront fees for processing or insurance, but the loan is never disbursed)
- Charity scams (e.g., Fraudsters collect donations for non-existent causes or disasters)
- Purchase scams (e.g., Victim is persuaded to pay for goods or services online that are never delivered or do not exist)
- Housing and rental scams (e.g., Victims pay for deposits or rentals on properties they've never viewed or that don't exist)
- Employment scams (e.g., Payments are requested for fake training, certification, or job placement)
- Healthcare or medical scams (e.g., Payments for fake insurance, miracle health products, or fraudulent healthcare providers)

**14. SCA-exempted transactions**

Eligible electronic payments that do not require SCA due to low risk or predefined regulatory exemptions (e.g., low-value payments, trusted beneficiaries, Recurring transactions).

**15. SCA-authenticated transactions**

Transactions successfully authenticated using Strong Customer Authentication methods compliant with PSD2 requirements.

**16. Real-time transaction monitoring**

Continuous surveillance of payments as they occur, analyzing behavioral and contextual risk indicators to identify and block fraud instantly.

**17. Customer education programs**

Structured initiatives designed to raise user awareness about fraud risks and promote safe digital payment behaviors.

**18. Device fingerprinting**

Technology that identifies a device based on unique characteristics (hardware, software, configuration), helping detect suspicious or repeated fraud attempts.

**19. Negative databases**

Databases containing known high-risk profiles (e.g., fraudulent devices, accounts, merchants) used to screen and block transactions from previously identified threats.

**20. AI/ML fraud scoring**

The use of artificial intelligence and machine learning models to assign risk scores to transactions, improving fraud detection accuracy through pattern recognition.

**21. Behavioral biometrics**

Authentication method based on individual behavioral patterns, such as typing rhythm, mouse movements, or touchscreen interactions, to detect anomalies and fraud.

# Shaping the Future of Strong Customer Authentication (SCA)

## Modernizing Europe's Approach to Fraud Prevention


**The Payments Association EU**

Thibault de Barsy
Vice-Chairman & General Manager
"The Lhoft", 9 Rue du Laboratoire,
1911 Luxembourg
Phone +352 621 355923
Email thibault.de.barsy@thepaymentsassociation.eu
Website: www.thepaymentsassociation.eu

**Twitter:** @PAssocEU

**LinkedIn:** The Payments Association EU


PayPal

pa eu
the payments association

Deloitte.