Deloitte.

Safeguarding trust:
Fraud and resilience in an evolving world

A survey of Belgian citizens' responses to payment fraud:
Understanding the gap between awareness and threat

May 2026

Table of contents

I. Foreword

Payment fraud and cybersecurity threats represent significant challenges for the Belgian payments ecosystem in the digital era. The payments ecosystem includes multiple stakeholder groups such as consumers, financial institutions, payment networks and infrastructure, fintech and technology operators, telecom providers, social media platforms, and regulators and policymakers. As our society and the payment ecosystem have become increasingly sophisticated and interconnected, the threat landscape has evolved, particularly with fraudsters now leveraging artificial intelligence to create more convincing and targeted attacks.

At Deloitte, we have built an important practice helping companies combat fraud.

This report presents findings from expert interviews, a comprehensive survey of 1,000 Belgian citizens conducted in December 2025, literature research, and critical insights from our experts. It explores consumer awareness, personal security practices, vulnerabilities, and preparedness for emerging threats related to AI-enabled fraud techniques and sophisticated social engineering.

Our research reveals a troubling paradox: **Belgian citizens possess reasonable awareness of fraud threats, yet this awareness fails to protect them sufficiently when facing sophisticated attacks**. The research uncovers critical vulnerabilities across awareness, behaviour, institutional support, and generational resilience, which demand continued actions and collaboration across the entire ecosystem. Without decisive intervention, the negative impact will only intensify:

- Significant financial costs associated with fraud losses
- Erosion of public trust in our payment systems
- Reduced resilience of the payment ecosystem itself

As Deloitte Belgium, we are committed to contributing to the most important topics on the agenda of the financial services industry. In the previous years, our reports have focused on sustainable and affordable housing (2022), financial health and inclusion (2023), sustainable investing (2024), and health protection (2025). We see it as a privilege to be able to focus on fraud and resilience in 2026.

Happy reading!

Kasper Peters
Partner
Financial Services Leader
kapeters@deloitte.com

Andrea Radu
Partner
Cyber, Technology & Transformation
andrearadu@deloitte.com

Jordan Brasseur
Senior Director
Forensic
jbrasseur@deloitte.com

Georges Gehchan
Director
Cyber, Technology & Transformation
ggehchan@deloitte.com

Stephanie Baele
Director
Organisation & Work Transformation
sbaele@deloitte.com

II. Executive summary

1. The core challenge:

Fraud can affect any of us and represents a multifaceted, deeply entrenched problem...

Fraud can affect any of us and represents a systemic, ecosystem-wide problem that cannot be solved by individual institutions or awareness campaigns alone. The payment ecosystem comprises diverse stakeholder groups: governments, regulators, law enforcement, financial institutions, telecom providers, social media platforms, and consumers. Effective fraud prevention requires coordinated action across all ecosystem participants, as focusing on a single stakeholder group or implementing solutions without understanding interdependencies will inevitably fall short. Our research uncovers critical vulnerabilities across awareness, behaviour, institutional support, and generational resilience.

2. Key findings at a glance

1

Fraud is prevalent and increasingly successful

Nearly half of surveyed citizens have experienced online fraud or identity theft. What is more alarming is that when fraudsters strike, they generally succeed. Our real-life testing with two sophisticated fraud scenarios—a phishing* attack using fake QR codes and a vishing* (voice phishing) attack impersonating the police—revealed that fraudsters overcome initial victim awareness through psychological manipulation and technical deception. The message is clear: fraud is no longer a rare occurrence; it is a widespread threat affecting millions of Belgians. Of the citizens surveyed, 25% and 30% fell for these scenarios respectively, implicating loss of citizen money to fraudster accounts.

* Refer to the glossary section for a description of the technical terms in this report.

2

The awareness-behaviour gap is large

Here lies the central paradox of our findings: awareness does not protect you anymore. When we presented respondents with realistic fraud scenarios, 68% initially recognised the threat and expressed suspicion. Yet when fraudsters applied pressure tactics—creating urgency, exploiting trust in authority, or offering attractive incentives—many of the aware citizens became victims. This is not a failure of knowledge; it is a failure of behaviour under pressure. Fraudsters have learned to overcome awareness through sophistication, not through stealth.

3

Critical gaps in citizen security practices adoption

Belgian citizens have access to powerful fraud prevention tools—multi-factor authentication, account alerts, transaction limits, password managers—yet many do not use them. Protecting digital identity on online platforms requires robust password hygiene and multi-factor authentication (MFA), yet adoption rates are alarmingly low: 80% claim to use secure passwords, but only 30% update them regularly, and less than half enable MFA. This gap is particularly concerning given that nearly half of Belgian citizens have already been targeted by online fraud or identity theft. The tools exist, but citizens either do not know about them, do not understand their value, or find them too inconvenient to use. This is not a technology problem; it is a behaviour and communication problem. In the payments space, many mechanisms are therefore imposed on clients to protect them.

4

A severe generational divide

Fraud does not affect all generations equally. Our research reveals two distinct pathways to victimisation. Older citizens—baby boomers and Generation X (Gen X)—fall victim to authority-based scams where fraudsters impersonate police, banks, or government officials. Their trust in institutions and difficulty navigating complex digital controls under pressure make them vulnerable. Younger citizens—millennials and Generation Z (Gen Z)—display high confidence in their digital abilities, yet this confidence is not matched by actual protection. They fall victim to incentive-driven fraud (rewards, refunds, exclusive offers) and fast-paced scams that exploit their financial stress. The generational divide means that one-size-fits-all solutions will fail.

5

Ecosystem support falls short, despite substantial efforts

When fraud strikes, victims need support. Instead, they often find themselves navigating complex bureaucratic processes, waiting for responses, and feeling abandoned. Just over 40% of fraud victims report feeling unsupported. Beyond victim support, there is a broader ecosystem failure: nearly half of citizens either do not know how or do not know where to report fraud, while most do not understand the regulations that protect them and have never undergone training on how to recognise fraud. This challenge extends across all payment channels and digital platforms, yet the institutions, platforms, and service providers meant to protect citizens remain largely invisible to them, despite the substantial efforts delivered. In addition, regulation on, for example, data privacy and on instant payments introduces complexities for certain protection mechanisms of financial institutions.

6

Trust in institutions is dangerously low

Trust is the currency of the financial system. Yet our survey reveals a crisis of confidence: nearly three-quarters of surveyed citizens do not trust government to protect their data, and nearly half do not trust financial institutions. A widespread lack of awareness about existing consumer protections and regulations further deepens this distrust. When this lack of trust is coupled with feeling unsupported, citizens become less likely to report fraud—one in three victims have not reported their experience. We fully acknowledge the extensive fraud prevention controls already in place, the regulatory landscape governing the payment transactions, and the initiatives to increase awareness among citizens. But collectively, we also need to recognise that it is simply not yet sufficient in the light of the new threats. Without trust, the entire fraud prevention ecosystem breaks down. Collaboration between law enforcement, financial institutions, and supervisory bodies could support earlier detection of fraudulent activity and increase the likelihood of interrupting suspicious transactions at an early stage. In this context, collaboration around sound data exchange to facilitate more timely access for competent authorities could prove beneficial. The strategic focus on payment fraud within the judicial system, including continued efforts to streamline procedures and improve the recovery of illicit proceeds, is equally an important matter. Such developments may contribute to a more effective and consistent way forward. Lastly, given the cross-border nature of many fraud schemes, sustained cooperation with European partners such as Europol and Eurojust will continue to play a key role.

7

AI fraud anxiety is high, but understanding is low

Artificial intelligence has entered the fraud landscape, and citizens are worried. Nearly 80% of survey participants feel stressed about AI-enabled fraud. Yet 55% do not understand how AI is being used against them. This combination—high anxiety and low understanding—creates a dangerous vacuum where fear replaces knowledge. Citizens are afraid of a threat they do not understand, and this fear itself is one of the vulnerabilities that fraudsters are exploiting.

3. Proposed actions: Two critical pillars

Fraud can affect any of us and represents a multifaceted, deeply entrenched problem. Before proposing solutions, it is essential to understand the ecosystem that has expanded through digitisation and innovation. The payments ecosystem comprises diverse stakeholder groups: governments, regulators, law enforcement, national security agencies, payment service providers, telecom and technology providers, social media platforms, consumers, and others. Understanding this complex landscape is critical because effective fraud prevention solutions require a holistic approach across all ecosystem participants, as relying on a single stakeholder group or implementing solutions without understanding interdependencies will inevitably fall short.

Drawing from our research findings, this study identifies key challenges observed in our survey and proposes actions that stakeholders could consider to reduce payment fraud and increase the resilience of the payment ecosystem. We fully acknowledge the extensive fraud prevention controls already in place, the regulatory landscape governing payment transactions, and ongoing initiatives to increase citizen awareness. Many stakeholders are actively working to address these challenges, and in some cases, our suggested actions align with and reinforce initiatives already underway. This is not an exhaustive set of actions but rather a focused analysis of critical issues.

a. Pillar I: Blending human vigilance with automated defence

The reality: Fraudsters have become more sophisticated than ever, and artificial intelligence will make a traditional awareness-based defence even harder. We need to call upon everyone's responsibility and foster critical thinking among consumers, but we cannot expect citizens to out-think criminals who operate with industrialised efficiency and access to advanced technology. Pairing awareness, consumer vigilance, and automated defences must be reinforced and enhanced through coordinated action across the entire ecosystem to create layered defences that effectively counter the evolving threat landscape.

The solution: While awareness remains important, all ecosystem players should continue to invest in automated, multi-layered defences that operate in real-time and do not rely on human judgment under pressure.
This means:

- Sharing fraud signals within the payment ecosystem as early as possible (e.g., as from the text or WhatsApp message)
- Real-time AI-powered transaction monitoring that detects anomalies in payment behaviour before transactions complete
- Advanced verification systems using behavioural biometrics aligned with current legislation and device intelligence to identify fraudulent access attempts
- Automated alerts and transaction controls that pause high-risk transactions for additional verification
- Intelligent blocking mechanisms that prevent fraudulent payments from reaching criminal accounts

Moreover, real-time intelligence sharing becomes important in systemic interventions as it enables stakeholders to collaborate to eliminate fraud at scale.

While we acknowledge the regulatory complexities of balancing instant payments and privacy regulation, this proposal should be considered. We have examples from other countries such as the **Australian Financial Crimes Exchange** (AFCX), a **platform uniting government agencies, banks, telecommunications companies, and social media platforms for real-time intelligence sharing**. It mitigates fraud by enabling rapid, cross-sector exchange of threat intelligence to combat evolving scam tactics. Another example is **the newly announced Fraud Strategy 2026-2029 by the UK government**. A third example is with the Spanish Financial Intelligence Unit (SEPBLAC) which collects and shares financial intelligence in real time with banks, law enforcement, and regulatory bodies to combat money laundering and fraud. In all of these cases, the regulatory bodies played a crucial role in shaping the required legislative changes in collaboration with the payment ecosystem.

The benefit: Automated defences and real-time data sharing work 24/7, do not get tired, do not fall for social engineering, and do not require citizens to make perfect decisions under pressure. They shift the burden of fraud prevention from the individual to the system.

b. Pillar II: Balanced regulation to maintain trust

The reality: There are two dimensions to address. The regulatory paradox with regards to fraud-related data sharing and liability frameworks. Citizens expect institutions to protect them, yet they do not believe institutions can deliver. This trust gap undermines the entire ecosystem. Regulation alone cannot solve fraud, but it provides a legal framework based on which all ecosystem actors can take action in the fight against fraud.

The regulatory paradox
Under the current PSD (Payments Services Directive) 2 framework, the EU faces a regulatory paradox in instant payments fraud prevention. While PSD2 mandates real-time fraud detection, GDPR's strict data protection provisions create barriers to the data sharing necessary for effective fraud prevention. PSD2 lacks an explicit legal basis for inter-institutional fraud data exchange, leaving payment service providers (PSP) operating in legal uncertainty. This is particularly problematic because fraudsters operate across multiple financial institutions, yet banks remain wary of sharing fraud intelligence due to privacy concerns and to remain compliant with GDPR. The result is a fragmented approach where individual PSPs implement fraud detection systems without access to industry-wide fraud intelligence, a critical limitation when instant payments must settle within 10 seconds.

The way forward: The Payment Services Regulation (PSR) resolves this paradox by explicitly creating a legal basis for fraud data sharing within a GDPR-compliant framework. This regulation mandates that payment service providers share fraud-related data via dedicated platforms, with strict safeguards including mandatory Data Protection Impact Assessments, data minimisation limiting shared information to unique identifiers (IBANs), retention periods strictly limited to what is necessary for fraud detection, and mandatory verification requirements ensuring shared data does not lead to unjustified termination of customer relationships. Critically, PSR establishes that security and data protection complement each other rather than conflict. For fraud prevention, the regulation mandates real-time transaction monitoring mechanisms that analyse environmental and behavioural characteristics such as location, time, device, spending habits, and transaction history.

In addition, if we look at how upcoming regulations change customer protection, PSR in particular offers a revised pathway forward by:

- Mandating reimbursement for victims when a third party manipulates a consumer by pretending to be the consumer's payment service provider (PSP) and victims are manipulated into authorising payments, of course taking into account the gross negligence standard, and shifting liability for customer losses to financial institutions, strengthening the banks existing "skin in the game" when it comes to fraud prevention, a change when compared with PSD2 focus on unauthorised transactions
- Establishing clear, conditional consumer rights for fraud and transaction errors, with payment service providers communicating protections, timelines, and notification obligations
- Creating transparent accountability mechanisms where institutions must report fraud trends and prevention efforts

The benefit: By resolving the regulatory paradox between fraud prevention and data protection, PSR enables payment service providers to share fraud intelligence within a GDPR-compliant framework. This allows for real-time transaction monitoring based on industry-wide fraud patterns rather than isolated institutional data. Combined with clear reimbursement conditions for PSP impersonation fraud victims and consumer education, the regulation creates a more cohesive fraud prevention ecosystem. The gross negligence standard and repeated fraud safeguards ensure that consumer protections do not undermine incentives for personal vigilance.

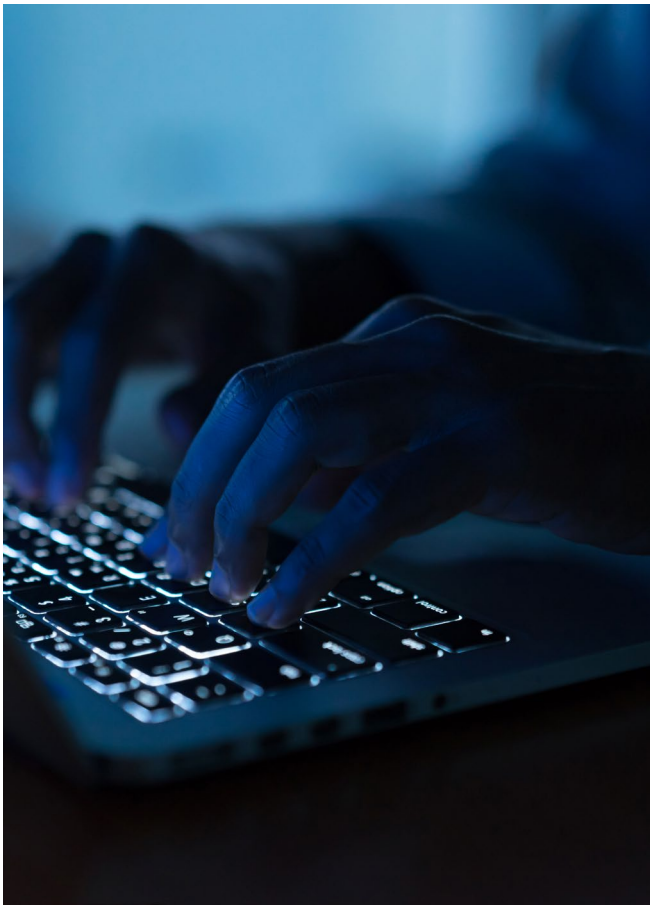
c. The ecosystem imperative

Neither pillar works alone. Automated defences without trust will be resisted by citizens who fear their data is being monitored. Regulation without technology will fail because no rule can stop a determined fraudster.

The path forward requires coordinated action:

- Financial institutions continuing to invest in technology and victim support
- Government and regulatory bodies establishing clear regulatory frameworks, public awareness campaigns, and investments
- Telcom providers and social media platforms implementing effective fraud prevention mechanisms
- Regulatory bodies should analyse how to introduce liability obligations for social media platforms, while there are already established specific liability obligations for telecom providers
- Employers providing generation-specific training
- Citizens adopting security practices and reporting fraud promptly

The bottom line: Payment fraud resilience is an ecosystem problem that requires ecosystem solutions. The time for incremental improvements has passed. Belgium's payment system requires a fundamental transformation in how we approach fraud prevention.



III. Introduction: Study approach and methodology

Our objective was to research the payment ecosystem literacy level of Belgians and examine how payment service providers, financial sector regulators, and other stakeholders in the ecosystem such as government, law enforcement, telecom and social media providers could help improve payment controls and fight payment fraud for citizens. To achieve these objectives, we employed a rigorous three-part research methodology.

1. Quantitative survey (December 2025)

We conducted a study combining **quantitative data collection**, **expert discussions**, and a **literature review**. The quantitative input was collected via a survey administered by a specialised marketing agency in December 2025. Targeting 1,000 Belgians who are customers of payment institutions, responsible for ordering payment transactions through all sorts of available payment channels, it investigated the five research topics listed in the methodology appendix using 45 questions and two real-life vishing and phishing attack scenarios.

2. Expert discussions

In January 2025, we held discussions with Deloitte subject matter experts from the fraud and payment industry to challenge and refine the study's preliminary findings. These discussions revolved around 10 driving questions and the two scenarios identified as critical to the research objectives.

For each question and both scenarios, the experts critically reviewed key figures and correlations from the survey and provided alternative perspectives and additional insights to enrich the report. The expert feedback played a key role in refining our recommendations and broadening the scope of our analysis.

3. Literature review

To further test the conclusions drawn from the quantitative data, we conducted a literature review using resources from our Belgian repository and wider networks, as well as a review of the regulatory framework of PSR and eIDAS 2.0. This allowed us to validate findings, contextualise them, and highlight where results either confirmed or nuanced our conclusions.

This comprehensive methodology ensured that the findings of this study are robust and actionable, offering clear insights into Belgian citizens' payment fraud literacy and the role of payment institutions and financial sector regulators in improving controls and fighting payment fraud.

IV. Examining fraud from two real-life scenarios

1. The scale of the problem

Nearly half of all Belgian citizens have experienced fraud. The survey reveals that 45% of respondents have experienced online fraud or identity theft, with 33% of attempts being successful, which translates to approximately **15% of the surveyed population being actual victims of payment fraud**.

This result aligns closely with official Belgian statistics (Febelfin*:August 2025: 13% phishing victimisation) and is about the same in France based on a press release dating August 2025*, validating the prevalence of fraud in Belgium.

** Refer to the bibliography section—If-it-smells-phishy-it-probably-is and Biocatch, respectively.*

The situation is even more aggregated with sophisticated payment fraud techniques involving emerging technologies, such as in the scenarios explored in this research.

2. How fraudsters win

To understand how sophisticated fraud operates in practice, we tested two realistic scenarios with surveyed respondents.

a. Scenario 1: Vishing attack (voice phishing)

Sam, a Belgian citizen, receives a series of phone calls from fraudsters impersonating police officers. The scammers claim Sam is involved in a crime linked to a car rental and pressure him to cooperate by verifying personal details and providing proof of the rental return. They then instruct him to transfer his bank funds to a supposed escrow account for protection during the investigation.

Despite initial suspicion and hesitation, Sam is manipulated into downloading a remote access app and authorising multiple transfers totalling over €52,000 to fraudulent accounts. The scammers exploit banking app features, including transfer limit increases, beneficiary name checks, and multi-factor transaction validation, which Sam overlooks. After the transfers, Sam realises that he has been scammed when he does not receive his escrow account details and after his bank confirms that no reversals of the transferred amounts could be made given the transactions were authorised by the account owner himself with all the associated controls validation and alert confirmation.

b. Scenario 2: Phishing via QR code

Alex, a Belgian internet service customer, receives a phone call from a fraudster impersonating the customer security team of his internet provider, warning him of a supposed hack on his account. The caller aims to collect personal and banking details for the purpose of verifying the customer's identity. The next day, Alex finds a fake delivery notice in his mailbox with a QR code for a 'complimentary' device, which he scans.

The QR code leads to a convincing fake bank payment page requesting his card number, PIN, and an SMS security code. Trusting the process, Alex enters the details and authorises a small payment. However, the fraudster uses this access to make multiple small fraudulent transactions and a large payment of €2,490, draining his bank account. When Alex contacts his bank, he is told that the transactions were authorised by the account owner himself using proper security codes, as well as PIN verification, leaving him unable to reverse the transferred amounts.

3. Why fraudsters win: The pull-push dynamic

Both scenarios reveal a critical insight: **fraudsters systematically dismantle each defence layer through social engineering, emotional manipulation, and technical deception.**

The attacker's strategy operates through what we call the pull-push dynamic, and the attacker's social engineering sophistication pulls victims through each resistance point, ultimately succeeding through:

- **Initial push (awareness):** Victims recognise the threat and resist
- **Attacker's pull:** Fraudsters overcome resistance by:
  - Exploiting trust in authority figures (police, banks, government)
  - Creating artificial urgency ("act now or lose access")
  - Leveraging psychological compliance principles
  - Targeting the weakest link: human judgment under pressure
  - Harvesting incremental data: Collecting personal information first (28% would disclose), then payment details
  - Bypassing verification: Only 8% would verify through secure channels login, the critical gap
  - Applying a multi-layered social engineering escalation strategy: The attacker carefully anticipates all possible reactions from the target, as well as the preventive controls built into the banking application, when designing the scam. With each step, the target becomes more vulnerable and the likelihood of achieving a successful payment fraud increases
  - Leveraging emerging technologies:
    - QR code obfuscation: Using newer technology that 20% of surveyed citizens couldn't recognise as their awareness hadn't caught up yet
    - Fake payment interface: Creating a convincing replica of the actual and legitimate bank page that 40% would enter their PIN into
- **Critical failure point:** When victims disregard automated and manual defences (ignoring bank alerts, controls over transfer limit increase, IBAN name check, failing to use MFA), they eliminate their final automated protection, allowing social engineering to succeed.

4. The outcome: Attacker wins the pull-push battle

a. Scenario 1: Vishing attack (voice phishing)

- 68% of surveyed citizens identified the first scam on vishing sensitive/personal data, constituting a high awareness level
  - The attacker's sophistication managed to convert 22% of those 'initially aware' into actual victims of the payment fraud (150 surveyed citizens)
  - Another 160 citizens fell victim to both the sensitive/personal data vishing and the payment fraud
- In total, 31% (310 citizens) ultimately fell victim to this scam and lost all their savings at the payment fraud level

b. Scenario 2: Phishing via QR code

- The targets' awareness created a strong initial defence barrier with 68% or 680 surveyed citizens identifying the scam in the first place
  - The attacker's sophistication managed to convert 18% of those 'initially aware' into actual victims of the QR code payment fraud level (120 surveyed citizens)
  - Another 130 citizens fell victim to both the initial personal data disclosure scam and the QR code payment fraud
- In total, 25% (250 citizens) ultimately fell victim to this scam and lost all their savings at the payment fraud level

5. Key findings

Both scenarios reveal that **Belgian citizens face a critical gap between knowing fraud exists and actually defending against it.** The vishing attack is more dangerous, with 31% victimisation, because it exploits authority and psychological pressure, while phishing relies on user mistakes due to threats of emerging technologies such as AI but still resulted in 25% victimisation.

As financial entities are building up their AI capabilities and digital offerings, fraudsters are also operating with industrialised efficiency, weaponising the very technology that drives digital finance to bypass security measures. The cost of creating real-life scenarios is minimal to them, and leveraging AI would allow mass deployment of such scenarios. Scammers are using AI to launch more convincing and widespread attacks. They send fake emails and make deceptive phone calls pretending to be working at trusted institutions or being trusted contacts. Using AI deepfakes, they can create realistic fake videos, audio recordings, images, and messages to trick consumers into giving up personal information or money.

The fundamental insight: Victim awareness creates a push against fraud, but attacker sophistication creates a pull that ultimately overcomes it. The attacker wins not only by defeating awareness, but by systematically dismantling each defence layer through social engineering, emotional manipulation, and technical deception.

a. A generational divide and the urgent need for systemic change

A critical situation is unfolding in the landscape of payment fraud, with **older generations bearing the brunt of increasingly sophisticated scams**. The data reveals a complex challenge that extends beyond individual vigilance, highlighting a **systemic vulnerability that demands immediate and advanced intervention** from the payment ecosystem participants.

There is a significant generational disparity in the victims of payment fraud. Baby boomers and Gen X are critically vulnerable, accounting for a staggering 70% of victims. They are followed by millennials at 20% and Gen Z at 10%.

Compounding this issue is a profound disconnect in perceived responsibility. The survey shows that 51% (510 individuals) do not believe they are responsible for losses incurred in both payment fraud scenarios. The vast majority of this group—67% or 340 individuals—are baby boomers and Gen X. They are followed by millennials at 23% (119 individuals) and Gen Z at 10% (51 individuals). Those 510 citizens out of 1,000 consider the responsibility rests with the banks and payment insurance providers (45% or 230 citizens), payment and mobile providers (40% or 205 citizens), and the regulatory bodies (15% or 75 citizens).

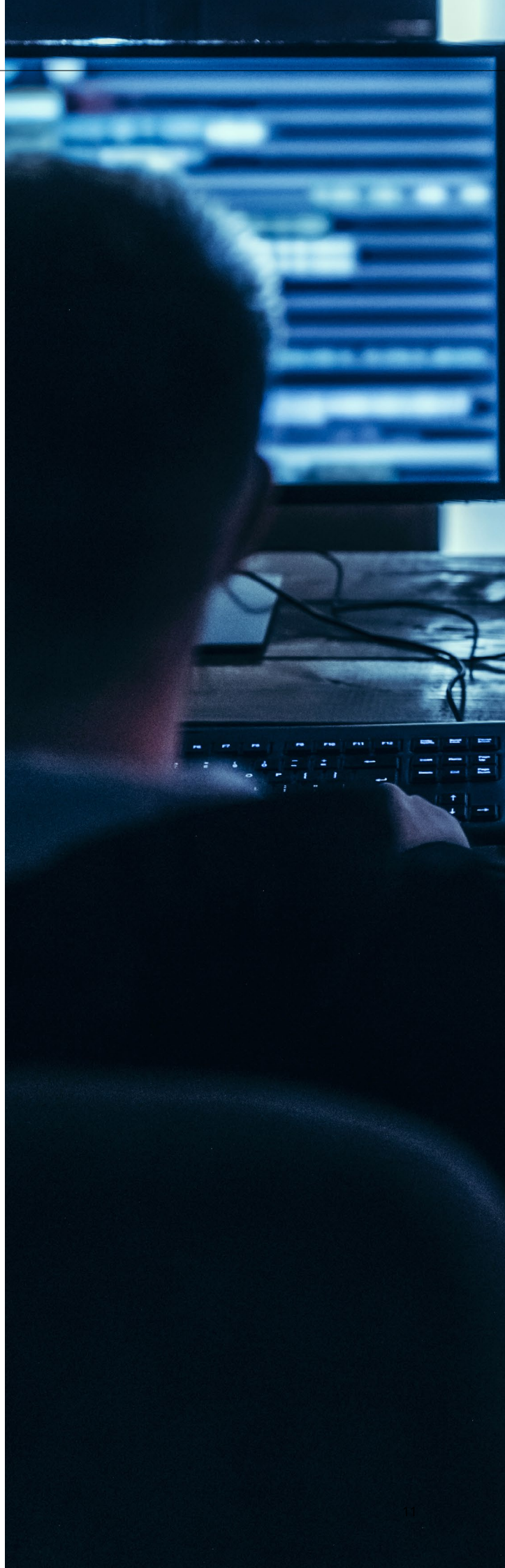
In contrast, 49% (490 citizens) believe that preventing fraud is a shared responsibility. Such allocation of responsibilities, where victims are partially blamed for the damages suffered, may deter them from seeking support and hinder effective prevention.

b. Outside awareness: The case for automated defence

Awareness campaigns provide a foundational and required defence layer in reducing financial fraud, especially now that fraudsters operate with industrialised efficiency, weaponising advanced technologies to bypass security controls. However, the escalating sophistication of frauds, including AI-powered voice cloning, deepfakes, and multi-vector attacks combining multiple attack vectors, renders traditional awareness campaigns insufficient. The question is: How could traditional awareness campaigns change to address this insufficiency?

c. The path forward

The path forward requires a shift in strategy. While financial institutions have made significant progress beyond customer education—implementing multiple controls and multilayered defences—there remains an opportunity to further strengthen their approach. What may be lacking is a more tailored strategy that considers generational differences. Knowing the current legislative constraints, institutions could explore fraud preventing initiatives, even if this might introduce some friction for customers, when it is ultimately in their best interest. Additionally, we want to further emphasise the need for enhancing real-time information sharing, enabling payment service providers to share fraud intelligence (e.g., unique identifiers of fraudulent accounts, attack patterns, emerging threats, etc.) through secure, GDPR-compliant channels to improve collective fraud detection and prevention capabilities. Fostering greater collaboration across the ecosystem is key toward building a truly resilient support infrastructure.



V. Key considerations

1. How large is the gap between awareness and behaviour?

The results from the survey provide a clear quantitative starting point for assessing the gap between awareness and behaviour. Nearly half of respondents (45%) report having experienced fraud directly, and in 33% of cases the fraud attempt was successful. At the same time, self-reported awareness and confidence in recognising fraud remain relatively high across the population. This contrast points to a structural discrepancy between perceived preparedness and actual behavioural outcomes.

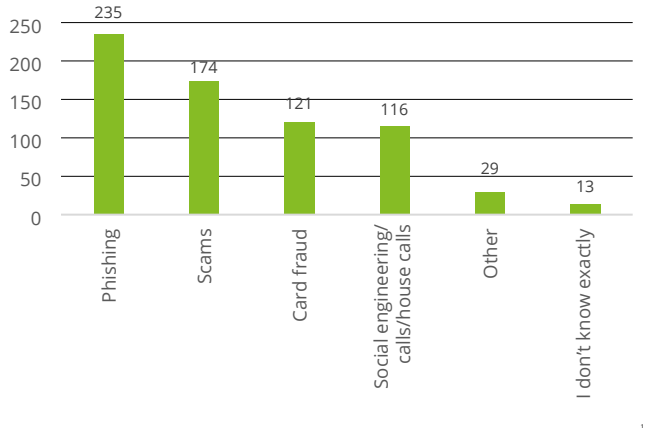
This discrepancy becomes more pronounced when awareness indicators are examined alongside experience-based questions. While a significant share of respondents indicates that they are confident in recognising fraudulent emails, messages, or websites, fraud exposure remains widespread and repeat victimisation is common. Awareness, in other words, does not function as a protective barrier. The survey shows no clear reduction in fraud success among those reporting higher awareness or confidence, suggesting that awareness operates largely as a self-perception rather than as a behavioural safeguard.

To address this gap, the desired behaviour must be one that truly reflects the level of awareness, translating knowledge into consistent, concrete actions. It is not enough for individuals to simply recognise the signs of fraud; they must also adopt vigilant practices such as carefully verifying unexpected requests, maintaining strong security habits, and exercising caution even when communications come from trusted contacts. Only when awareness is matched by such proactive and informed behaviour can it serve as an effective defence against fraud attempts and reduce the risk of victimisation.

The nature of fraud attempts reinforces this conclusion. As shown in Figure 1 (Types of fraud the surveyed population was confronted with), phishing accounts for 52% of all fraud cases, making it by far the most prevalent attack vector, followed by other scam types (39%). Phishing does not succeed because victims are unaware of its existence, but because it exploits how people actually behave when interacting with digital messages.

Survey responses on social circle fraud further support this point: fraud attempts involving known or trusted contacts show markedly higher success rates than direct attacks. Trust consistently lowers vigilance, even among respondents who consider themselves knowledgeable.

Figure 1 - Most common types of fraud the surveyed population was confronted with



Insights from the scenario analyses complement these findings by illustrating how this behavioural gap materialises in practice. Fraudsters apply time pressure ("act now or lose access"), authority cues (impersonating banks or government bodies), and incentive mechanisms ("you have won a reward") to push individuals toward immediate action. Under these conditions, respondents do not engage in reflective risk assessment; instead, they default to rapid, automatic decision-making.

This approach aligns closely with the Deloitte Behaviour FIRST Change methodology, which begins with observed behaviour rather than stated knowledge. Behaviour FIRST recognises that most human decisions are automatic, context-dependent, and influenced by subtle environmental cues rather than deliberate reasoning. From this perspective, the survey results represent the identify phase: they help us pinpoint which behaviours are falling short—such as rapid compliance, insufficient verification, reduced scepticism in trusted contexts, and inconsistent reporting—without presuming an abstract lack of awareness.

The FIRST framework then provides a structured way to understand the underlying drivers of these behaviours:

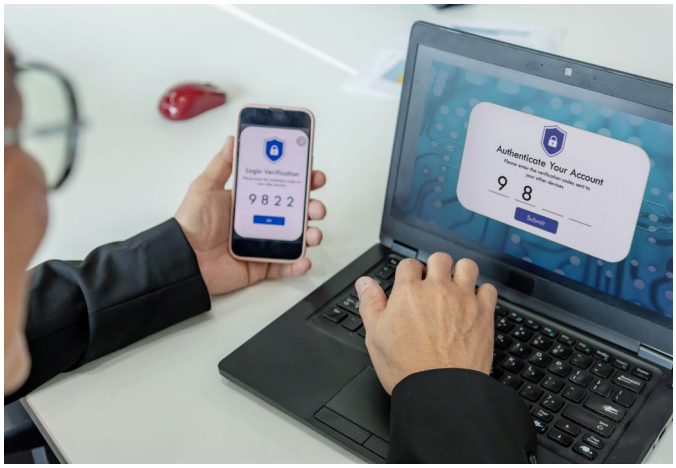
- **Fundamentals:** Overconfidence ("I would recognise fraud"), optimism bias ("this won't happen to me"), and loss aversion ("I might lose access or miss out") are evident in the contrast between high confidence and actual victimisation rates.
- **Incentives:** The survey reveals limited motivation to report fraud and widespread perceptions of inadequate post-incident support, which diminish incentives for vigilance and learning.
- **Relationships:** The higher success rate of fraud within social circles highlights how trust can suppress critical evaluation.
- **Stories:** Persistent self-narratives such as "I am careful" or "fraud happens to others" endure even after individuals have been victimised.
- **Tools:** Digital payment and communication systems prioritise speed and convenience, reinforcing habitual behaviour and leaving little opportunity for reflection.

Viewed through this lens, the awareness–behaviour gap identified by the survey is neither accidental nor surprising. It is the predictable outcome of environments where awareness remains static, but behaviour is dynamic and shaped by pressures, trust, and system design. Consequently, awareness campaigns alone struggle to reduce fraud because they do not intervene at the critical behavioural moments when risk actually materialises.

Importantly, the Behaviour FIRST framework is not only a diagnostic for current behaviour, it also provides a foundation for designing targeted interventions and developing clear pathways toward the desired behaviour. By addressing the specific behavioural drivers identified, organisations can move beyond raising awareness to fostering sustained behavioural change that effectively mitigates fraud risk.

Key finding

The survey evidence confirms that the gap between awareness and behaviour is both large and systemic. High self-reported awareness and confidence coexist with high fraud exposure and substantial fraud success rates. Behaviour FIRST helps explain this gap by shifting the focus from what respondents know to how they act under real world conditions. Closing the gap requires moving beyond awareness toward behavioural interventions that reshape decision-making at critical moments—where fraud succeeds.



2. Knowledge of payment and security controls

While Belgian respondents demonstrate strong financial monitoring habits and awareness of data privacy risks, critical gaps exist in the adoption and effective use of payment and security control mechanisms. As sophisticated fraud schemes such as the one described in the vishing scenario require fraudsters to collect information about the victim and potentially identity theft, our survey reveals a dangerous contradiction that undermines the foundation of account security: **despite 80% of respondents claiming to use secure passwords on online platforms, only 30% update them frequently.** Multi-factor authentication (MFA) adoption on online platforms remains low at 45%, and despite some banking-specific fraud countermeasures, such as withdrawal limits and transaction limits, being enabled by default. The customisation use is limited with, with 50% using withdrawal limits and 42% using transaction limits.

These gaps reveal a troubling pattern: respondents possess the tools to protect themselves but lack either the knowledge, motivation, or understanding of how to make use of them effectively. This section examines the disconnect between awareness and action, identifying where respondents are most vulnerable and what interventions could close the protection gap.

a. The illusion of password security: Why regular updates are crucial

Of the survey respondents, 80% claim to use secure passwords, yet only 30% update them frequently. Not updating passwords regularly creates vulnerabilities in case of data breaches, credential stuffing attacks, and social engineering. Cybercriminals often maintain (or sell) databases of leaked credentials and systematically test them across multiple platforms. A password that was secure when created may have been exposed in a breach months or years ago—yet if never changed, it remains an open door to account takeover.

The problem is compounded by generational patterns. Older respondents (baby boomers and Gen X) are more likely to claim secure password practices but less likely to update them regularly, suggesting they may be relying on outdated security practices. Younger respondents show better awareness of the need for regular updates, but overall adoption remains dangerously low across all age groups.

b. The control gap: Tools available, but underutilised

Financial institutions have deployed sophisticated fraud prevention tools, yet the survey respondents remain largely unaware of them or when enabled by default, they fail to utilise the controls or customise them to their own personal situations.

Despite the critical importance of robust security measures, adoption rates for key protections remain low. Only 45% of respondents utilise multi-factor authentication (MFA), a highly effective defence against account takeover. Similarly, just 57% have activated account alerts, leaving 43% without real-time notification of suspicious activity, and only 24% use card

notifications. Furthermore, a mere 8% use advanced features like call-back hotlines or geo-blocking. This gap between available tools and actual adoption suggests that respondents either do not understand the purpose of these controls, do not know they exist, or perceive them as creating too much friction in their banking experience.

The generational divide is pronounced. Baby boomers and Gen X show significantly lower adoption of MFA and advanced controls, suggesting both a knowledge gap and potential difficulty navigating digital interfaces. Millennials and Gen Z show higher adoption but still fall short of optimal protection levels.

c. Positive indicators: Financial monitoring and privacy awareness

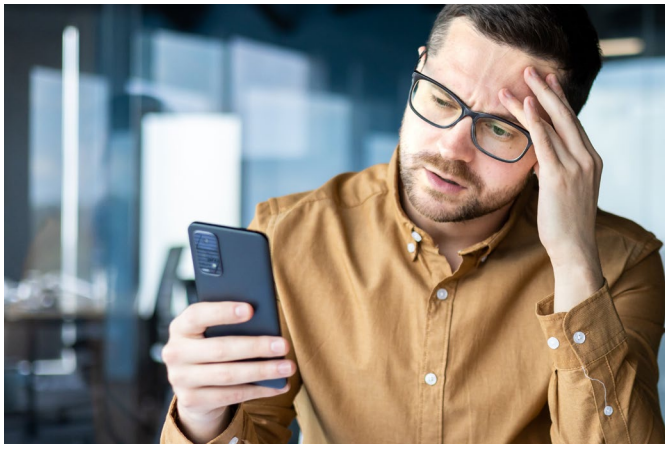
The survey also reveals some reassuring notes, especially in two areas with strong respondent engagement and awareness. When it comes to financial monitoring, 78% of respondents frequently check their bank statements, indicating active engagement with their accounts and ability to detect unauthorised activity. Regarding data privacy awareness, 90% of respondents are aware of risks in sharing personal information, demonstrating strong foundational security consciousness.

These positive indicators suggest that respondents have the foundational awareness and motivation to protect themselves. The challenge remains the same: closing the gap between intention and action.

Key finding

The survey indicates that the respondents have strong foundational awareness of fraud risks and demonstrate engagement with financial monitoring. However, a gap still exists in the adoption of security control mechanisms.

This awareness-to-action gap is compounded by pronounced generational divides. The ecosystem should implement targeted interventions—including behavioural nudges and tailored approaches for different age groups—that leverage citizens' existing positive habits to empower them to take consistent security action.



3. A generational divide

The survey results reveal a clear generational differentiation in how fraud risk materialises. When awareness, confidence, and actual fraud outcomes are examined together (Figures 1–3), it becomes evident that different generations do not merely experience different levels of fraud but follow distinct behavioural pathways to victimisation. These pathways are further illustrated by the fraud scenarios described in this report and can be meaningfully interpreted using insights from the Deloitte Global 2025 Gen Z and Millennial Survey.

Figure 1 (Overall awareness of payment-related fraud) shows that baby boomers and millennials report the highest levels of awareness, while Gen X and Gen Z display lower overall awareness. This finding already challenges the common assumption that younger generations are inherently more aware of fraud risks. However, as illustrated by the scenarios, awareness alone proves insufficient once individuals are exposed to urgency, emotional pressure, or perceived legitimacy.

Figure 2 - Overall awareness of payment-related frauds

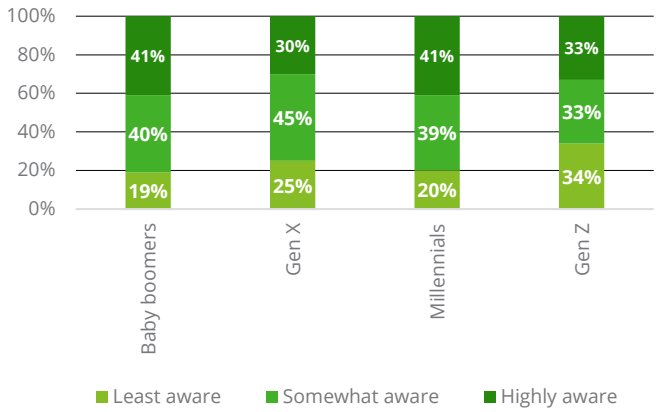


Figure 2 (Confidence in recognising fraudulent emails, messages, or websites) introduces a critical behavioural divergence. Confidence rises sharply among younger cohorts: both millennials and Gen Z report the highest levels of confidence (64%), despite Gen Z simultaneously reporting lower awareness in Figure 1. This confidence–awareness mismatch is a key risk indicator. It suggests that confidence is driven less by fraud-specific knowledge and more by digital familiarity and comfort with online environments.

Figure 3 - Confidence in recognising fraudulent emails, messages, or websites

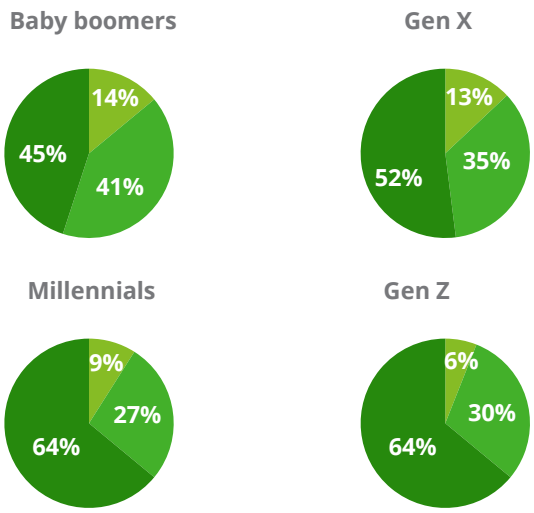


Figure 4 - Fraud experience and successful fraud attempts rate

The Deloitte Global 2025 Gen Z and Millennial Survey reveals that these cohorts are deeply immersed in digital ecosystems and generally confident in navigating technology, platforms, and online information. While Gen Z and millennials are digital natives, this does not necessarily extend to being AI natives. The survey indicates that AI is more integrated into their personal lives compared to other generations; however, this familiarity does not automatically translate into AI adoption in professional settings or other contexts such as fraud prevention. These generations operate in fast-paced, multitasking environments with constant digital interaction, which fosters behavioural acceleration characterised by rapid engagement, reliance on intuition, and less frequent verification. Their digital fluency may boost confidence, but limited AI-native experience could explain why their knowledge of AI-related fraud does not lead the field. The fraud scenarios involving too-good-to-be-true gifts, rewards, or refunds illustrate this mechanism clearly. Younger victims are shown to accept prompts rapidly, relying on their perceived ability to recognise fraud rather than actively questioning the legitimacy of the request. In these cases, fraud does not rely on authority or fear, but on familiarity, platform trust, and incentive framing.

The behavioural consequences of these perceptions become visible in Figure 3 (Fraud experience and successful fraud attempts). Baby boomers and Gen X are the most frequently targeted groups and experience the highest rates of successful fraud attempts. Scenario narratives explain this pattern. In scenarios where fraudsters impersonate banks, government institutions, or service providers and introduce urgency ("act now to avoid account suspension" or "immediate action required"), older cohorts are more likely to comply. Trust in institutional authority and familiarity with formal communication channels reduce scepticism, while time pressure and complex digital controls (e.g., authentication apps, password management, verification steps) increase cognitive load. Under these conditions, even respondents with relatively high awareness default to compliance rather than verification.

For millennials and Gen Z, the pathway differs but remains equally concerning. Although these cohorts are targeted slightly less often than older generations, their fraud success rates remain high relative to exposure. The Deloitte Global 2025 Gen Z and Millennial Survey provides important context here: both Gen Z and millennials report elevated levels of financial stress and insecurity, with many living paycheck to paycheck or expressing concern about their financial future. In such circumstances, fraud scenarios promising immediate gain, relief, or exclusive opportunity resonate more strongly and are more likely to trigger rapid, unreflective action.

Taken together, the figures, scenario illustrations, and Deloitte insights reveal two distinct yet complementary behavioural pathways to fraud:

- Authority- and urgency-driven compliance, predominantly affecting baby boomers and Gen X, where trust in institutions and difficulty navigating digital controls under pressure override awareness
- Confidence- and incentive-driven acceleration, predominantly affecting millennials and Gen Z, where high digital confidence, platform trust, and financial pressure reduce scepticism and verification

Crucially, Figures 2 and 3 demonstrate that confidence is not a reliable proxy for protection. The generations reporting the highest confidence in recognising fraud are not those with the lowest fraud success rates. Instead, vulnerability emerges where confidence, trust orientation, and contextual pressure combine to suppress reflective decision-making—precisely the conditions engineered in the fraud scenarios described in this report.

Key finding
The generational divide in fraud vulnerability is behavioural rather than informational. Older generations are disproportionately affected by authority-based phishing and PSP impersonation, despite relatively high awareness. Younger generations—particularly Gen Z—display high digital confidence that is not matched by awareness or outcomes, making them vulnerable to platform-embedded and incentive-driven fraud in fast-paced, financially pressured contexts. The generational divide in fraud vulnerability can, thus, be seen to be driven less by what people know about fraud, and more by how they act under pressure in real-life situations.

Insights from Figures 1–3, the scenario illustrations, and the Deloitte Global 2025 Gen Z and Millennial Survey converge on a single conclusion: effective fraud prevention cannot rely on uniform awareness raising. It must instead adopt generation-specific, behaviour-centric strategies that reflect how different cohorts allocate trust, interact with technology, respond to incentives, and make decisions under pressure in real-world fraud situations.

4. Is there a gap with institutional support?

Although 45% (450 respondents) have experienced fraud as a result of a general inquiry, the institutional infrastructure seems to fall short of their needs. Institutional support includes support from all the payment ecosystem participants (governments, regulators, law enforcement, national security agencies, payment service providers, telecom and technology providers, social media platforms, and others).

Additionally, among those 510 respondents who are identified as victims in the real-life payment scenarios, 33% or 170 respondents had already experienced fraud, indicating fraud is still recurring. Moreover, 42% (420 citizens) felt unsupported when dealing with incidents, undermining the essential trust required for effective fraud prevention.

This gap in institutional support is evident across four interconnected areas:

- Regulatory awareness: 54% of respondents are unaware of the protections available to them
- Reporting accessibility: 45% do not know where to report
- Fraud prevention training: 70% have never undergone formal training on fraud prevention
- Victim support: 42% of victims felt unsupported during their experience

While these statistics highlight current gaps in institutional support, they more importantly illuminate a clear path forward. Addressing these areas is not simply about correcting shortcomings, it is a strategic opportunity to build a more resilient fraud prevention ecosystem. This requires a collaborative approach centred on innovation in customer experience design, proactive intelligence sharing between institutions, and transforming the customer experience from a point of friction into a source of trust and resilience.

a. Knowledge and awareness gaps: Regulatory rights and fraud recognition

A fundamental disconnect seems to exist between regulatory intent (current and upcoming) and respondent understanding. Despite robust European frameworks, such as the Payment Services Directive (PSD2) which establishes clear liability rules, and the upcoming Payment Services Regulation (PSR) which introduces new protections, **54% of respondents remain unaware of the payment regulations designed to protect their identity and financial interests.**

This awareness gap has cascading consequences. When respondents do not understand their rights, they are unable to advocate for themselves when victimised. They may accept financial losses they are legally entitled to recover, hesitate

to report fraud due to a mistaken belief that they bear full responsibility, and lose confidence in the institutions.

The training gap compounds this problem: although 54% of respondents express confidence in recognising fraudulent communications, **70% have never undergone formal training**. The discrepancy between perceived and actual capability is reflected in the survey scenarios, where **31% were deceived by sophisticated vishing attacks (scenario 1) and 25% of respondents fell victim to phishing attacks despite initial suspicion (scenario 2)**. The gap is particularly acute among vulnerable populations: baby boomers and Gen X are both the least informed and most frequently victimised, with 65% and 48% respectively declaring themselves unaware of regulatory protections.

Empowering citizens with accessible knowledge about how these protections function can contribute to bridging the gap between regulatory intent and actual consumer protection, particularly before citizens become fraud victims.

b. Accessibility and response gaps: Reporting and victim support

The survey also highlights a significant lack of knowledge about how to report suspected fraud: **45% of all respondents do not know where to report or whom to contact**. Among respondents who have experienced fraud, only 66% actually reported the incident, leaving one-third of fraud cases unreported.

This reporting gap has systemic consequences. Unreported fraud remains invisible to authorities and to the payment ecosystem participants, allowing fraudsters to operate with reduced risk of detection. As a result, aggregate fraud patterns go unidentified, and victims suffer in silence without access to recovery mechanisms.

Regarding victim support, the survey reveals that among the 66% of respondents who reported fraud incidents, **42% felt unsupported**. Victims reported extended processing times, complex procedures requiring repeated provision of information, long waits without case updates, and insufficient communication about resolution timelines. While institutions have procedures in place, from the victims' perspective these processes often feel cold, bureaucratic, and indifferent to their distress.

Key finding

These gaps are not inevitable as they reflect institutional choices about resource allocation and customer experience design. While many institutions are making substantial efforts to prevent fraud and support victims, by identifying where support infrastructure falls short, institutions can identify concrete opportunities to rebuild respondent confidence and strengthen Belgium's overall fraud resilience. The path forward requires integrated action across awareness, accessibility, and victim care.The path forward requires integrated action across awareness, accessibility, and victim care.

5. Trust in entities

Trust is the currency of the financial system. However, the survey reveals significant deficits in confidence in regulatory bodies and the payment ecosystem participants. Although respondents expect institutions to protect them from fraud, figures indicate a lack of confidence that institutions can actually do so.

The implementation of robust reimbursement mechanisms, particularly for victims of PSP impersonation fraud, as increasingly mandated by regulatory frameworks like PSR, offers a critical pathway to restore this trust and demonstrate tangible protection. However, reimbursement is only one component of a broader ecosystem-wide approach. Today, regulation is too narrowly focused on one part of the chain (e.g., banks and payment institutions), whilst the scope should cover all parties. It is crucial to recognise that effective fraud prevention requires shared responsibility across the entire ecosystem, which means implementing fraud protection mechanisms beyond the payment service providers. Fraudsters systematically exploit weaknesses across multiple touchpoints—from PSP impersonation via phone calls to fake payment interfaces. A comprehensive approach should involve all ecosystem participants, including telecom providers, technology platforms, and others who control channels used in fraud attacks. We should also not discount the responsibility of the consumer to undertake the necessary precautions, apply critical thinking, and fulfil their obligations.

Through coordinated action, information sharing, and collective accountability trust can be restored, and consumers can be adequately protected against increasingly sophisticated fraud techniques.

The trust crisis is evidenced by the following results:

- 72% of respondents do not trust regulatory bodies to protect their data against cyber threats
- 45% do not trust financial institutions to do the same
- 78% feel stressed and worried about AI-enabled fraud
- 51% believe they are not responsible for preventing fraud, indicating a potential disconnect in perceived roles and responsibilities

This discrepancy between expectation and trust is not inevitable; rather, it highlights key areas for improvement, including communication, transparency, and victim support. Trust can be rebuilt through demonstrated competence, transparent communication, and consistent action.

a. Institutional competence and transparency: Regulatory bodies and financial Institutions

Regulatory bodies play a critical role in the fraud prevention ecosystem, setting regulatory frameworks, enforcing compliance through supervisory authorities (FSMA, NBB), coordinating national fraud prevention initiatives, and providing law enforcement response.

Yet 72% of survey respondents report low or medium confidence in regulatory bodies' ability to perform these functions effectively. This statistic could be explained by the following factors: current (and upcoming) regulatory frameworks have become increasingly complex (PSD2, PSR, GDPR, DORA, NIS2), regulations often lag fraud evolution due to unprecedented technology evolution, and most fundamentally, respondents are simply unaware of the fraud prevention efforts that the government is undertaking.

Similarly, **45% of respondents have low or medium trust in financial institutions to protect their data against cyber threats**. This trust deficit reflects multiple institutional pitfalls: data breaches have undermined confidence in institutions' ability to protect data, inadequate fraud prevention (45% of respondents experienced fraud, 33% of attempts were successful), poor victim support, insufficient communication about security measures, perceived responsibility shift, AI fraud concerns, and lack of transparency about what security measures are actually in place. However, upcoming regulatory changes, such as those within PSR, are set to significantly alter the landscape by mandating reimbursement for victims of certain types of fraud.

This shift toward greater financial institution responsibility for customer losses, particularly in cases of PSP impersonation fraud, is a crucial step toward rebuilding trust and demonstrating tangible victim support. However, it should not end there and also include other players in the payment ecosystem. It is not effective to only focus on the last mile in the fraud chain. Collaboration between law enforcement, financial institutions, and supervisory bodies enables earlier detection of fraudulent activity and increases the likelihood of interrupting suspicious transactions before completion. Enhanced data exchange between competent authorities can facilitate more timely intervention. The strategic focus on payment fraud within the judicial system, including continued efforts to streamline procedures and improve the recovery of illicit proceeds, strengthens enforcement effectiveness.

These trust deficits have concrete consequences: respondents are less likely to report fraud if they do not believe government, law enforcement or the payment ecosystem participants will respond effectively, fraud goes undetected, and fraudsters remain active.

b. Expectations, responsibility and emerging threats: The trust responsibility and AI anxiety

The prevailing trust deficits in both government and financial institutions set the stage for a broader challenge: the gap between public expectations and the realities of fraud prevention responsibilities. Understanding how these perceptions influence attitudes toward accountability and emerging threats, such as AI-enabled fraud, is essential to addressing the root causes of distrust and enhancing overall fraud resilience.

On this matter, the survey reveals a critical gap exists between expectation and reality: 53% of respondents believe they are not solely responsible for preventing fraud, expecting institutions (e.g., government, policy) or other parties (e.g., banks, insurers) to bear the primary responsibility. This expectation is an ideal target which cannot be met as no institutions or third parties can prevent 100% of fraud. Some fraud schemes require respondent vigilance to recognise and resist, some exploit vulnerabilities in human psychology that no technology can fully address, and some can be so sophisticated that even well-trained, vigilant respondents can fall victim. Yet when fraud occurs, as it inevitably will, respondents feel betrayed, and their trust erodes. The generational breakdown highlights differences: baby boomers and Gen X tend to attribute responsibility to the victim more easily than millennials and Gen Z. Interestingly, in relation to the second scenario of the survey, 24% of Gen Z respondents indicated that they did not know who holds the responsibility.

Anxiety about AI-enabled fraud is also a notable factor: 78% of respondents feel stressed and worried, yet 55% are unaware of AI-enabled fraud techniques, and 52% believe insufficient attention is being paid to this threat. **This paradox of low awareness and high anxiety fuels irrational fear and distrust.**

Key finding

The trust crisis facing the financial system is a permanent challenge to be addressed. It demonstrates that significant efforts will continue to be needed in the areas of communication, transparency, and victim support. By demonstrating competence, maintaining transparent communication, and taking coordinated action, the payment ecosystem participants can rebuild trust and enhance system resilience. It is also time that all players in the ecosystem are alerted to their responsibilities, not just the banks.

VI. The path forward: A unified approach

Drawing from the key findings of our research, we have outlined several actions that could be considered by stakeholders to reduce payment fraud and increase the resilience of the payment ecosystem. We fully acknowledge the extensive fraud prevention controls already in place, the regulatory landscape governing the payment transactions, and the initiatives to increase awareness among citizens, and understand that many stakeholders are actively working on these stream aspects to reduce the challenges facing citizens. In some cases, our suggested actions align with and reinforce initiatives already underway.

a. The imperative for unified ecosystem action

The fragmented approach to fraud prevention, where individual institutions, because of current regulatory restrictions, operate independently without shared intelligence, creates critical vulnerabilities that fraudsters systematically exploit operating simultaneously across payment channels, telecom networks, and social media platforms. Yet, without a coordinated approach individual institutions find themselves limited in detecting patterns or preventing fraud at scale.

International examples demonstrate that cross-sector collaboration, involving regulators, governments, financial institutions, telecom operators, and social media platforms, enables real-time threat detection and collective response that individual actors cannot achieve alone. The shift from fragmentation to coordination requires that all ecosystem participants create a unified approach as neither technology nor regulation alone can succeed, but coordinated action across all stakeholders creates layered defences that operate continuously against increasing fraudster sophistication. This unified approach transforms fraud prevention from an institutional burden into a systemic capability.

b. Blending human vigilance with automated defence

The path forward requires a fundamental shift in strategy from the payment ecosystem participants. We need to evolve the traditional awareness, blend human vigilance with automated defences, and build a resilient support infrastructure beyond technology.

While some of these solutions are already widely adopted across the ecosystem, this requires participants to continue investing and implementing automated, multi-layered defences that operate in real time and do not rely solely on human judgment under the pressure of a scam, via:

Real-time AI-powered transaction monitoring

- Share early fraud signals from social media platforms or telecom messages
- Share fraud intelligence across ecosystem stakeholders
- Detect payment anomalies through behavioural analysis
- Analyse customer behaviour and historical payment trends
- Monitor user interactions with devices (keystroke, mouse, touchscreen patterns)
- Flag suspicious activities and require human validation before payment completion

Advanced verification systems

- Bot detection and behavioural biometrics
- Authentication challenges and redirects
- Device intelligence (device identifier, IP, reputation, patch level, malware detection, geolocation)

Automated alerts and transaction controls

- Real-time alerts for suspicious activity
- Transaction limits and withdrawal limits, potentially aligned across all institutions in a uniform way
- Flagging and blocking of fraudulent payments with human validation

c. Trusted digital identity and authentication

Financial institutions, governments, employers, and citizens must adopt reusable, trusted digital identity solutions that enable secure, high-assurance onboarding and authentication without repeated identity proofing. This supports regulatory compliance (e.g., AML, PSD2/3) and reduces identity theft risks. Strengthening password management and mandating multi-factor authentication (MFA) across all accounts is essential to build a robust security foundation.

d. Enhancing human defence and traditional awareness

Traditional awareness campaigns are insufficient against increasingly sophisticated AI-enabled attacks and social engineering. Tailored education programmes should address generational differences in fraud risk and behaviour, helping citizens, employees, and customers recognise and respond effectively to threats. This includes pairing critical thinking with knowledge of the security protections they have access to. Employers and communities play a key role in delivering generation-specific training and fostering cross-generational learning.

e. Bridging the generational and behavioural divide

Messaging and controls should be tailored to generational trust patterns and behavioural risks, addressing overconfidence in younger users and authority bias in older cohorts. Encouraging personal delay rules, independent verification, and recognising urgency or secrecy as red flags empowers citizens to act prudently and report suspicious activity promptly.

f. Improving support systems and reporting

Victim support must be accessible, inclusive, and victim-centric, with clear multi-channel reporting mechanisms and rapid response frameworks. Many victims currently feel unsupported, and reporting rates remain low. Simplifying fraud reporting through one-click options and providing immediate feedback can bridge the gap between awareness and action, encouraging timely reporting and intervention.

g. Regulatory coordination and transparency

Governments and regulators should consider fostering collaboration with all the ecosystem participants to deploy advanced fraud detection technologies such as AI and behavioural biometrics. Collaboration between law enforcement, financial institutions, and supervisory bodies enables earlier detection of fraudulent activity and interrupts suspicious transactions at an early stage. Enhanced data exchange between competent authorities facilitates timely intervention, while the judicial system's strategic focus on payment fraud, including streamlined procedures and improved recovery of illicit proceeds, strengthens enforcement. Transparent communication of fraud trends, enforcement actions, and prevention efforts build trust. Regulatory frameworks like PSR will increase institutional responsibility for fraud losses and mandate victim reimbursement for some fraud scenarios, reinforcing ecosystem accountability. PSR will also harmonise requirements to remove limitations linked to data sharing enforced by GDPR's strict data protection provisions and instant payment obligations.

What remains to be clarified is the scope of responsibility of social media platforms, including specific protection requirements and liability obligations with regards to fraud, aligned with their role in the fraud chain.

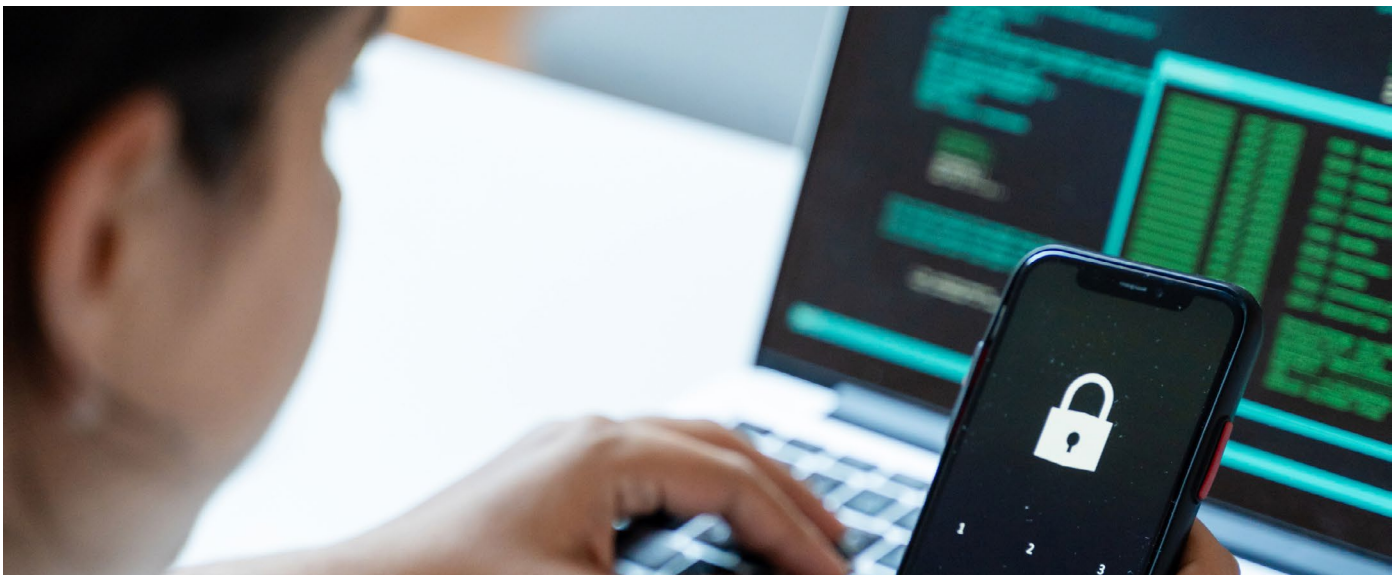
The bottom line

If payment fraud is not addressed proactively, its negative consequences are likely to intensify. The potential costs—ranging from financial losses and diminished trust to reduced system resilience—are likely to outweigh the investments needed to enhance the security of the payment ecosystem.

Stakeholders across the payment ecosystem are encouraged to build on existing efforts by adopting a more proactive, automated, and collaborative approach to fraud prevention. Incremental improvements may no longer be sufficient. Belgium's payment system would benefit from accelerating the fundamental shift, where awareness-based defences work hand in hand with human vigilance, automated defence mechanisms, meaningful customer support, governmental fraud protection programmes, and other actions linked to the full ecosystem.

By working together across the ecosystem, starting from the first fraud message to citizen support, stakeholders can help preserve the trust that is essential to the stability of the payment ecosystem.

This study was not designed to prescribe a single path forward, but rather to raise critical questions about what more can be done to address this increasingly complex fraud challenge. The evidence and insights presented here are based on the survey described earlier and provide a basis for a dialogue for the ecosystem participants to decide the way forward in alignment with existing regulations and safeguarding resilience against fraud.



VII. Methodology appendix

1. Research dimensions

We examined the following five critical dimensions:

1. Awareness and behaviour: Understanding how Belgians recognise and respond to fraud threats
2. AI-driven threats: Emerging risks from artificial intelligence-enabled fraud techniques
3. Security practices: Current adoption of protective measures and digital hygiene
4. Trust and expectations: Confidence in financial institutions and regulatory bodies protection
5. Institutional measures: Knowledge of regulations and reporting mechanisms

2. Survey design and sample

iVOX ensured the sample was nationally representative through the following quotas:

- **Age:** Almost balanced across three decennial segments (26% < 34 years, 32% < 35-54 years, and 41% > 55 years)
- **Generations:** Baby boomers (1946-1964) (N = 355/1000), Generation X (1965-1980) (280 = XX/1000), millennials (1981-1996) (235 = XX/1000), and Generation Z (1997-2012) (N = 130/1000)
- **Gender:** 52% female, 48% male
- **Language:** 44% French-speaking, 56% Dutch-speaking
- **Social grade** (represented by education levels): 62% with 'At most upper secondary education' and 38% with 'Higher education'

3. Scenario testing

Two real-life fraud scenarios were tested with respondents:

- Vishing attack: Voice phishing impersonating police
- Phishing attack: QR code fraud impersonating internet service provider

4. Lexicon

In this survey, the fieldwork and the dataset are specified as below:

Fieldwork:

Instead of inviting all the selected people at once and collecting the data within a few hours, iVOX uses micro-sends spread out over an entire week (or at least a few days). This ensures that no particular psychological or psychographic profile is overrepresented in the final sample. By spreading the sample throughout the day, across days, weekends, and weekdays, iVOX can best guarantee a sample that is not only representative of hard socio-demographic factors but also a cross-section of the targeted population on more difficult-to-measure aspects.

In addition, iVOX uses a proportional stratified random sample, in which different subpopulations are invited to participate in the study on the basis of a random selection. Using propensity scores based on historical data, iVOX knows the response rate of all individuals and subgroups in the panel and can predict how many people per subgroup should be invited to achieve a perfectly filled sampling frame that best represents the target group.

Dataset: Once all the data has been collected, iVOX applies weighting to ensure that the sample matches the population 100% on several variables recorded together with the client. For this, iVOX uses official figures from the CIM and Statbel (Centrum voor Informatie over de Media).

For example, in a sample of Belgians, the standard interlaced weighting is applied to the variables language, gender, and age (18-34, 35-54, 55+), and the non-interlaced weighting is applied to the variable education (diploma). Interlaced weighting ensures that within each of these variables, the sample is still representative of the other Belgians. Specifically, when focusing on women within the sample of Belgians, this group of women is still representative by age. iVOX uses a maximum weighting of 3. This can be reviewed in consultation with the client.

This method's strength lies in its ability to capture the complexity of socio-economic realities, ensuring a more accurate analysis of the usage of payment solutions, fraud and security. While it is difficult to assign a fixed description to each group due to the variety of scenarios possible, the use of this framework allows us to draw meaningful conclusions about how different segments of society experience payment fraud and payment resilience.

VIII. Bibliography

- PSD3: https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2023/0210(COD)
- e_IDAS 2.0: https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng
- Deloitte Global 2025 Gen Z and Millennial Survey
- Deloitte Behaviour FIRST Framework
- https://www.belganewsagency.eu/phishing-netted-fraudsters-nearly-50-million-euros-in-belgium-in-2024
- https://febelfin.be/en/publications/2025/if-it-smells-phishy-it-probably-is
- https://www.biocatch.com/press-release/france-loses-billions-to-fraud-every-year

IX. Colophon

This report has been set up by :

Kasper Peters
Partner
Strategy, Risk & Transactions
kapeters@deloitte.com

Nicolas Georlette
Partner
Technology & Transformation
ngeorlette@deloitte.com

Andrea Radu
Partner
Cyber, Technology & Transformation
andrearadu@deloitte.com

Georges Gehchan
Director
Cyber, Technology & Transformation
ggehchan@deloitte.com

Jordan Brasseur
Director
Strategy, Risk & Transactions
jbrasseur@deloitte.com

Laurent Culot
Director
Strategy, Risk & Transactions
laculot@deloitte.com

Stephanie Baele
Director
Human Capital, Technology & Transformation
sbaele@deloitte.com

Jonas Tombeur
Industry Advisor
Growth, Clients and Industries
jtombeur@deloitte.com

Nivine Rawas
Manager
Cyber, Technology & Transformation
nkhalifehrawas@deloitte.com

Roos Klaver
Manager
Human Capital, Technology & Transformation
roklaver@deloitte.com

Raffaele Minicozzi
Senior Consultant
Cyber, Technology & Transformation
rminicozzi@deloitte.com

Oscar Alexander
Business Analyst
Technology & Transformation
oalexander@deloitte.com

X. Glossary

Phishing: Phishing is a broader form of cyber fraud where attackers use fake emails, websites, messages, or other digital communications to deceive individuals into providing confidential information like passwords, credit card numbers, or login credentials. It often involves fake websites or links that look legitimate.

Multi-vector phishing: Multi-vector phishing is a sophisticated phishing attack where attackers leverage multiple channels or techniques in a coordinated manner (i.e., simultaneously or in sequence) to compromise a target. As an example, in a multi-vector phishing, attackers combine methods such as email, text (smishing), voice calls (vishing), and malicious websites to confuse the victim and bypass traditional defences.

Vishing: Vishing (voice phishing) is a type of scam where fraudsters use phone calls or voice messages to impersonate legitimate organisations (such as banks, police, or service providers) to trick individuals into revealing personal, financial, or security information. The goal is often to gain access to bank accounts or sensitive data.

Multi-factor authentication (MFA): Security system requiring multiple forms of verification before granting access to accounts.

Authorised push payment (APP) fraud: Fraud where victims are manipulated into authorising payments to fraudster-controlled accounts.

Behavioural biometrics: Authentication method analysing unique patterns in user behaviour (keystroke, mouse movement, touchscreen interaction).

Device intelligence: Security assessment of device characteristics including identifier, IP address, reputation, patch level, malware status, and geolocation.

Gross negligence standard: A safeguard in the Payment Services Regulation (PSR), the gross negligence standard ensures that consumer protections do not undermine incentives for personal vigilance. Under this standard, reimbursement may be denied only in cases where the consumer has acted with gross negligence—such as deliberately ignoring obvious fraud warnings, deliberately sharing security credentials with unauthorised parties, or consciously disregarding clear indicators of fraud—rather than in cases of sophisticated social engineering or psychological manipulation.

Payment service provider (PSP) impersonation fraud: The Payment Services Regulation establishes a strict liability regime for PSP impersonation fraud. When a consumer is manipulated by a third party pretending to be an employee of their payment service provider using the PSP's name, email address, or telephone number unlawfully and this manipulation results in fraudulent authorised payment transactions, the PSP must refund the consumer the full amount of the fraudulent transactions. This reimbursement obligation is mandatory and has no cap, regardless of the transaction amount. However, the consumer must meet three critical conditions: (1) report the fraud to police without any undue delay after becoming aware of it, (2) notify the payment service provider of the fraud, and (3) file an official police report.

Deloitte.