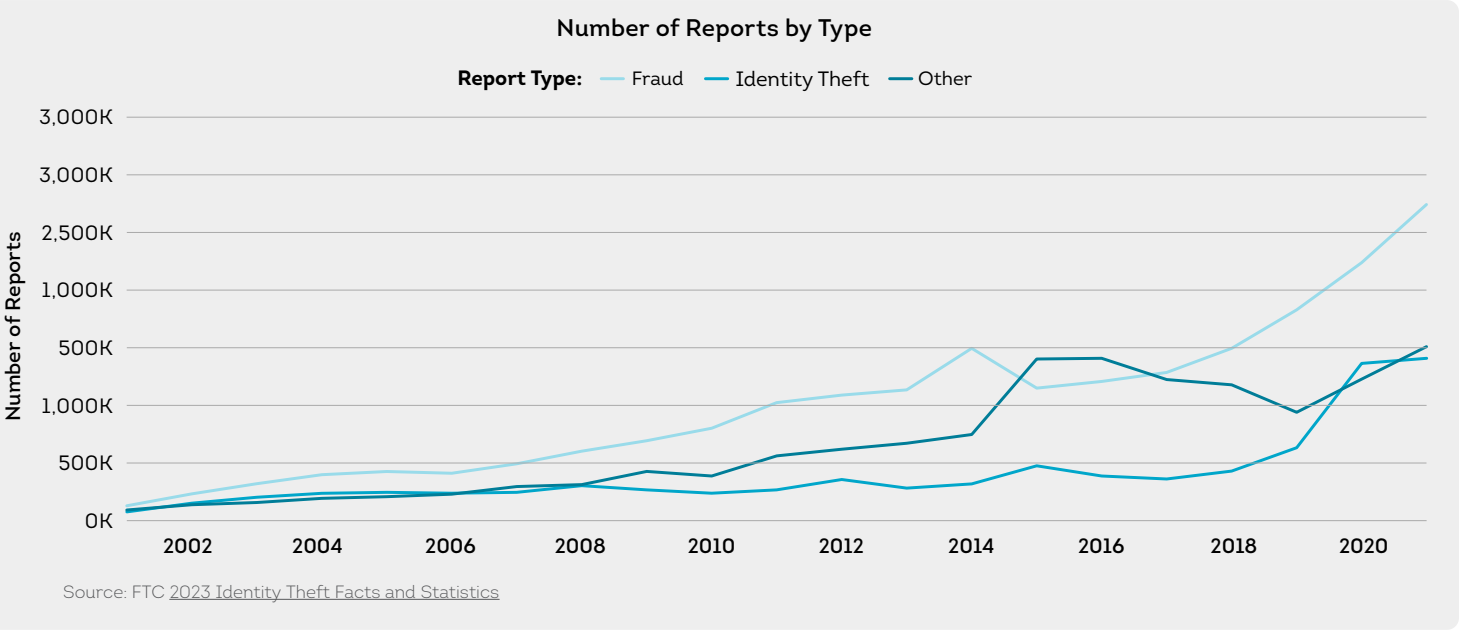
TransUnion

2023 Report

Telecommunications Consumer Report

Introduction

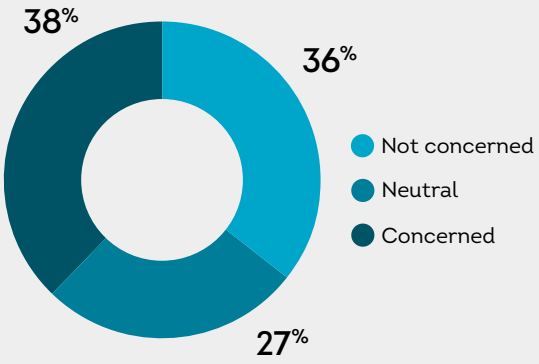
Fraud and identity theft have been on the rise since the advent of the internet – and further supercharged with the adoption of mobile and social media technologies. Since 2018, the FTC data show reports of fraud and identity theft have more than doubled across several categories. As mobile devices and digital tools become ubiquitous features of life, and new technologies are deployed at an ever-increasing rate, consumer vulnerabilities to various forms of fraud will only increase. While most consumers take steps to protect themselves against fraud attacks, they won't be able to do it alone. Securing the digital ecosystem and shielding the identities and information of consumers requires and all hands on deck approach from device manufacturers to ISPs to mobile phone carriers.



Source: FTC 2023 Identity Theft Facts and Statistics

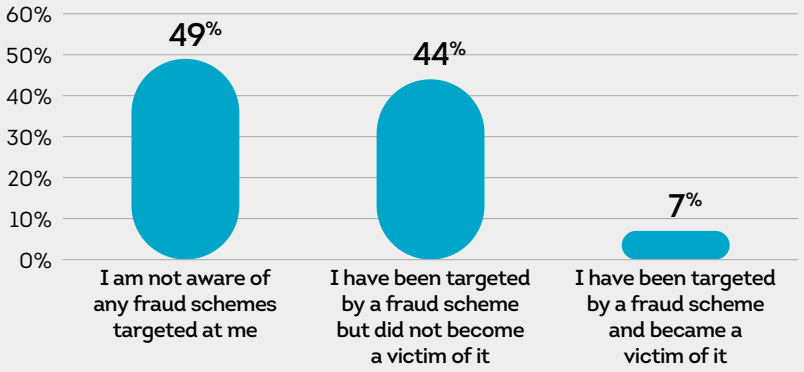
To better understand the concerns and attitudes of consumers related to fraud, as well as what steps they're taking to combat it, TransUnion conducted a survey to gain further insight into the state of fraud on mobile devices. Just over half of respondents said they've been targeted by a fraud scheme in the past three months, with 44% saying they did not fall victim to the scheme and another 7% who did. Despite the prevalence of fraud attempts, consumers were split about how concerned they should be. Thirty-eight percent of consumers said they were concerned about fraud when using their mobile devices. Another 36% said they weren't concerned, and the remaining 27% expressed neutrality. Though fraud and identity theft continue to plague consumers, attitudes remained somewhat sanguine among the population.

When using your mobile phone, how concerned are you about fraud?



Source: TransUnion Telecommunications Survey 2023
Totals may not add to 100% due to rounding

Which statement best describes your personal experience with any fraud attempts* in the last three months?

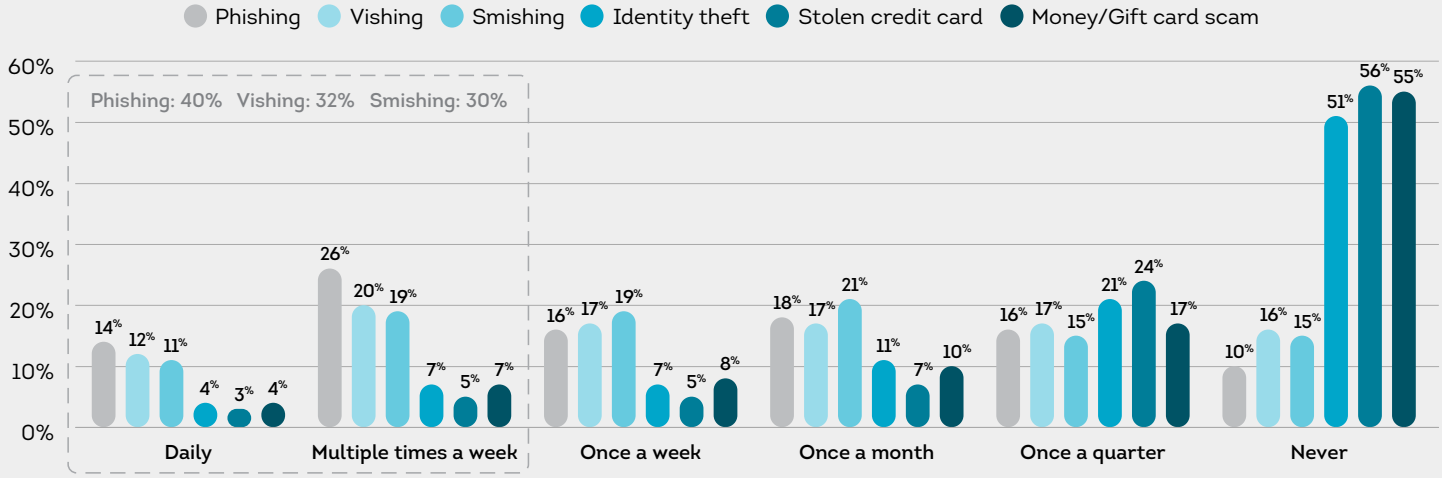


Source: TransUnion Telecommunications Survey 2023
Totals may not add to 100% due to rounding
* *Fraud attempts* encompasses online, email, phone call or text messaging fraud

GENERATIONS EXPERIENCE FRAUD DIFFERENTLY

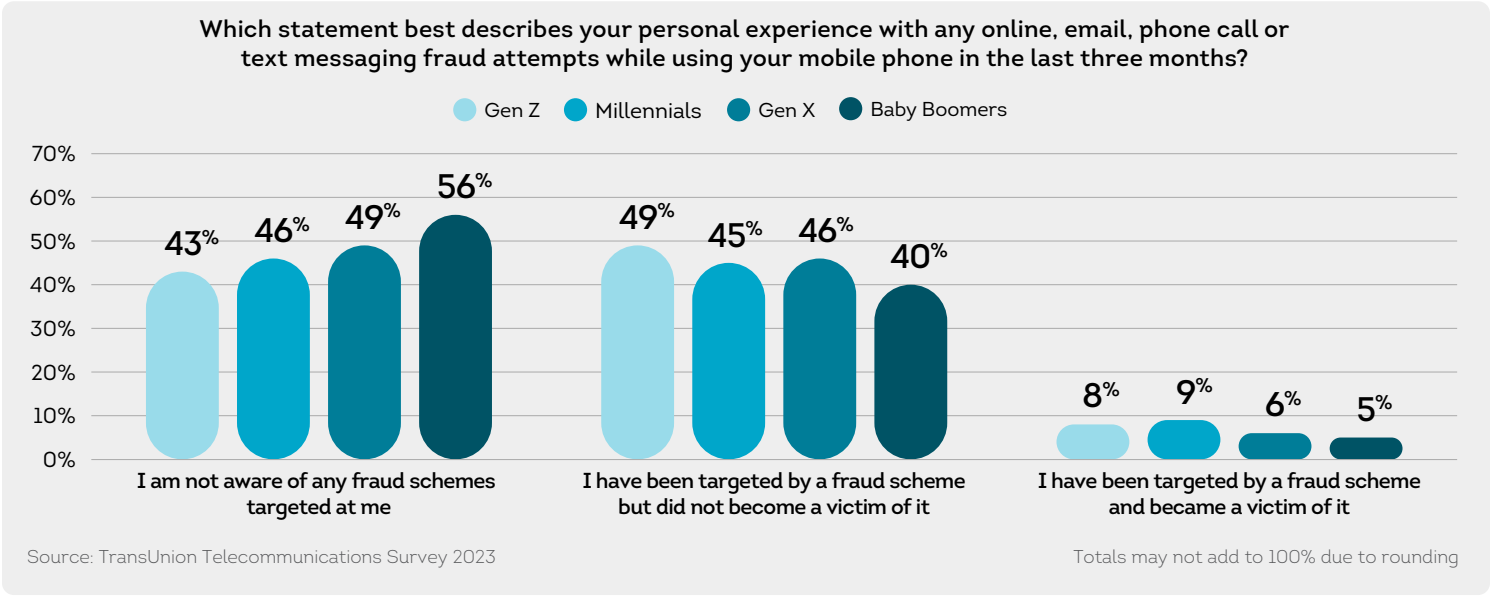
Consumers reported experiencing a wide variety of fraud attacks, though the most prevalent were phishing related. Whether using email, SMS or calls, fraudsters are attempting to get ahold of sensitive consumer data using digital communication tools. Forty percent of consumers reported they were targeted with phishing attacks either daily or multiple times a week; 32% said the same with voice (vishing) related attacks; and 30% were targeted daily or multiple times a week with SMS related fraud attempts. Considering those who experienced these types of attacks at least once per week, the figure jumped to nearly 50% across all categories. Other fraud schemes like identity or credit card theft were much less prevalent. Over half of consumers didn't experience these types of attacks, but those who did were much more likely to have encountered these types of schemes once per month or once per quarter. Fraudsters appear to be taking advantage of communication channels where they can attack at scale.

How often have you been targeted while using your mobile phone over the last three months?



Source: TransUnion Telecommunications Survey 2023

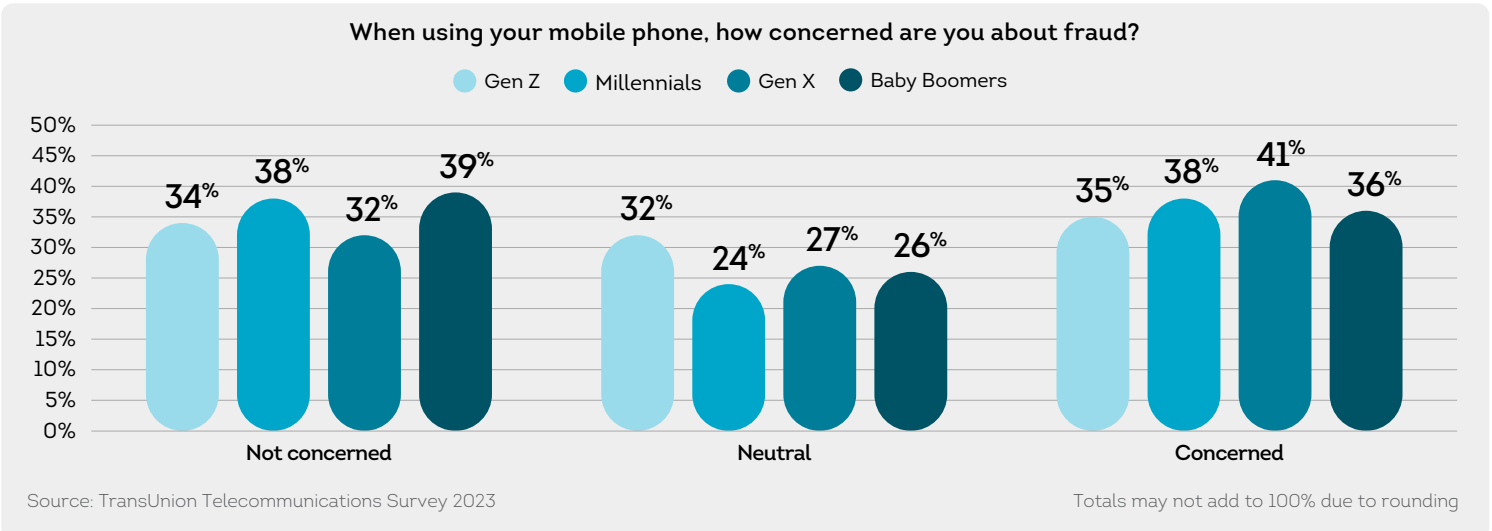
When analyzing fraud attempts across generations, we saw younger cohorts reported falling victim to fraud schemes at a higher rate than older generations. Almost twice as many Millennials (9%) reported falling victim to a fraud scheme than Baby Boomers (5%). Millennials and Gen Z may be more digitally savvy than past generations, but their higher usage of technology and greater reliance on their phones for transacting may leave them more vulnerable to fraud attempts. We noted some evidence of this when looking at fraud attempts. For example, 49% of Gen Z consumers said they were targeted by a fraud scheme but did not fall victim to it, while 40% of Baby Boomers said the same.



Source: TransUnion Telecommunications Survey 2023

Totals may not add to 100% due to rounding

Despite experiencing higher levels of fraud attacks, overall concern about fraud wasn't noticeably higher among younger generations. Millennials and Gen Z expressed similar levels of concern as Baby Boomers, while Gen X was most likely to be concerned about fraud. Awareness about different fraud schemes may have played a factor as younger cohorts deal with fraud on a frequent basis; however, lack of preparedness to take steps to combat fraud, especially among younger cohorts, may have contributed to their higher likelihood to fall victim to fraud attempts.



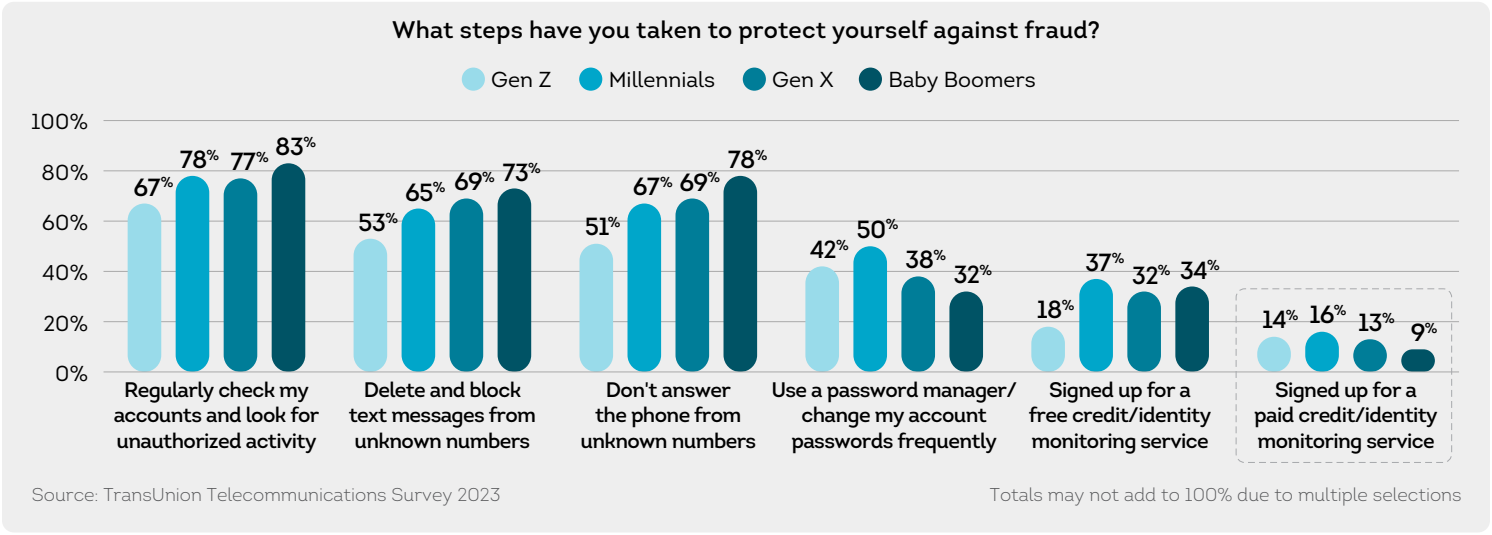
Source: TransUnion Telecommunications Survey 2023

Totals may not add to 100% due to rounding

TransUnion

CONSUMERS ARE TAKING ACTION – BUT EXPECT HELP

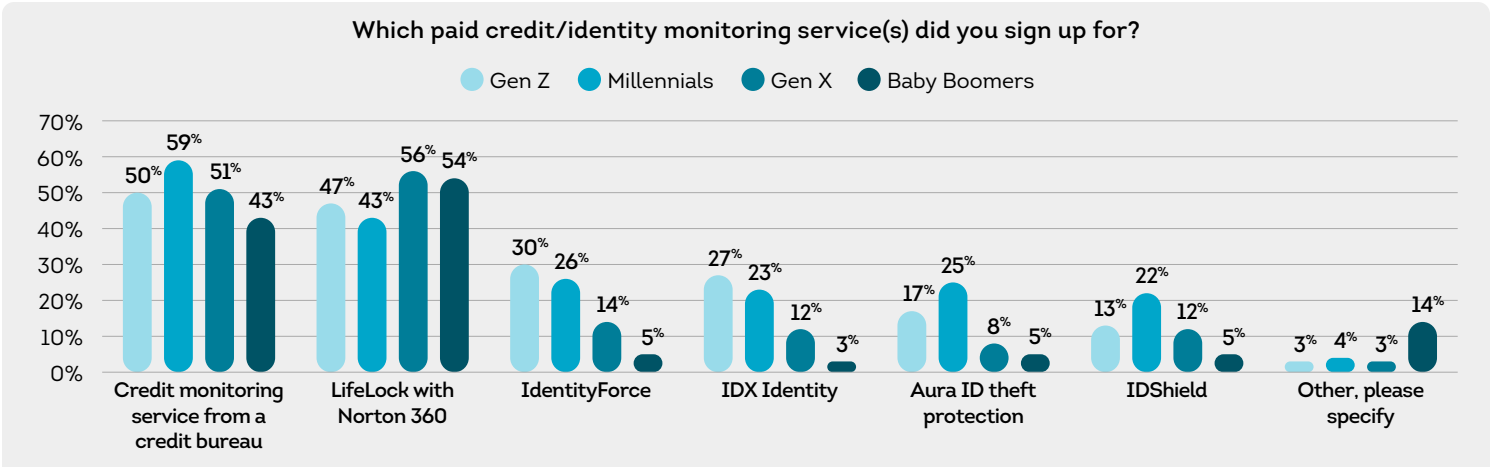
Potentially emanating from their relative lack of concern, younger cohorts were generally less likely than older cohorts to take proactive steps toward combating fraud. Gen Z consumers were the least likely generation to take action to protect themselves against potential fraud. Among all generations, regularly checking accounts and monitoring for suspicious activity was the most common anti-fraud tactic. Deleting and blocking messages, as well as avoiding calls from unknown numbers were also commonly deployed tactics for combatting potential fraud.



Source: TransUnion Telecommunications Survey 2023

Totals may not add to 100% due to multiple selections

Among consumers who signed up for a paid credit or identity monitoring service, the most popular options selected were services offered from one of the three credit bureaus or LifeLock with Norton. Younger generations were more likely to sign up for identity monitoring services with a non-traditional provider, suggesting there's room to grow among younger audiences with new and novel identity protection capabilities.

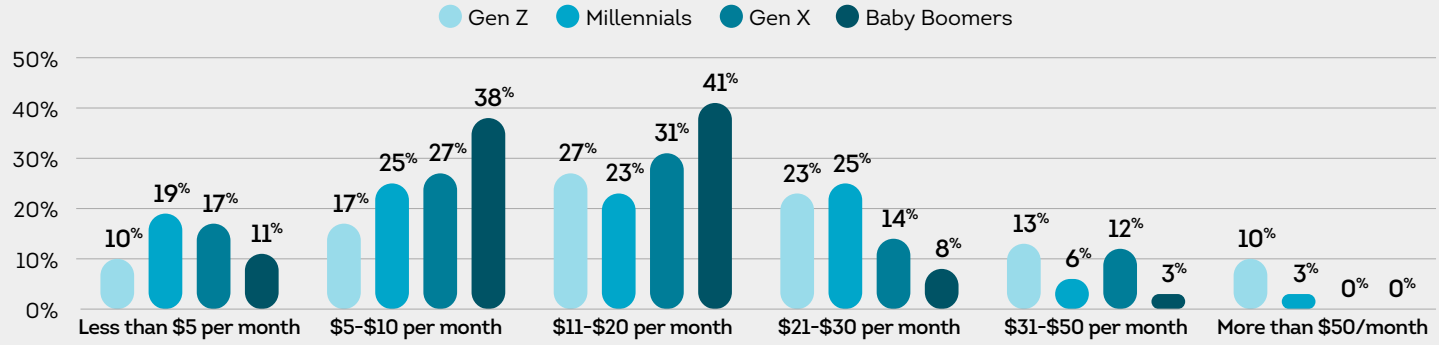


Source: TransUnion Telecommunications Survey 2023

Totals may not add to 100% due to multiple selections

TransUnion

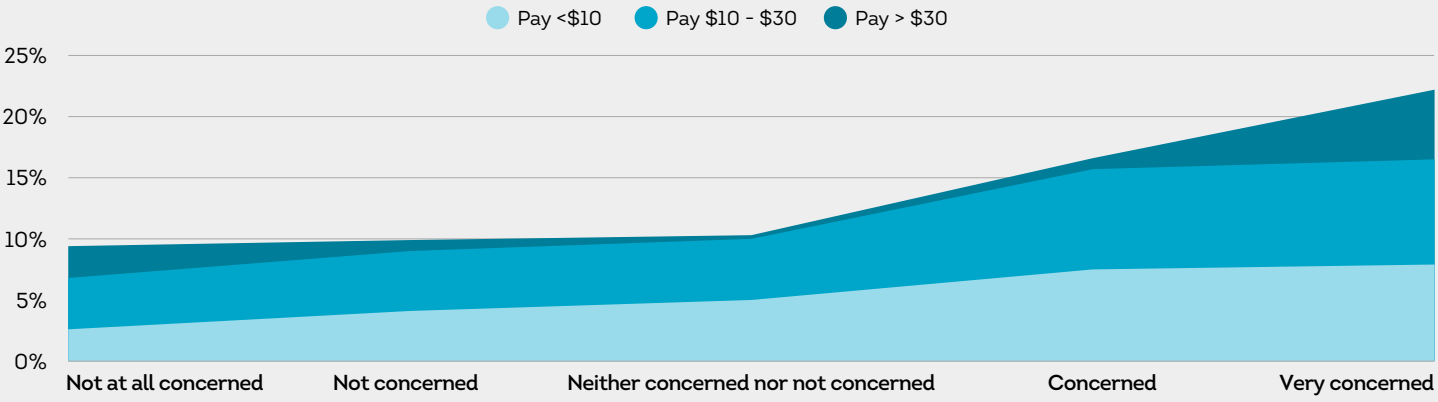
For consumers who signed up for a paid service, the majority of them pay less than $20 per month. For those paying more than $20 per month, they were much more likely to be from a younger cohort. Forty-six percent of Gen Z consumers who signed up for a paid identity monitoring service paid more than $20 per month, while 34% of Millennials fell into this category. Though younger consumers were less likely to take proactive steps to combat fraud, they were more likely than older generations to sign up for and pay more for identity and credit monitoring services.



Source: TransUnion Telecommunications Survey 2023

Totals may not add to 100% due to rounding

Unsurprisingly, concern about fraud was correlated with how much a consumer is willing to pay for fraud protection services. Of those who reported being very concerned about fraud, 23% signed up for a paid service compared to just under 10% of those who were not concerned at all. It should also be noted those who expressed no concern about fraud may feel that way because they signed up for a paid service. Still, there was a clear correlation between willingness to pay for fraud protection and concern about fraud. Being able to identify consumers who are most concerned and proactively offer them protection can potentially enhance customer retention strategies for telco providers.



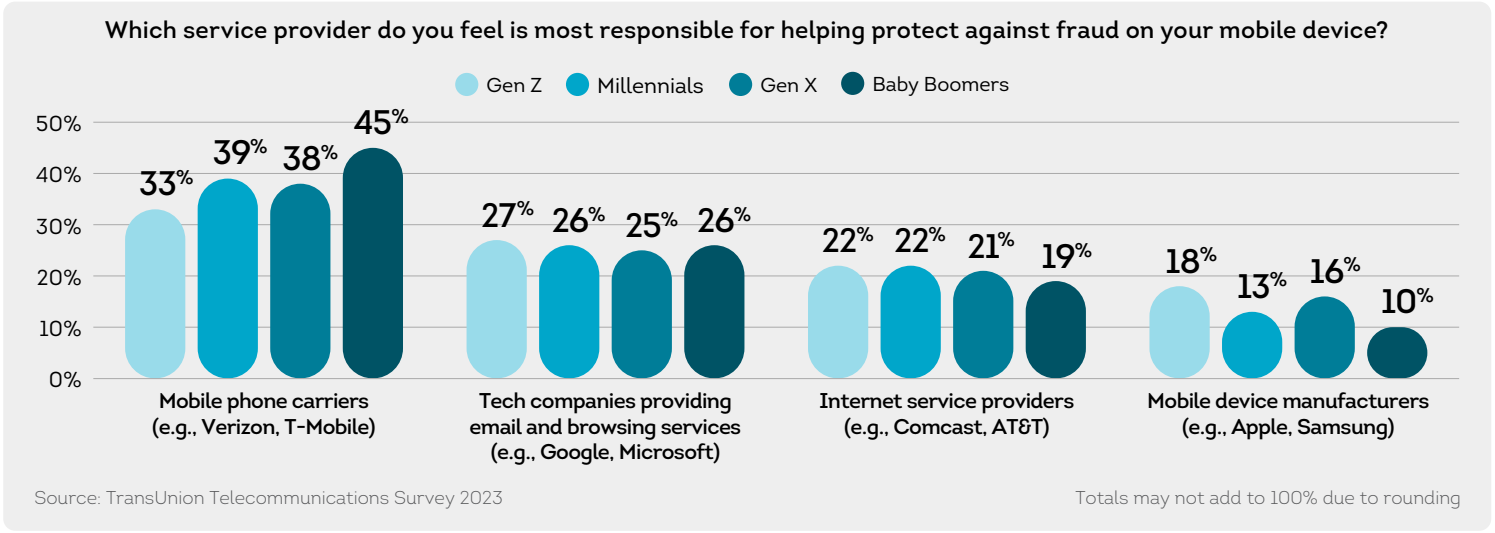
Source: TransUnion Telecommunications Survey 2023

Totals may not add to 100% due to multiple selections

TransUnion

Consumers aren't expecting to go it alone

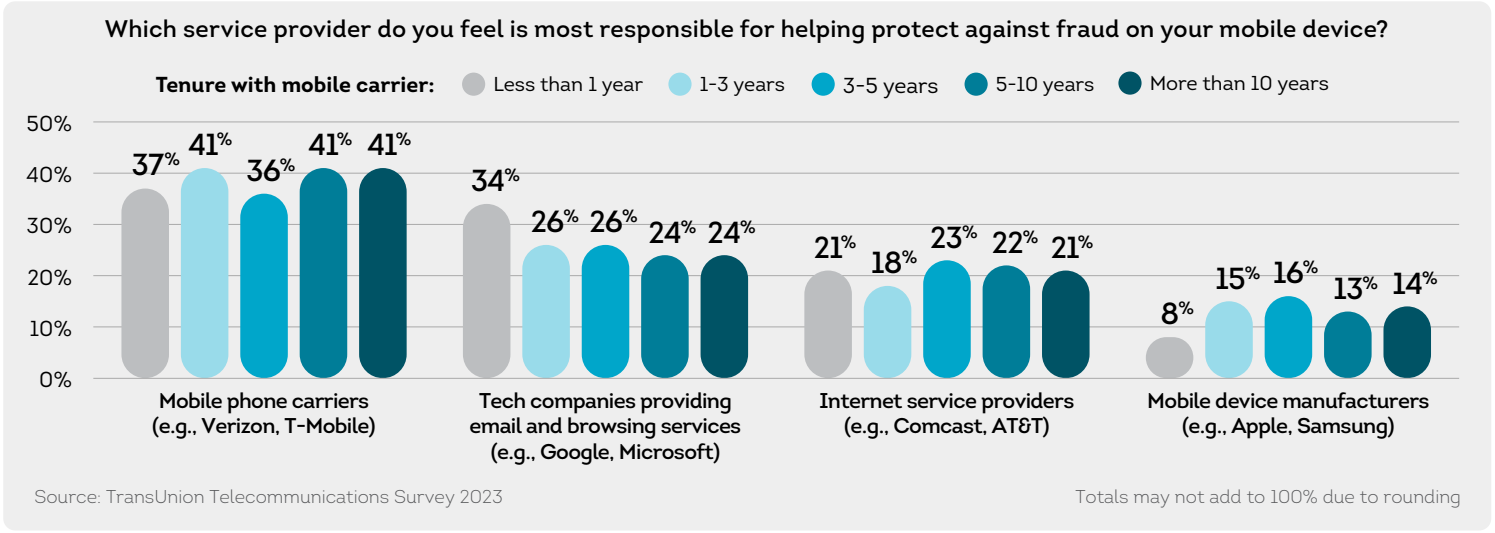
As consumers do their best to protect themselves against fraud and identity theft, they expect companies within the digital ecosystem to shoulder some of the burden. Among all age cohorts, mobile phone carriers were identified as having the most responsibility for helping consumers protect against fraud on their mobile devices. Given the prevalence of SMS and voice phishing attacks, it's no surprise consumers feel mobile carriers should step in to help them protect against fraud. Tech companies providing email and browsing services were also cited by over a quarter of consumers as having responsibility to help protect against fraud, likely tied to email phishing attacks.



Source: TransUnion Telecommunications Survey 2023

Totals may not add to 100% due to rounding

The same trend held true when considering tenure with a mobile phone carrier. Notably, those who were new customers (with less than a year with their mobile phone carriers) were almost as likely to say tech companies are as responsible as mobile carriers to help them combat fraud. This drops dramatically as customers age with their mobile carriers, shifting the burden away from tech companies and toward mobile carriers as having the most responsibility to help them fight against fraud. It's important for a mobile carrier's retention strategy to deploy solutions to help address their customers' concerns relating to fraud – as their longest tenured customers expect the most out of them.



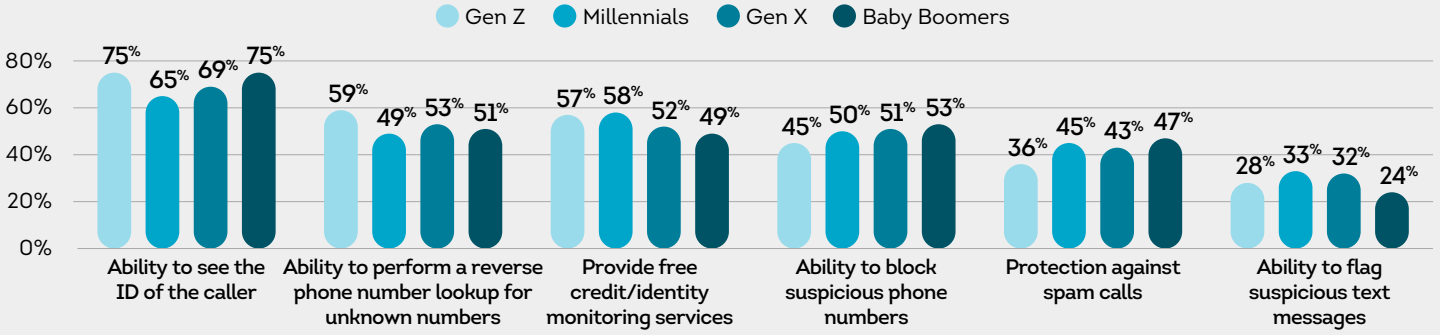
Source: TransUnion Telecommunications Survey 2023

Totals may not add to 100% due to rounding

TransUnion

When it came to the types of fraud protection solutions consumers are looking for, telco service providers have a variety of options. Across generations, having the ability to see the ID of callers was nearly universally desired. What's more, having the ability to perform a reverse phone number lookup for unknown callers, blocking suspicious numbers and getting protection against spam calls were also popular options, suggesting solutions that address call spam and voice phishing attacks are top of mind for consumers. Providing free credit monitoring services was more popular among younger cohorts, while having the ability to flag suspicious text messages wasn't highly prioritized. Whatever the solution, telco service providers have many options for meeting the fraud prevention demands of their customer bases.

What are the top three fraud prevention services would you like to see provided by your mobile service provider?



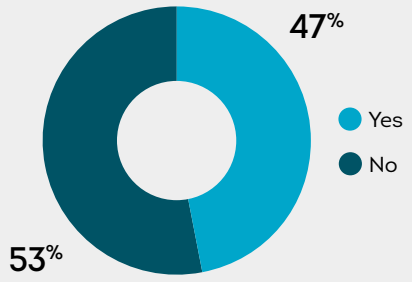
Source: TransUnion Telecommunications Survey 2023

Totals may not add to 100% due to rounding

NEW TECHNOLOGY, NEW CONCERNS

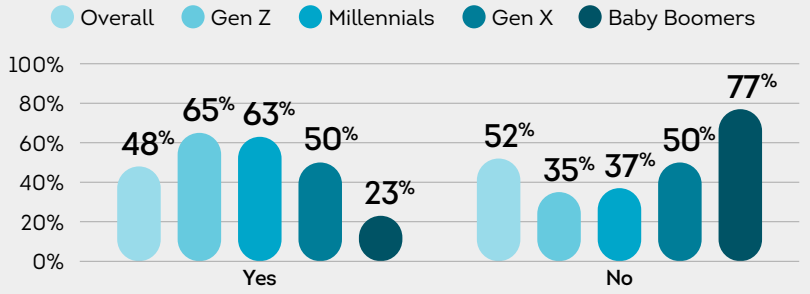
As the world becomes increasingly more digital and new technologies like AI are deployed, consumer data are exposed to higher levels of risk. One risk in particular is the impact of data breaches and the amount of private customer information that's exposed. Nearly half (47%) of consumers reported a company that houses their personal information had experienced a data breach. Among those whose data was exposed, 48% reported experiencing an increase in spam calls after the breach. Across generations, the difference was even more pronounced; 65% of Gen Z and 63% of Millennials reported an increase in spam calls. Half of Gen X reported an increase in unwanted spam calls, while only 23% of Baby Boomers reported the same.

Has a company that has your personal information experienced a data breach?



Source: TransUnion Telecommunications Survey 2023
Totals may not add to 100% due to rounding

Did you experience an increase in unwanted/spam calls after the data breach?

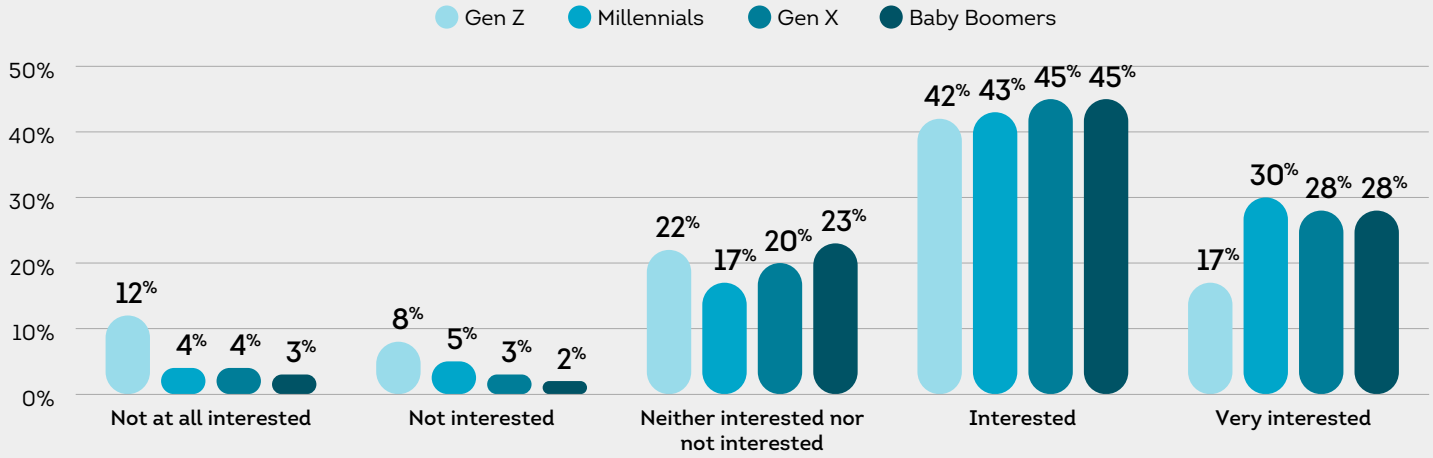


Source: TransUnion Telecommunications Survey 2023
Totals may not add to 100% due to rounding

TransUnion

Given the rise in data breach activity and subsequent increase in unwanted spam calls resulting from exposure of sensitive information, many consumers expressed high levels on interest in solutions that would help mitigate the rise in unwanted call volumes. For telco service providers and mobile carriers in particular, given the high expectations from their customers related to fraud prevention, deploying solutions that ease consumers' burdens dealing with spam calls would likely receive a warm reception from those of all ages. Only among Gen Z did fewer than 60% of consumers say they'd be interested (42%) or very interested (17%) in this type of solution.

How interested would you be in a solution to deal with unwanted/spam calls resulting from a data breach at a company that has your personal information?

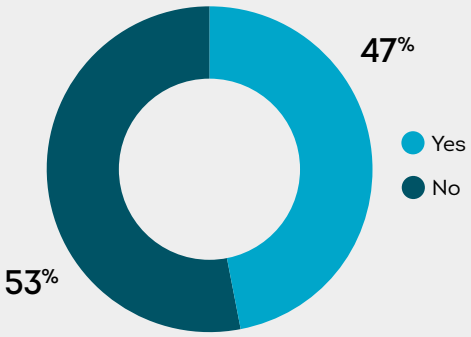


Source: TransUnion Telecommunications Survey 2023

Totals may not add to 100% due to rounding

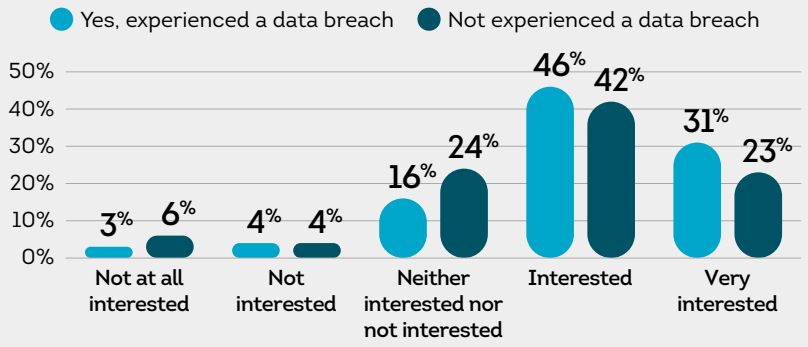
Examining the data by who has been impacted by a data breach, we saw a similar story. Of consumers whose information was exposed by a data breach, 77% said they were either interested (46%) or very interested (31%) in a solution that deals with unwanted spam calls compared to 65% of consumers who were not impacted by a data breach. Whether or not a consumer had been directly impacted by data breach activity, the demand for dealing with unwanted spam calls was high across the population. As consumers expect more from various service providers in the digital and mobile ecosystem, protection against unwanted calls or call-related fraud attempts could serve as a key differentiated customer experience .

Has a company that has your personal information experienced a data breach?



Source: TransUnion Telecommunications Survey 2023
Totals may not add to 100% due to rounding

How interested would you be in a solution to deal with spam calls resulting from a data breach that exposed your personal data?



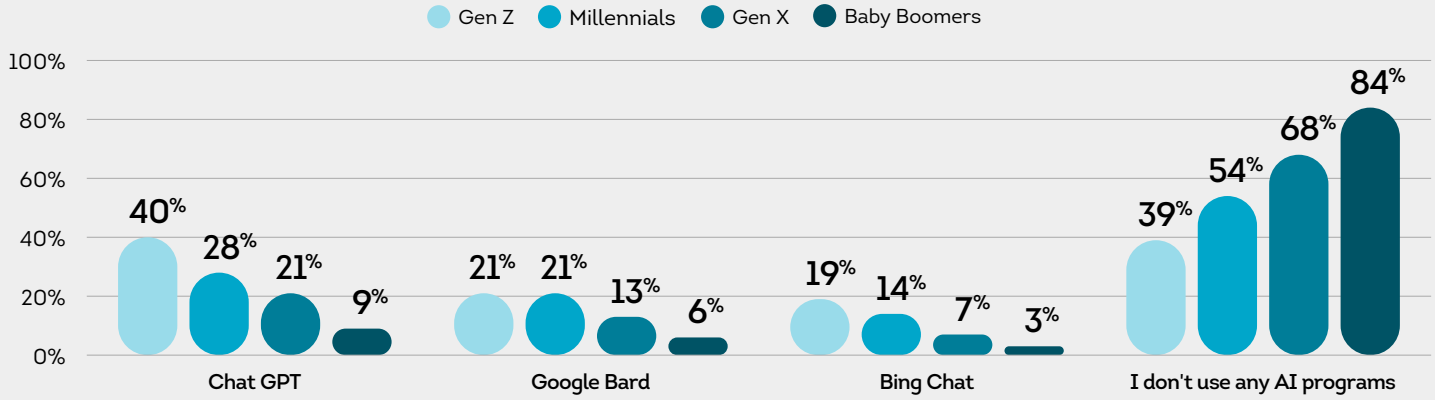
Source: TransUnion Telecommunications Survey 2023
Totals may not add to 100% due to rounding

TransUnion

AI creates new risks

For many, the rapid rise of large language models and new generative AI tools is an exciting development, though not without risks. Despite the relative newness of these tools, adoption is already high, especially among younger generations. Sixty-one percent of Gen Z and 46% of Millennials reported using AI programs on their mobile devices. As these tools improve and become embedded into existing applications, this number is sure to rise quickly and dramatically. And while new AI tools will be a key component of the digital space, new risks are already emerging and being felt by early adopters.

Which of the following AI programs have you used on your mobile device?

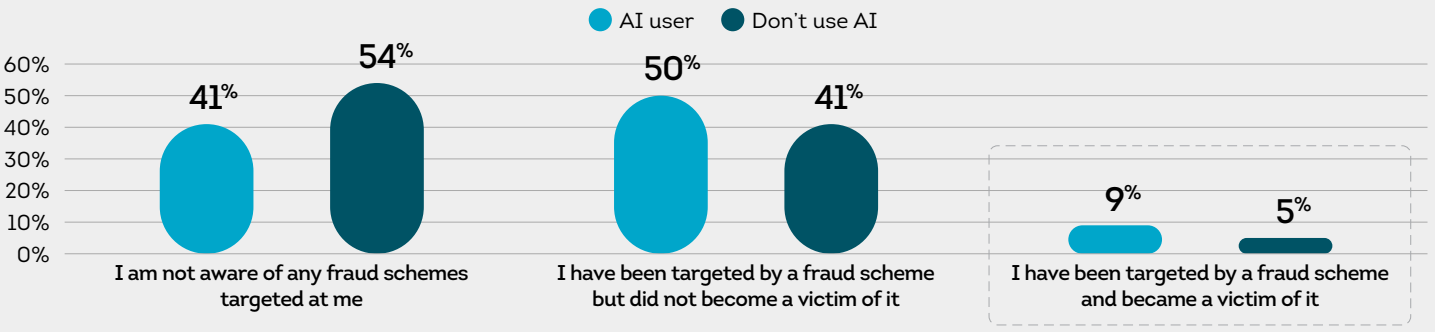


Source: TransUnion Telecommunications Survey 2023

Totals may not add to 100% due to multiple selections

Existing AI users were nearly twice as likely to report being targeted by and falling victim to a fraud scheme as non-AI users in the past three months (9% vs. 5%). What's more, AI users appeared to have been targeted with fraud schemes at a much higher rate than non-AI users. Half of AI users said they were targeted but did not fall victim to a fraud scheme, while 41% of non-AI users said the same. Given the newness of AI tools, users may be more vulnerable as they learn how to use and interpret these new tools. Perhaps more concerning was these powerful programs are also available to fraudsters and will undoubtedly increase the productive capacity and effectiveness of those looking to commit fraud or identity theft. Already there have been reports of AI voice scams where fraudsters are able to use AI programs to pose as a relative in distress and demand payment.

Which statement best describes your personal experience with any online, email, phone call or text messaging fraud attempts while using your mobile phone in the last three months?

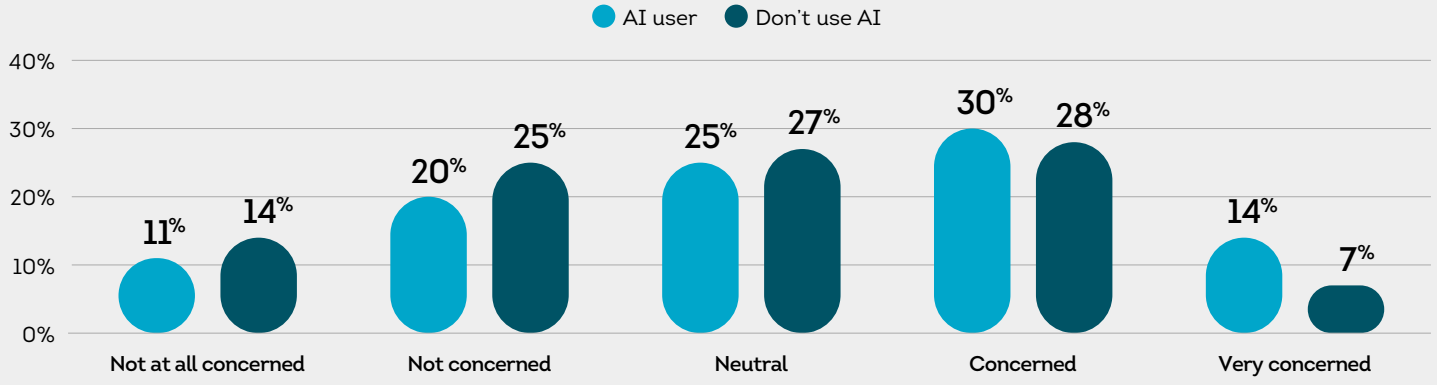


Source: TransUnion Telecommunications Survey 2023

Totals may not add to 100% due to multiple selections

Early AI users are likely among the most digitally savvy consumers – and already seeing the risks related to these tools. AI users were twice as likely to report being very concerned about fraud (14%) when compared to non-AI users (7%), and more likely to be concerned overall 44% vs. 35%. This is an important signal for service providers looking to help consumers safeguard their personal information and protect against fraud. As less sophisticated users begin adopting AI, their risk exposure may grow significantly. The time to heed the warning from early AI adopters is now. As data breach activity leads to more and more personal data being exposed, and as fraudsters take advantage of sophisticated new tools, the need for newer and more effective fraud prevention tools for consumers will only grow.

When using your mobile phone, how concerned are you about fraud?



Source: TransUnion Telecommunications Survey 2023

Totals may not add to 100% due to rounding

CONCLUSION

Fraud and identity theft attempts continue to plague consumers. Across generations, more than half of consumers said they deal with some kind of fraud attempt at least once a week. While fraudsters have become more sophisticated as new technologies emerge, fraud and identity theft largely remain volume driven. Consumers are most frequently subjected to voice, messaging and email fraud attempts, and while they've taken steps to stay vigilant, more and more consumers are expecting help from communications service providers (CSPs) in their fights against fraud.

As data breaches increase and more customer data is exposed, consumers are seeing a rise in unwanted spam calls and expect mobile carriers to provide them with the tools to avoid falling victim to fraud attempts.

What's more, the rise of new artificial intelligence programs is increasing the risk to consumers. Though we're early in the adoption cycle for generative AI, early users report falling victim to fraud at nearly twice the level as non-AI users.

Moreover, fraudsters will also be able to access these new tools and potentially increase the effectiveness of their schemes. With only a minority of consumers having signed up for paid identity protection services, there's potential for a widening gap between the sophistication of fraudsters and the abilities of consumers to elude fraud attempts with common sense tactics, such as blocking unknown numbers and deleting phishing messages.

CSPs can help protect consumers by continuing to comply with ongoing regulations and mandates from the Federal Communications Commission (FCC), and other regulators; by leveraging robocall mitigation solutions; and by ensuring their networks support branded calling and call authentication solutions that help reduce call spoofing and fraud - restoring trust to the telecom ecosystem.

APPLYING CONSUMER FINDINGS IN 2024

Even as the voice channel remains essential to customer service, 88% of business calls still go unanswered because customers fear illegal robocalls, phone scams and identity spoofing. For enterprises that depend on the global voice ecosystem for global commerce, as well as communications service providers (CSPs) that deliver and authenticate calls across networks, we enable trusted connections to help make every touchpoint count. The bottom-line benefits of our TruContact™ Trusted Call Solutions (TCS), powered by Neustar®, are clear: CSPs can meet regulatory requirements, implement STIR/SHAKEN call authentication, protect consumers and empower enterprises with new, revenue-generating services.

When revenue, reputation and relationships are at stake, you need the right intel and resources to respond efficiently and effectively. Our full suite of Trusted Call Solutions helps CSPs and outbound calling operations protect customers from fraudulent calls while getting legitimate calls through. Future-proof customer contact with a reliable, compliant approach to manage the accuracy and consistency of enterprise brand identity and business information displayed to consumers.

Identity theft is a very real concern and consumers are looking to businesses they trust to provide support. Now you can better protect consumers against identity theft and other concerns with sound guidance and robust tools. With the increased volume and velocity of data breaches, including personal information being sold on the dark web, IdentityForce takes protecting identities seriously. IdentityForce is a brand built on trust with a clean compliance history, decades of experience, and the agility and flexibility to respond to industry trends to deliver a top-rated solution that protects what matters most. For more than 40 years, IdentityForce has built a community unified by its collective mission: to make a difference in the lives of its members – the people who rely on it every day to safeguard their identities. It enables continuous monitoring of your identity, privacy and credit via innovative and proactive identity theft protection technology. We detect illegal selling of your personal, financial and credit information, providing robust monitoring required in today's connected world. IdentityForce features an early warning system that notifies you when your personal information is at risk. Our alerts are sent to your smartphone, tablet or computer, giving you the power to act before damage is done. When you want total identity control, count on IdentityForce.

RESEARCH METHODOLOGY

This online survey of 1,500 adults was conducted from September 2023 by TransUnion in partnership with third-party research provider, Dynata. Survey participants included adults 18 years of age and older residing in the United States. Participants were surveyed using an online research panel method across a combination of desktop, mobile, and tablet devices. Survey questions were administered in English. To ensure general population sample representativeness across United States resident demographics, the survey targeted respondents in line with the census statistics on the dimensions of age, gender, and household income. Generations are defined as follows: Gen Z, born 1995-2005; Millennials, born 1980-1994; Gen X, born 1965-1979; Baby Boomers, born 1945-1964. These research results are unweighted and statistically significant at a 95% confidence level within ±3 percentage points based on calculated error margin. Please note some chart percentages may not add up to 100% due to rounding or multiple answers being accepted.

For more information about TransUnion marketing solutions: **transunion.com/truaudience**
fraud solutions: **transunion.com/truvalidate**
credit solutions: **transunion.com/truvision**
communications solutions: **transunion.com/trucontact**
identity protection solutions: **transunion.com/truempower**

TransUnion

About TransUnion (NYSE: TRU)

TransUnion is a global information and insights company that makes trust possible in the modern economy. We do this by providing an actionable picture of each person so they can be reliably represented in the marketplace. As a result, businesses and consumers can transact with confidence and achieve great things. We call this Information for Good®.

A leading presence in more than 30 countries across five continents, TransUnion provides solutions that help create economic opportunity, great experiences and personal empowerment for hundreds of millions of people.

transunion.com