Overexposed

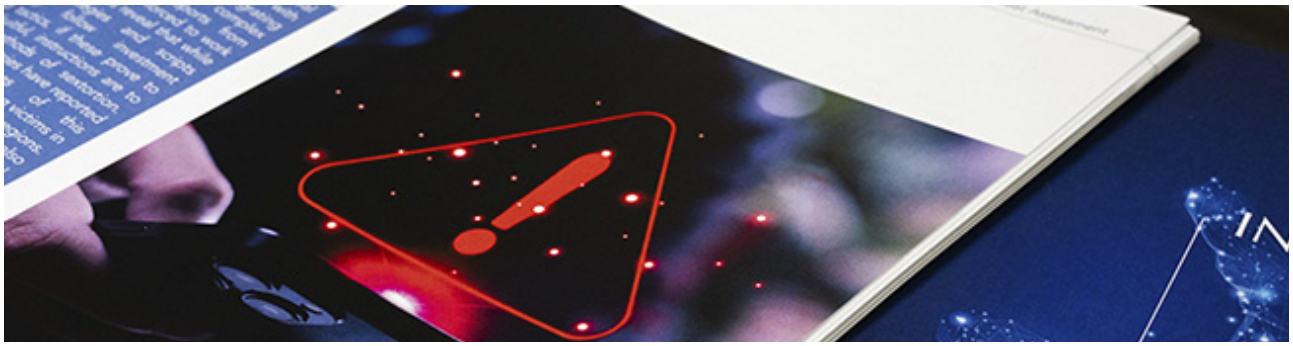
How fraud is reshaping behaviour and trust in North America

LSEG RISK INTELLIGENCE

Contents

LSEG RISK INTELLIGENCE

Introduction



North Americans stand out globally for their acute awareness of fraud risk. They are more likely than consumers in other regions to say scams are increasing sharply, and many describe themselves as well educated about how to protect against them. Yet this awareness is not translating into safety. Consumers in the US and Canada report higher rates of personal targeting, some of the most intense emotional fallout after being scammed, and near-universal changes in how they pay, share information and trust others.

As part of LSEG Risk Intelligence's research on global fraud, our North America report explores how financial scams are reshaping trust, behavior and emotional wellbeing in North America, with a focus on consumers in the US and Canada. Drawing on a survey of 4,000 people, it examines perceived scam trends, personal exposure,financial losses, and the growing role of AI-enabled fraud.

Respondents were asked about the types of scams they encounter, how often they are targeted, how much money they lose, and how these experiences affect their emotions, everyday decisions and trust in digital channels. Together, these insights provide an evidence-based view of how "overexposed" North American consumers feel to fraud and points to practical steps financial firms can take to rebuild trust.

Key Findings

01. Exposure to scams

Personal exposure in North America is higher than other regions. More than one in three adults (35%) have been personally targeted by a financial scam in the last two years, and a further 37% say someone they know has been targeted, leaving only around one in three (32%) untouched.

Exposure is particularly concentrated among younger generations. Two-thirds of Gen Z (67%) and nearly as many Millennials (65%) report that they or someone they know has been targeted, compared with just over half of Baby Boomers (52%), underlining that scams are a cross-generational challenge but with sharper pressure on younger adults.

02. Financial losses

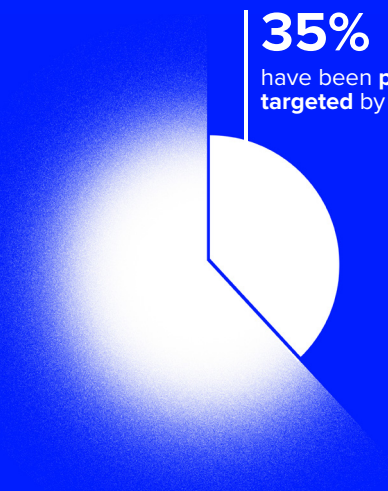
Among those who have been personally targeted by a financial scam in the past two years, around one in three (34%) have lost money, and over a third (35%) know someone who has lost money, with loss awareness slightly higher in the US (37%) than in Canada (33%).

Generational patterns show younger adults bearing more of the financial fallout: Gen Z (46%) and Millennials (42%) are more likely to know someone who has lost money than Gen X (31%) or Baby Boomers (24%), suggesting that losses concentrate in the more digitally active cohorts.

03. Impact of AI and technology

A new layer of AI-enabled scams is emerging in North America, with almost one in four adults exposed in the past 12 months to AI-generated images (23%) or AI chatbots posing as a bank, retailer or tech support service (19%).

The threat extends into voice and video: 18% report encountering a voice clone that sounded like a family member or colleague asking for urgent help, and 18% have seen a deepfake video of a known person asking them to take action, showing how convincingly personal these scams can appear.



35%

have been **personally targeted** by a financial scam.

18%

report encountering a voice clone and have seen a deepfake video of a known person asking them to take action.

LSEG RISK INTELLIGENCE

Key Findings

04.

Behavioral and emotional impact

Being scammed is reshaping how North Americans behave with money and digital channels. Among those who have lost money in the past two years, nearly all (98%) say their behavior has changed, with 45% now more cautious when making online payments and 40% more careful about where and how they share financial details.

The emotional toll is substantial: 58% of victims report anger or frustration, 36% experience anxiety or fear around money (rising to 40% in the US and 43% among women), and many also report embarrassment or shame (41%), helplessness or loss of control (32%), guilt (29%) and stress or sleep difficulties (28%), underscoring that the damage goes well beyond financial loss.

05.

Education, protection gaps and information sources

Most North Americans feel at least somewhat educated about how to protect themselves from financial scams, with nearly a third (31%) saying they are very well educated and over half (54%) somewhat educated, yet a notable minority (9%) feel poorly educated and 3% say they have not been educated at all, leaving meaningful pockets of vulnerability.

Awareness of protections and reimbursements lags significantly: while two-thirds (67%) say they are aware that protections exist, only around one in ten (13%) are fully aware of what they are entitled to, and even among those who have lost money to a scam in the past two years, just 15% say they are fully aware of their rights.

Chapter 01: Canada

Vigilant but vulnerable

In Canada, fraud is reshaping financial behavior in ways that are both practical and psychological. Consumers are alert to the threat, actively seek out information, and are especially likely to change their habits after being scammed. Yet this heightened vigilance sits alongside a significant knowledge gap about what support is available when fraud does occur, leaving many Canadians better prepared to avoid scams than to recover from them.

8 in 10

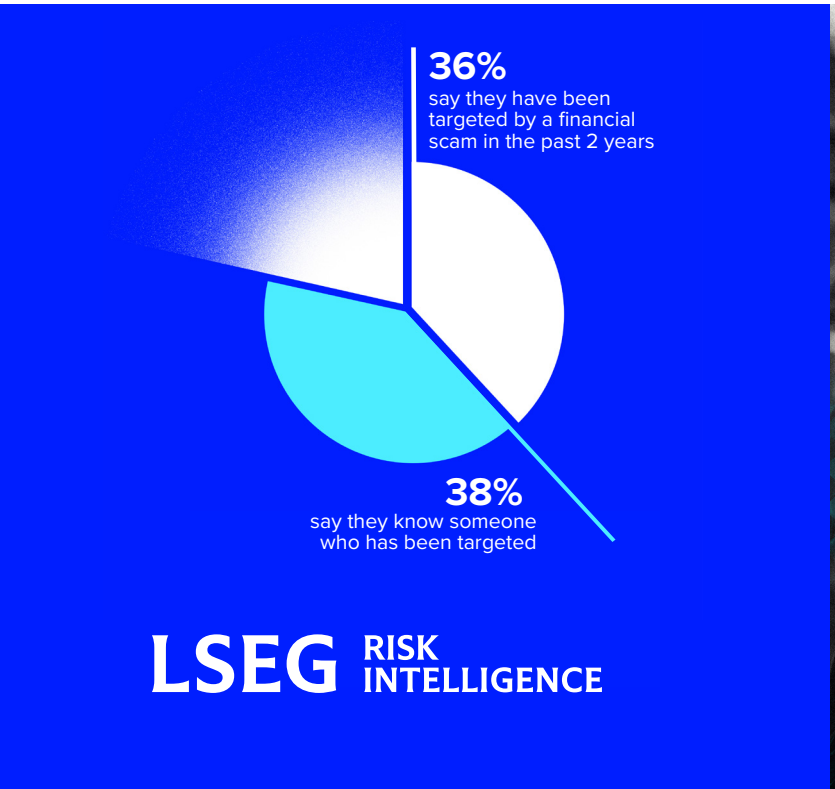
Canadians say financial scams are increasing compared with two years ago.

Among the 2,000 consumers in Canada surveyed, three key findings emerged:

Financial scams on the rise

In Canada, fraud is increasingly encroaching on everyday financial life. Eight in ten Canadians say financial scams are increasing compared with two years ago, including more than half (55%) who believe they are increasing significantly. **More than a third of Canadian adults (36%), say they have personally been targeted by a financial scam in the last two years, while 38% say someone they know has been targeted.** Only 30% report no personal or indirect scam exposure, highlighting its prevalence.

Canadians are highly aware of common scam formats, and like North Americans overall, are most familiar with phishing, payment scams and impersonation scams. But familiarity has not eliminated risk. **Almost one in five (19%) have personally lost money and one in three Canadians (33%), say they know someone who has lost money to a scam in the past two years,** showing that financial harm is not remote or abstract, but visible in people's personal networks.



Intense emotions change behavior

When scams succeed, the consequences extend well beyond money. Across North America, a majority (58%) of victims report anger or frustration, 41% embarrassment or shame, 36% anxiety or fear around money, 32% helplessness or loss of control, 29% guilt and 28% stress or sleep difficulties.

In Canada, the way these experiences translate into behavior is especially striking. Among those who have been scammed, **48% say they are now more cautious when making online payments, and 49% say they double-check the legitimacy of companies before making financial decisions. Fraud is not just creating victims; it is creating a more guarded consumer.**

Gaps highlight need for education

More than half (53%) respondents in Canada say they primarily get information about scams and how to protect themselves from news media. Across Canada, 45% also rely on banks or payment providers and 33% on government or regulatory bodies, suggesting that scam education reaches consumers through a mix of public, institutional and personal channels. Canadians appear engaged and alert, but this awareness does not always translate into confidence about what happens after a scam.

This is where one of the clearest vulnerabilities in the Canadian market emerges. Across North America, 67% say they are aware of protections, reimbursements or support services available to scam victims, yet only 13% are fully aware of what they are entitled to. In Canada, full awareness falls to just 10%. That gap between vigilance and practical knowledge is critical. Canadians are changing their habits, checking more carefully and taking fraud seriously, but many still do not have a clear understanding of how they would be supported if they lost money.

For financial institutions, regulators and brands, the challenge is not only to help Canadians spot scams earlier, but to ensure they understand what recovery pathways exist when prevention fails.

LSEG RISK INTELLIGENCE

Chapter 02: United States

Overconfident and overexposed

In the United States, fraud is pervasive and deeply embedded in consumers' day-to-day sense of financial risk. Common scam types such as phishing, payment scams and impersonation scams remain the most familiar, while emerging threats such as deepfakes and AI-generated content are adding new layers of uncertainty to how Americans judge messages, calls and online interactions.

Among the 2,000 consumers in Americans surveyed, five key findings emerged:

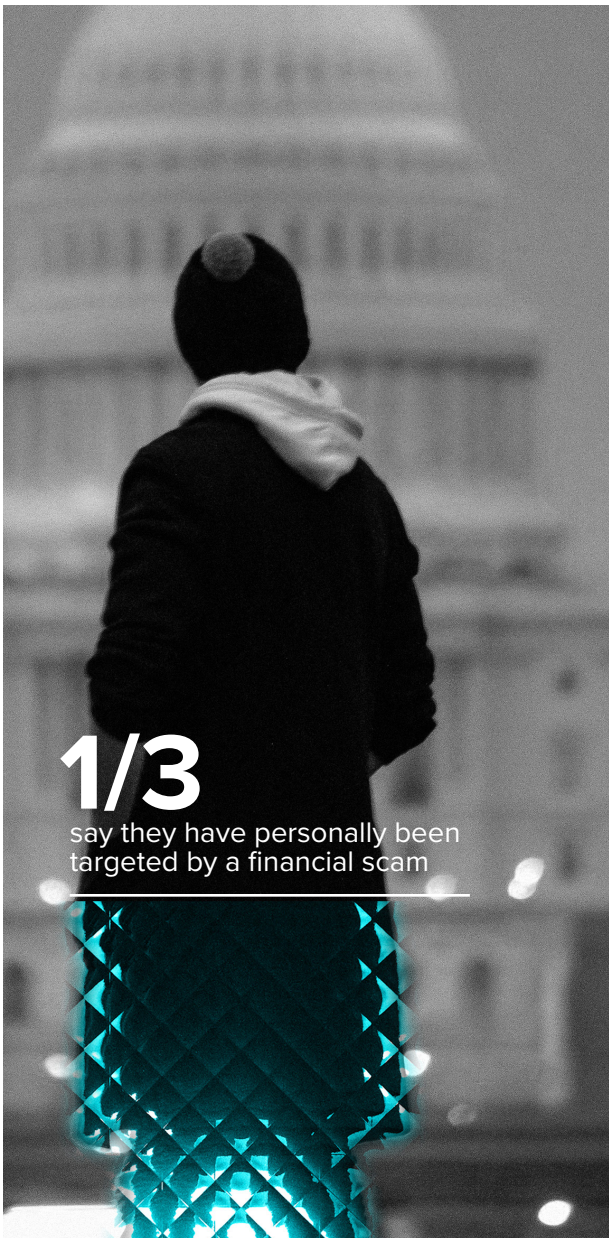
Escalating fraud hitting American's wallets

In the United States, self-reported education levels are high: the majority of adults consider themselves well or somewhat well educated about how to protect themselves from scams. Younger Americans are more likely than older ones to say they feel uneducated, suggesting that those who spend the most time online do not always feel they have the tools they need.

More than three quarters (77%) of Americans say financial scams are increasing, including more than half (53%) who believe they are increasing significantly. A third (33%) say they have personally been targeted by a financial scam in the last two years while 36% say someone they know has been targeted.

Across North America, Gen Z (46%) and Millennials (42%) are more likely to have known someone who lost money compared to their older counterparts – Gen X (31%) and Boomers (24%).

This high level of exposure is reinforced by the visibility of financial loss. In the United States, one in five (20%) admit they have lost money and more than one in three (37%) say they know someone who has lost money to a scam in the past two years.



Higher emotional toll in the US

The emotional toll of fraud is especially important in the US context. Across North America, anger and frustration are the most common reactions after being scammed, reported by 58% of victims.

But the data also shows that anxiety or fear around money and finances is particularly acute in the United States, reaching 40%. Embarrassment or shame affects 41% of American victims, while 34% report helplessness or loss of control, 23% guilt and 27% stress or sleep difficulties. These findings suggest that in the US, fraud is not just a financial event but a destabilizing emotional experience that can linger well after the loss itself.

Low awareness of newer types of scams

American consumers show strong awareness of mainstream financial scams. In the US sample, most adults recognize phishing scams (76%), payment scams (75%) and impersonation scams (69%) when prompted, and most say they know what these scams are rather than simply having heard the term.

Awareness falls away for newer or more technical formats: only about six in ten (62%) say they are familiar with deepfake scams and only about half recognize quishing scams that use QR codes to direct people to fake websites. This profile suggests that while Americans are broadly literate on traditional fraud tactics, there is still a sizeable knowledge gap around AI-enabled and QR-based fraud.

Among Americans who have been targeted by a financial scam in the past two years, phishing is by far the most common contact point, with a one in five (20%) saying they have received fraudulent emails or messages designed to steal personal or financial information. Slightly fewer (18%) report being targeted by a payment scam that looked like a routine invoice or payment request, and roughly one in ten recall an impersonation attempt by someone posing as a trusted person. A smaller but still significant proportion of respondents say they have been approached by investment scams (9%) or by scams using deepfakes (7%) and QR codes (6%).

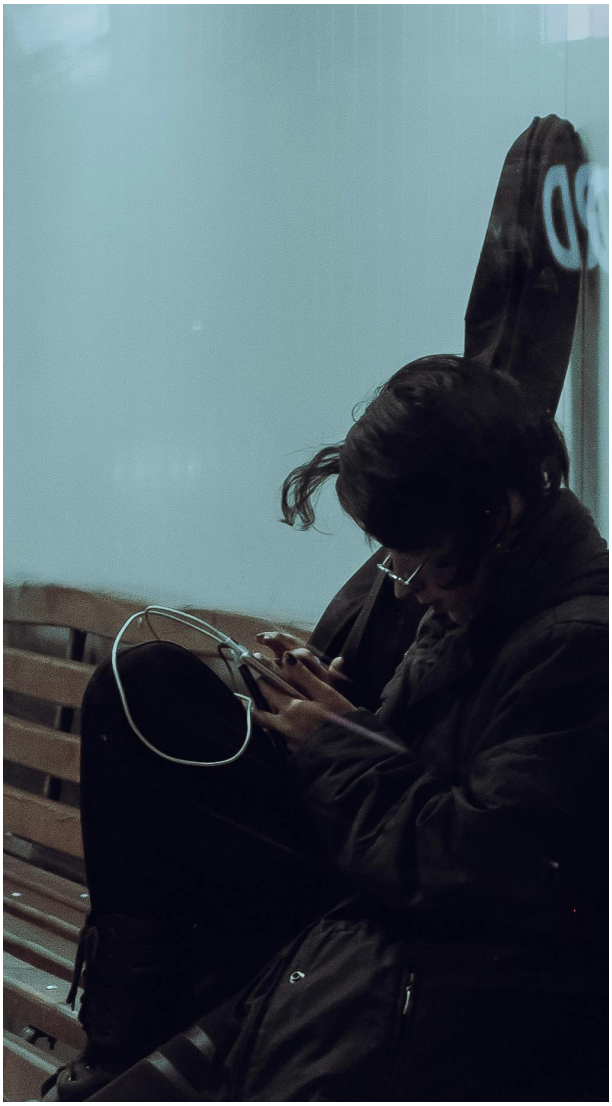
Emotional impact changes behavior

Across North America, 98% of those who have lost money to a scam say the experience changed how they behave with slightly higher impact recorded among US victims across most categories. In the US, 41% percent of consumers say they are now more cautious when making online payments, 39% are more careful about where and how they share financial details, 38% avoid certain types of transactions or channels, 38% have added extra security measures, and 36% say they have lost trust in people or companies. In the United States, this points to a market where fraud is increasingly influencing how people transact, how much they trust digital communications and how much friction they are willing to accept in exchange for safety.

Education opportunity for financial firms

Americans access scam information from a broad mix of sources. Nearly half (49%) say they primarily rely on news media, while North America-wide figures show strong use of banks or payment providers and government or regulatory sources as well. This makes the US a market with relatively high information flow, but not necessarily high clarity. Only 16% of Americans say they are fully aware of the protections, reimbursements or support services available if they are scammed and lose money. That means most consumers still lack a complete understanding of what help exists after fraud has occurred.

The US fraud story is therefore one of high exposure, emotional strain and incomplete reassurance. Fraud is seen as rising, losses are socially visible, and the psychological effects are substantial. Consumers are adapting, but they are doing so in an environment where confidence is being eroded faster than support is being understood. For organizations operating in the US market, that makes rebuilding trust just as important as preventing the next scam.



Conclusion

Financial scams are a growing concern across North America, with most consumers believing scams are increasing and many saying the rise is significant.

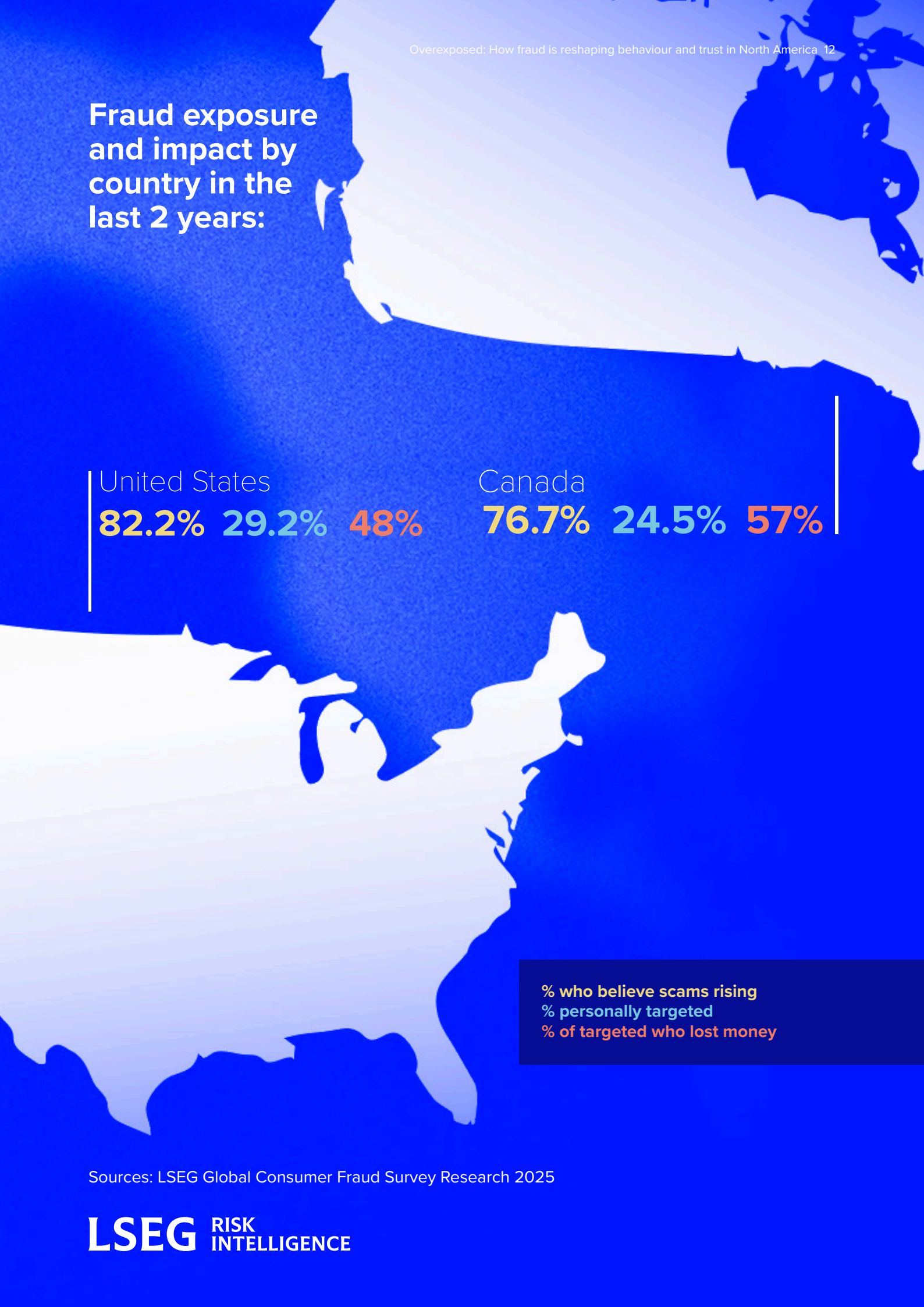
Personal exposure is high, with over a third having been directly targeted in the past two years, and younger generations more likely to report direct or indirect exposure.

Phishing, payment and impersonation scams remain the most common across the region. While phishing is widespread, it tends to result in lower financial losses, whereas payment and investment scams carry a higher risk, particularly for younger adults. At the same time, AI-enabled scams are becoming more visible, with growing exposure to AI-generated images, chats, voice clones and deepfake videos, which is already undermining trust in everyday communication channels.

Canadians tend to be vigilant but uncertain about what happens after a loss, while Americans combine relatively high exposure and self-reported education with particularly acute emotional strain and incomplete knowledge of support options.

Overall, the research suggests that strengthening fraud prevention in North America will mean pairing consumer education with practical safeguards and better coordination across the customer journey. Markets that combine awareness with protective measures may be better equipped to respond to evolving fraud risks, reinforcing the importance of sustained vigilance – including effective detection, coordination and post-incident support – in helping to reduce the human toll of fraud and support confidence in digital payments, financial services and everyday online interactions.

Fraud exposure and impact by country in the last 2 years:



Sources: LSEG Global Consumer Fraud Survey Research 2025

LSEG RISK INTELLIGENCE

A shared responsibility

Trust plays a central role in the digital economy. Fraud incidents can undermine consumer confidence in financial services, commerce and digital communication, while effective prevention, timely support for victims and successful enforcement actions can help reinforce that trust over time.

As fraud tactics continue to evolve, so too must the responses. Scam activity is likely to remain dynamic, shaped by both technological change and human behavior. The findings from this research highlight the importance of ongoing adaptation – strengthening controls where vulnerabilities emerge and maintaining vigilance as risks shift. In doing so, organizations can contribute to reducing harm and supporting confidence in digital engagement across markets.

Taken together, the findings of our research point to several recurring focus areas for organizations seeking to strengthen their response to consumer fraud. While approaches will necessarily vary by market, the research highlights four broad areas where attention and coordination may play an important role in mitigating risk and supporting consumer confidence across North America:

01.
Prioritising areas of greatest risk

The findings suggest that integrating risk intelligence across the customer lifecycle – from onboarding through to ongoing activity – can support more responsive fraud mitigation. Approaches that combine verification, screening and account monitoring may help ensure that fraud prevention remains adaptive rather than static.

02.
Encouraging coordinated responses

Survey results underline the role of education and accessible tools in helping consumers recognize and respond to scams. Market-specific communication, informed by local risk profiles and cultural context, can support understanding of emerging threats and the safeguards available.

03.
Encouraging coordinated responses

The research points to the potential value of collaboration across sectors, including financial services, telecommunications and digital platforms. Information-sharing arrangements and cooperation between public and private stakeholders may help address gaps that fraudsters seek to exploit.

04.
Improving transparency and support

Clear communication around reporting processes, available support and reimbursement frameworks can help ensure that consumers know where to turn following a scam. Simplified pathways and consistent guidance may contribute to improved confidence and trust over time.

Appendix:

Research methodology

This research is based on an online survey of 21,000+ adults across 14 markets, conducted between early November and early December 2025. The sample was designed to provide broad geographic coverage across North America, EMEA and APAC, reflecting a range of market maturities, regulatory environments and digital adoption levels.

Sample distribution by region and market:

North America
4,000 total

United States: 2,000
Canada: 2,000

APAC
7,000 total

Australia: 2,000
China: 2,000
Singapore: 1,000
Japan: 1,000
Hong Kong: 1,000

EMEA
10,000 total

United Kingdom: 2,000
Germany: 2,000
France: 2,000
Spain: 2,000
Denmark: 1,000
Switzerland: 500
UAE: 500

Demographic groups in scope

Gen Z
Aged between 18-28 years old

Millennials
Aged between 29-44 years old

Gen X
Aged between 45-60 years old

Baby Boomers
Aged between 61-79 years old

LSEG RISK INTELLIGENCE

Appendix:

Research methodology

This report covers a wide range of scams:

Deepfakes

AI generated videos, images or audio designed to convincingly mimic real people or events.

Investment scams

Fake financial opportunities promising high or guaranteed returns.

Phishing

Fraudulent emails, texts or messages crafted to steal personal or financial information.

Impersonation scams

A fraudster pretends to be a trusted person (e.g., friend, family member, colleague) to deceive or pressure you.

Payment scams

Fraudsters send realistic looking fake invoices or payment requests to trick individuals or businesses into sending money.

Quishing

Scanning a malicious QR code that redirects to a fake website designed to steal information or install malware.

LSEG RISK INTELLIGENCE

LSEG Risk Intelligence

Your partner in the fight against fraud

LSEG Risk Intelligence provides a suite of solutions to help organizations efficiently navigate risks, limit reputational damage, reduce fraud and comply with legal and regulatory obligations around the globe. From screening solutions through World-Check, to detailed background checks on any entity or individual through enhanced due diligence reports, and innovative identity verification and account verification solutions – organizations can trust LSEG Risk Intelligence to help them manage their risk, so they can operate more efficiently, more effectively and more confidently.

To learn more, visit
www.lseg.com/risk-intelligence

LSEG RISK INTELLIGENCE