javelin | BioCatch

The Emotional Undercurrent of Financial Scams

WHITEPAPER | AUGUST 2024

Table of Contents

Table of Figures

javelin

Meet the Author

Suzanne Sando
Senior Analyst,
Fraud & Security

Suzanne is a senior analyst in Javelin's fraud & security practice. She tracks trends and risks in cybersecurity, and delivers practical recommendations for fraud protection. Her specific areas of interest are government cybersecurity, behavioral sciences and fraud, and consumer empowerment and education against fraud.

Foreword

This report, sponsored by BioCatch, explores the financial and emotional impact of scams on victims of various backgrounds, as well as critical evidence needed for the financial services industry to successfully combat scams.

This report was adapted from data collected by Javelin Strategy & Research's 2024 Scams and Financial Loss survey, fielded in May 2024. Javelin Strategy & Research maintains complete independence in its data collection, findings, and analysis.

Overview

The impacts of identity fraud and scams cannot be understated—from the financial to the emotional and psychological. Victims of financial scams are often left feeling helpless in the wake of the crime perpetrated against them, not knowing whom to report the crime to, what steps are needed to resolve issues, or if they are even entitled to any sort of financial safety net in the form of provisional credit or reimbursement from their financial institution. Understanding the typical victim profile, the anatomy of a scam, and life after the scam provides essential guidance to the financial services industry as work continues to lessen the financial and emotional toll on scam victims.

Executive Summary

No 'typical' scam victim exists, as the financial and emotional effects of scams do not align with stereotypes. There are more than a few misconceptions when society considers the profile of a scam victim. One might assume that older consumers are more likely victims of scams, but Javelin's research reveals that consumers ages 18-44 make up a larger portion of scam victims than those 45 and older. Two-thirds of scam victims are 44 and under; 17% are between the ages 45 and 54; and only 17% of scam victims are 55 and older. Additionally, more affluent households are generally considered a more likely target for criminal activity; however, Javelin research shows that consumers reporting an annual household income of $150,000 or more amount to only 18% of scam victims.

Regardless of the amount lost in a scam, the financial damage can feel irreparable if there's no reimbursement. Over one-third (39%) of scam victims lose more than $500 in each scam interaction with criminals, with 22% of those scam victims losing between $1,000 and $5,000. As reimbursement of lost funds resulting from a scam is not a guarantee, a monetary loss of this magnitude leaves many victims unable to pay scheduled bills, afford unplanned purchases, and cover any overdraft fees incurred on their affected accounts.

Those victims who report their scam interactions to their financial institutions and receive reimbursement are generally satisfied with the experience. A significant number of scam victims, 54%, report getting a full reimbursement of their lost funds from their financial institution, with 13% receiving partial reimbursement, 5% waiting for a response from their financial institution, and the remaining 28% receiving no reimbursement.

Despite elevated levels of confidence in detecting scams, nearly half of scam victims are repeat victims. Scam victims are generally confident in their ability to identify suspicious behavior and stop scam interactions before any damage is done, with an overwhelming 80% of victims stating they feel as though they are equipped to identify a scam before falling victim again. But an examination of the frequency of scam incidents shows that nearly half (49%) of scam victims reported experiencing two or more incidents in the past two years that resulted in monetary loss.

Scam victims are often their own first line of defense. Only 15% of scam victims reported discovering their scam through a suspicious-activity alert from their bank or credit union. Nearly two-thirds (64%) of scam interactions were discovered by the victim by reviewing their account statements and ledgers.

Victims are often left holding the bag after a scam and wondering what to do next. One-quarter (26%) of scam victims do not know to whom they should report their scam interaction, leaving a significant gap in the victim experience that FIs should work to close.

Scam victims report a multitude of tactics used by cybercriminals to persuade victims to authorize transactions or send money to the criminal. Counterfeit purchases (13%), communication from imposters posing as legitimate companies (9%), and social media requests from strangers (8%) are just a few ways that criminals have exploited scam victims in the past two years. Notably, 6% of scam victims reported that they were victimized in another way, indicating that these interactions represent just the tip of the iceberg.

Lacking industry-wide scam classification and categorization lengthens the resolution process. With no industry standard and official reporting procedures in place, financial institutions spend too much time during the resolution process understanding exactly what kind of crime the victim experienced, as well as how to best resolve the situation.

Recommendations

Overhaul scam education. It's beyond time to accept that scam education should not be a one-size-fits-all approach. What affects one consumer will not make an impact on the next. Expose consumers to regularly updated scam education, focusing on new threats on the horizon or scams that target their demographic. Consider personalizing education in online and mobile app banking sessions, creating targeted lists of pertinent articles and tips for individual customers based on their demographics and spending habits.

Offer provisional credit during the scam investigation and resolution process. The offer of provisional funds from a victim's financial institution is a must. Finances are a stressor in many consumers' lives, and with the added strain of unexpected losses, a scam victim experiences more than just a monetary impact. Because of the difficulty in distinguishing first-party fraud from a legitimate scam loss, banks should use historical account data to determine if a victim qualifies for provisional credit. Financial institutions can lessen the financial and mental burden of these losses with a cushion to cover the loss while the transaction in question is investigated. This would ease the strain on the victim and create a stronger relationship of trust and satisfaction between victims and their FIs.

Reassess reimbursement policies. Reimbursement plays a significant role in overall satisfaction in a banking relationship. Along with provisional credit offerings, FIs should use historical transaction activity and account status to earn and uphold the trust and satisfaction of the customer, which is essential in maintaining a long-standing financial relationship.

Avoid notification fatigue by offering customized alerts. Provide options for relevant alerts to specific customers and members that they express interest in receiving or alerts for threats that specifically target their demographic. Create a customizable alert experience that doesn't contribute to notification fatigue (push notifications that consumers ignore because of their irrelevance or excessive frequency). Consumers who make use of important fraud and scam alerts greatly increase the likelihood of recognizing a scam interaction either before a transaction is authorized or immediately after, which could make investigations into these crimes less of a herculean effort.

Integrate real-time scam detection technology into existing fraud prevention and detection tool suites. Real-time payment controls significantly reduce the probability of becoming a scam victim. Financial institutions that invest in real-time scam detection and intervention solutions can monitor existing accountholder activity, including transaction history and behavioral biometrics, to determine the legitimacy of a transaction that is taking place. If suspicious activity is detected, the FI can intervene and prevent the payment from going past the point of no return.

Profile of a Scam Victim

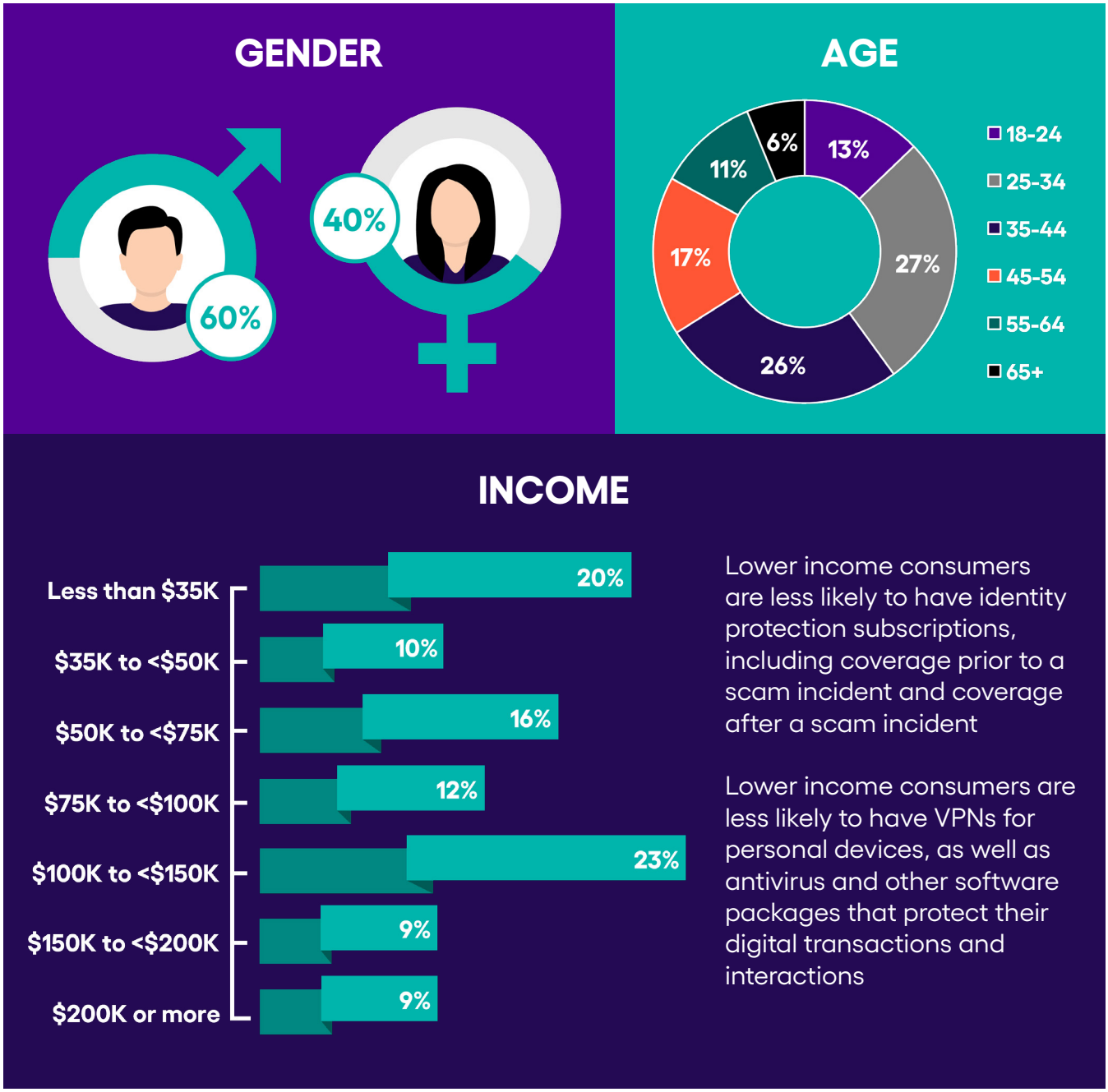
Rapidly developing technology and dynamic spending habits have allowed cybercriminals a host of opportunities to exploit consumers. Because of their ability to discover and manipulate weaknesses in existing financial institution processes and policies and prey on who they perceive to be the most vulnerable consumers, criminals worldwide have carved out a lucrative corner. Taking into consideration the wide array of prospects awaiting criminals, it's critical to consider the profile of the "perfect" scam victim.

Despite many common misconceptions, criminals don't discriminate when it comes to choosing a target for their scams. Many might assume that older consumers or those with higher annual household incomes might be the prime targets, but recent Javelin research, undertaken to better understand trending scams and their effects on consumers, proves otherwise. In fact, consumers ages 18-44 make up a larger portion of scam victims than those 45 and older (see Figure 1). Two-thirds of scam victims are 44 and under, 17% are between 45 and 54, and only 17% of scam victims are 55 and older.

Another common belief is that criminals set their sights on more affluent households, with the assumption that larger incomes and more significant assets are incentives for pursuing these consumers. In reality, Javelin research shows that over half (58%) of targeted victims report an annual household income of less than $100,000. More affluent households, earning $150,000 or more annually, amount to only 18% of scam victims.

Criminals Consider Every Consumer When Selecting Victims

Figure 1. Demographic Breakdown of Scam Victims, by Gender, Income, and Age



Source: Javelin Strategy & Research, 2024

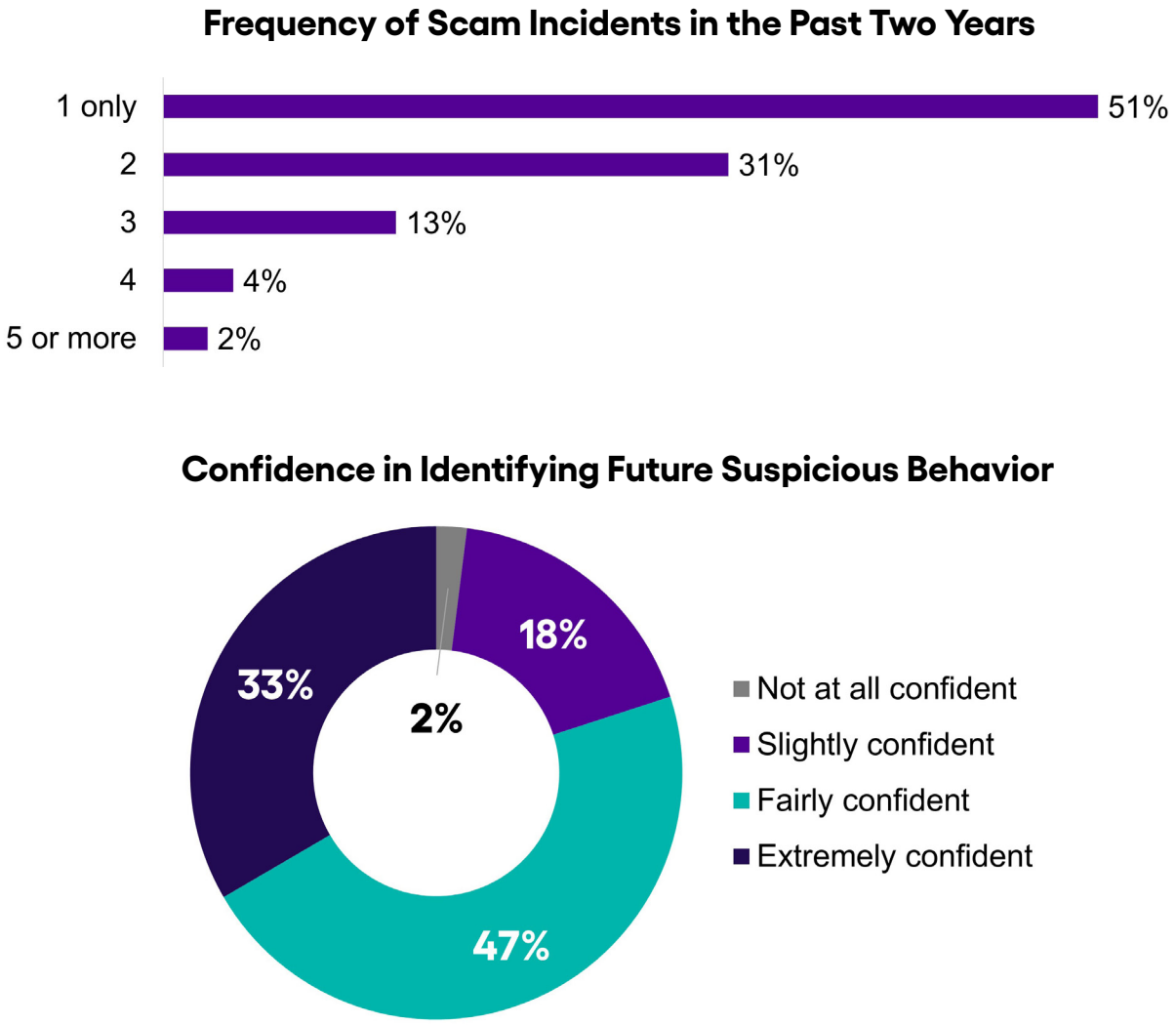
javelin

Every consumer is considered a viable option for a criminal scheme, regardless of their demographic characteristics, such as gender, income, and age. What differs from consumer to consumer are the methods a criminal might use to establish and maintain contact, as well as the payment or transaction methods used to perpetrate the scam. Leaving no stone unturned when choosing targets significantly increases the criminal's likelihood of ensnaring a victim.

Scam victims are generally confident in their ability to identify suspicious behavior and stop scam interactions before any damage is done, with an overwhelming 80% stating they feel as though they are equipped to identify a scam before falling victim again. Much of this could be attributed to feelings of "I won't get fooled again," with many scam victims presuming they will be more guarded in future interactions with strangers. But an examination of the frequency of scam incidents shows that nearly half (49%) of scam victims reported experiencing two or more occurrences in the past two years resulting in financial loss.

Despite High Levels of Confidence in Detecting Scams, Nearly Half of Scam Victims Are Repeat Victims

Figure 2. Scam Victim Confidence in Detecting Future Scams vs. Frequency of Scam Incidents



Source: Javelin Strategy & Research, 2024

javelin

Either scam victims' perception of their detection abilities must be adjusted or the financial industry needs to immediately reassess how much of a handle it has on the fast-paced and always-evolving scam landscape. One of the key reasons scam losses continue to cause major headaches for consumers and financial institutions is that criminals constantly switch tactics and exploit new payments technology and economic disruptions, such as the COVID-19 pandemic or economic instability in 2023. FIs and other financial organizations must remain keenly aware of shifting criminal tactics if scam losses are to drop.

Over one-third (39%) of scam victims lose more than $500 in each scam interaction with criminals, with 22% of those scam victims losing between $1,000 and $5,000. Reimbursement of funds lost in a scam is not guaranteed, so a financial loss of this magnitude leaves many victims unable to pay scheduled bills, make unplanned purchases, and cover any overdraft fees incurred on their affected accounts. Even if a scam loss reimbursement is imminent, the long-lasting damage may already be done to a victim's account.

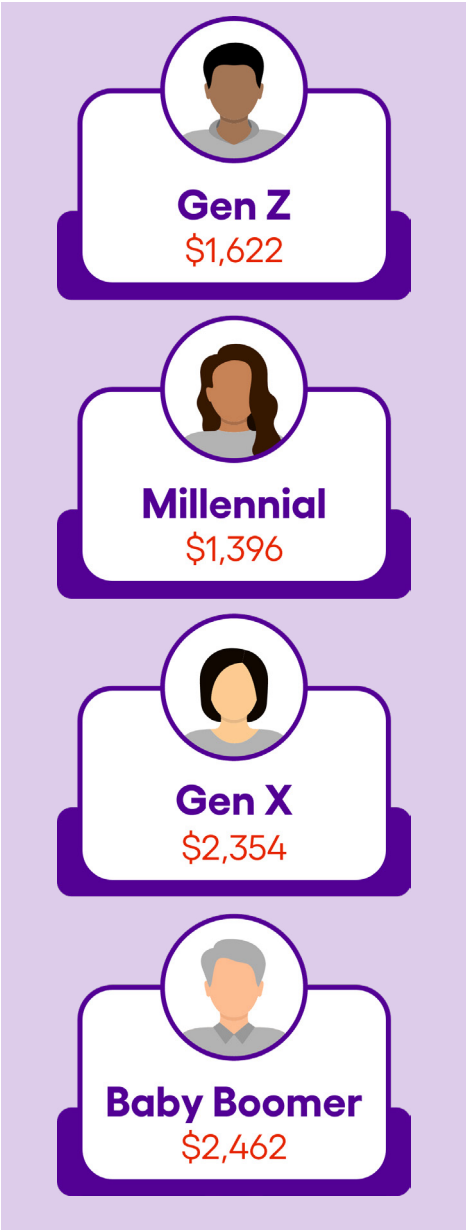
Because many scam victims come from lower-income households, losses of any kind can set a victim financially behind, and not just until the next paycheck. According to Empower, 37% of U.S. adults are unable to afford unexpected emergency expenses in excess of $400.[1] Financial losses due to scam victimization certainly qualify as an unexpected emergency expense.

The offer of provisional funds from a victim's financial institution is a must during the investigation and resolution process. Finances are a stressor in many consumers' lives, and with the added strain of unexpected losses, a scam victim experiences more than just a monetary impact. Javelin recognizes the difficulty banks face in distinguishing first-party fraud from a legitimate scam loss; thus, banks should use historical account data to determine if a victim qualifies for provisional credit. Financial institutions can lessen the financial and mental burden of these losses with a cushion to cover the loss while the transaction in question is investigated. This would ease the strain on victims and create a stronger relationship of trust and satisfaction between victim and their FIs.

Scam losses affect each victim differently, but there is undoubtedly a financial and emotional effect in some regard. An examination of the financial losses for each generation showed that Baby Boomers topped the charts with an average of nearly $2,500 in losses in one scam interaction, with Gen X following closely behind at $2,354 (see Figure 3). Millennials lost significantly less than the older generations—just under $1,400—and Gen Z experienced an average loss of $1,622.

Baby Boomers Top the Average Losses, with Millennials Coming in Last

Figure 3. Average Scam Losses, by Generation



Source: Javelin Strategy & Research, 2024

javelin

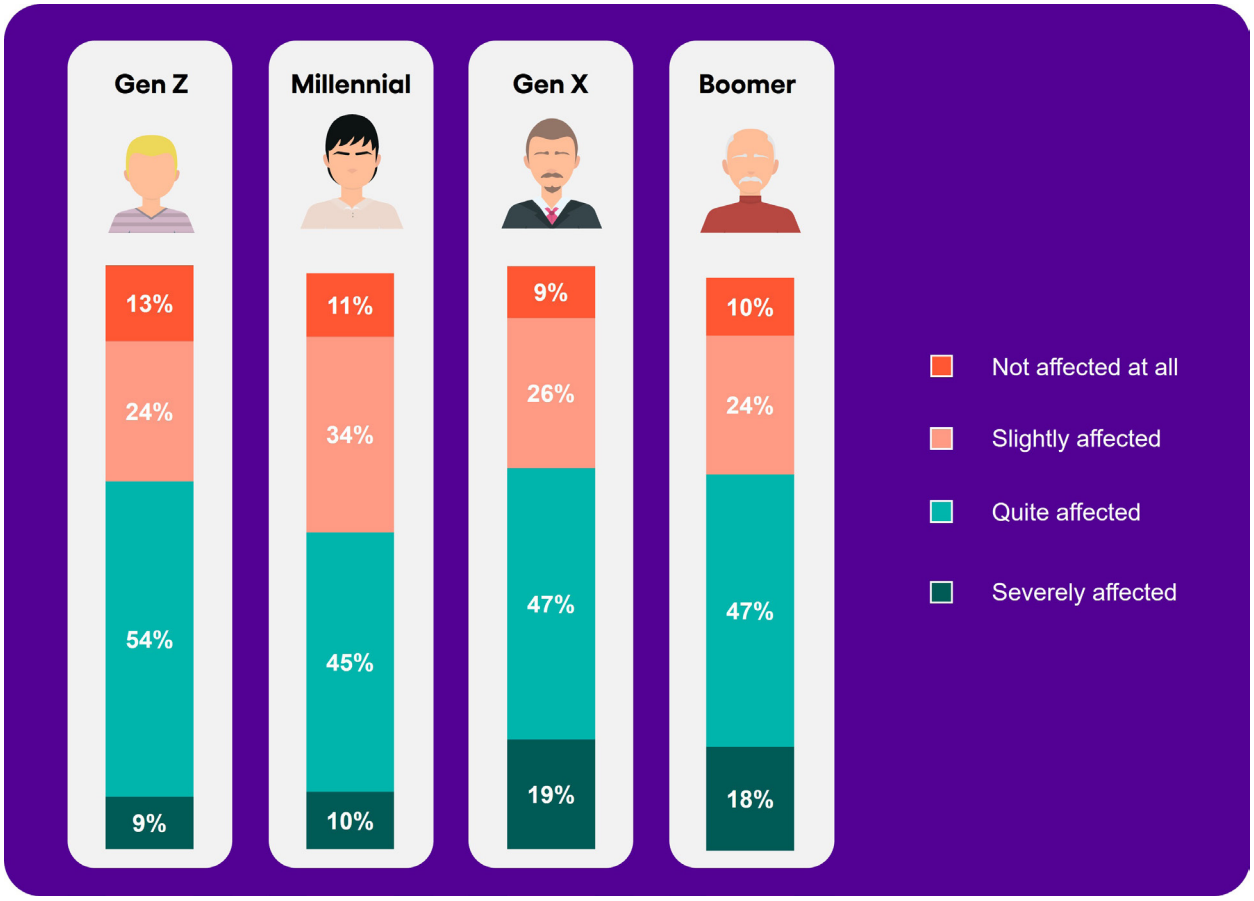
Baby Boomer consumers are now mostly in retirement, with Gen X not too far behind. Criminals view these consumers as lucrative scam targets because many have significant retirement savings, often across multiple accounts, and have more to lose in one single scam if they can be ensnared. Even if an older consumer does not have the largest nest egg, they've likely saved more than their younger counterparts.

The negative effects of any financial emergency for most consumers are far-reaching, causing ripples throughout related financial accounts. Scam losses are no exception, and often those experiencing the most financial impact aren't necessarily the ones losing the most money. Javelin research shows that Millennial scam victims feel the financial impacts of a scam interaction at slightly higher rates than other generations, even though they lose the least amount, on average (see Figure 4).

Many Millennial consumers tend to be frugal and more conscious about spending. Many Millennials were entering the workforce during the Great Recession of 2008 or had done so a few years earlier, making them prime targets for layoffs—a perfect storm when coupled with starting to pay back exorbitant student loans and purchasing their first homes.

Millennial Scam Victims Feel the Financial Woes

Figure 4. Financial Effects of Scam Losses, by Generation



Source: Javelin Strategy & Research, 2024

javelin

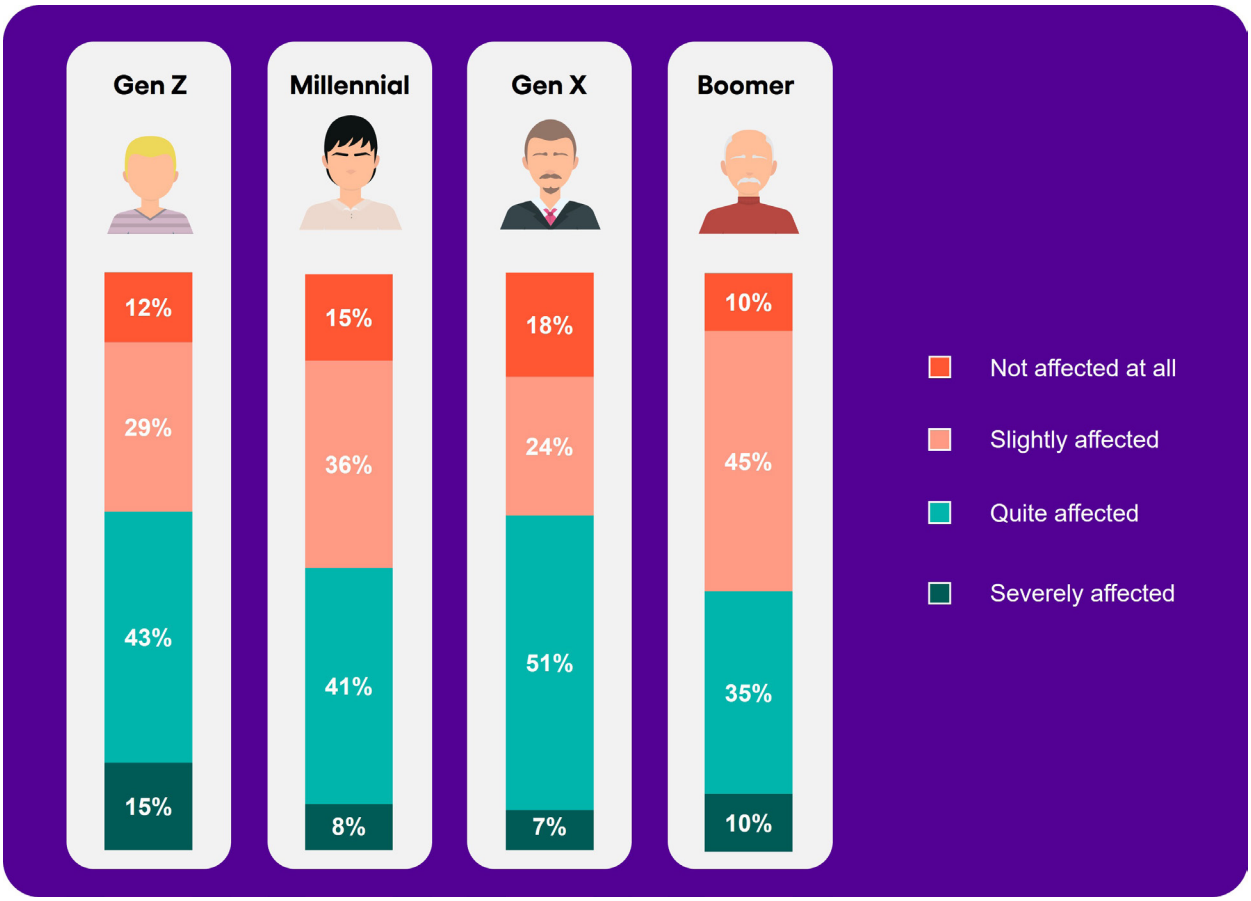
Living through a volatile economic period has long-standing effects on consumers. Criminals targeting Millennials may face resistance when it comes to authorizing transactions the consumers are unsure of, or when Millennial consumers are unwilling to authorize purchases or payments for larger amounts. This accounts for why this generation has lost the least amount of money to scams, even if many of those consumers find themselves in a much more stable financial situation than they used to be in.

The financial effects are not the only aspect of scams afflicting consumers. The emotional and mental effects of becoming a scam victim and experiencing losses cannot be understated. The psychological toll of becoming a scam victim has become a leading discussion topic among expert fraud and scam advocacy groups and practitioners, but additional attention must be paid to how scams emotionally affect distinct groups of consumers.

Over half (55%) of Baby Boomer scam victims feel quite or severely emotionally affected after their victimization, at slightly higher rates than most younger victims (see Figure 5). Though Baby Boomers aren't being victimized at higher rates than their younger contemporaries, the emotional toll they carry is greater. The intensified negative mental impact is due in large part to the negative stigma of and stereotypes placed upon older consumers.

Baby Boomers Take On the Emotional Burden of Scams

Figure 5. Emotional Effects of Scam Losses, by Generation



Source: Javelin Strategy & Research, 2024

The driving forces behind why those hit by scams don't report their victimization are manifold and will be discussed later in this report. However, one of the most prevalent reasons for remaining silent after being exploited by a criminal is biased and unwarranted stereotypes. Consumer advocacy groups are working to remove unfair stereotypes, but much work remains to be done by the financial services industry to drastically lessen the emotional burden on scam victims.

The Anatomy of a Scam

Understanding the current conditions of the scam landscape is vital in determining the most effective solutions to detection and intervention. Because of the dynamic nature of scams, financial institutions must stay ahead of the trends as much as possible. Knowing how consumers are victimized, how suspicious activity is detected by victims, and how long it takes for discovery are equally critical in battling scams.

Scam victims report a multitude of tactics used by cybercriminals to persuade victims to authorize transactions or send money to the criminal. Counterfeit purchases (13%), communication from imposters posing as legitimate companies (9%), and social media requests from strangers (8%) are just a few ways that criminals have exploited scam victims in the past two years. Notably, 6% of scam victims reported that they were victimized in another way, indicating that these methods represent just the tip of the iceberg. Figure 6 shows the overwhelming variety of tactics leading to monetary loss. Criminals have expansive playbooks and are ready to move to a different method whenever necessary.

Variety of Tactics Makes Scam Detection More Complex

Figure 6. Scam Victims' Initial Actions Leading to Monetary Loss

Source: Javelin Strategy & Research, 2024

javelin

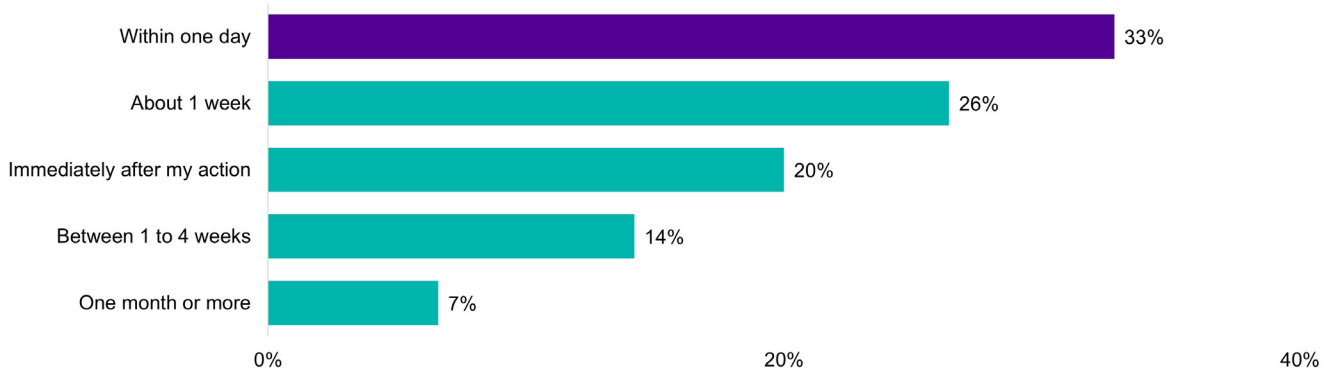
Though tactics for criminal exploitation remain diverse, there is some good news on which FIs should capitalize. Just over half (53%) of scam victims discovered they had been targeted and victimized in one day or less, with 20% having an immediate realization after the fact (Figure 7). Exposing consumers to regularly updated scam education and focusing on new threats on the horizon will encourage more situational awareness in future interactions.

Additionally, FIs should reevaluate their existing alerting options. Provide options for relevant alerts to specific customers and members who express interest in receiving them, or for alerts about threats that specifically target their demographic. Create a customizable alert experience that doesn't contribute to notification fatigue (push notifications that consumers ignore because of their irrelevance or excessive frequency). Consumers who make use of important fraud and scam alerts greatly increase the likelihood of recognizing a scam interaction before authorizing a transaction or immediately after, perhaps making investigations into these crimes less of a herculean effort.

Scam detection and prevention should not solely rest on the shoulders of consumers. Real-time payment controls significantly reduce the probability that a consumer becomes a scam victim. Financial institutions that invest in real-time scam detection and intervention solutions can monitor existing accountholder activity, including transaction history and behavioral biometrics, to determine the legitimacy of a transaction taking place by measuring the risk level of the payment. If suspicious activity is detected, the FI can intervene with critically timed pop-up messages and warnings, thus preventing the payment from going past the point of no return.

Many Victims Realize Their Victimization Within One Day

Figure 7. Length of Time Before a Scam Is Discovered



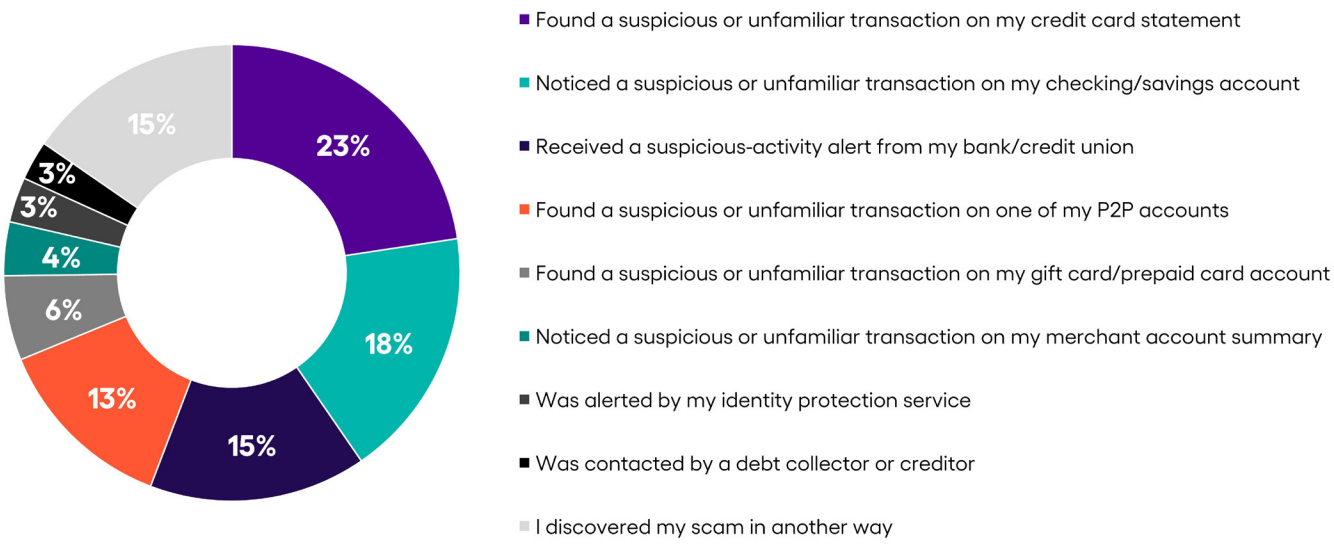
Source: Javelin Strategy & Research, 2024

Transaction intervention will become increasingly crucial as more banks and credit unions adopt real-time payments, as criminals are sure to exploit this new-to-consumers payments innovation. Legislation recently proposed in the United Kingdom suggests that banks should have an extended timeline to determine the legitimacy of suspicious authorized push payment (APP) transactions.[2] Lawmakers are advocating for a 72-hour window to suspend completion of any suspicious transaction in the wake of massive APP fraud losses, providing FIs and other financial service providers much-needed time to work with the victim to verify the validity of a payment.

Financial institutions' involvement in the detection of scams is shockingly low. Only 15% of scam victims reported discovering their scam through a suspicious-activity alert from their bank or credit union (Figure 8). Nearly two-thirds (64%) of scam interactions were discovered by the victim themselves in reviewing their account statements and ledgers.

Scam Victims Are Their Own First Line of Defense

Figure 8. Ways Scam Victims Discovered Suspicious Transactions



Source: Javelin Strategy & Research, 2024

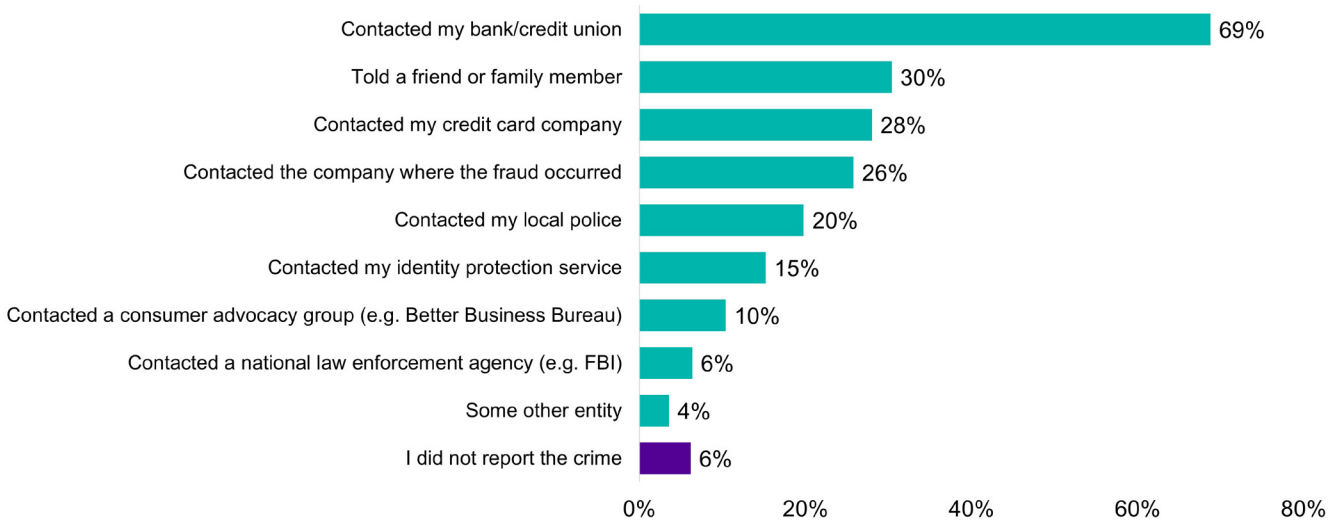
It bears repeating that consumers should not be exclusively responsible for the detection and prevention of scams. Of course, educating and empowering consumers to recognize suspicious activity from strangers or those posing as legitimate companies is critical, as consumers are indeed a key line of defense in stopping scams, but FIs must not rely on consumers alone to stop scams. Financial services providers have access to robust technology and solutions that can prevent and detect scams with more precision than the human eye alone.

The State of Reimbursement

For most victims seeking assistance in the wake of a scam, turning to their financial institution is the most logical step. Nearly seven in 10 scam victims reached out to their bank or credit union for help post-scam, leaning on their FI for guidance in investigating the scam, looking into reimbursement or options for provisional funds, preventing further loss, or getting advice on next steps. Law enforcement, at local and national levels, are lagging in terms of being the first points of contact for victims. Minimum stolen funds may preclude certain scams from receiving a legal criminal investigation from a law enforcement agency, and victims may be turned away after filing a police report.

Financial Institutions Are a Scam Victim's Best Friend

Figure 9. Steps Taken to Report Scam



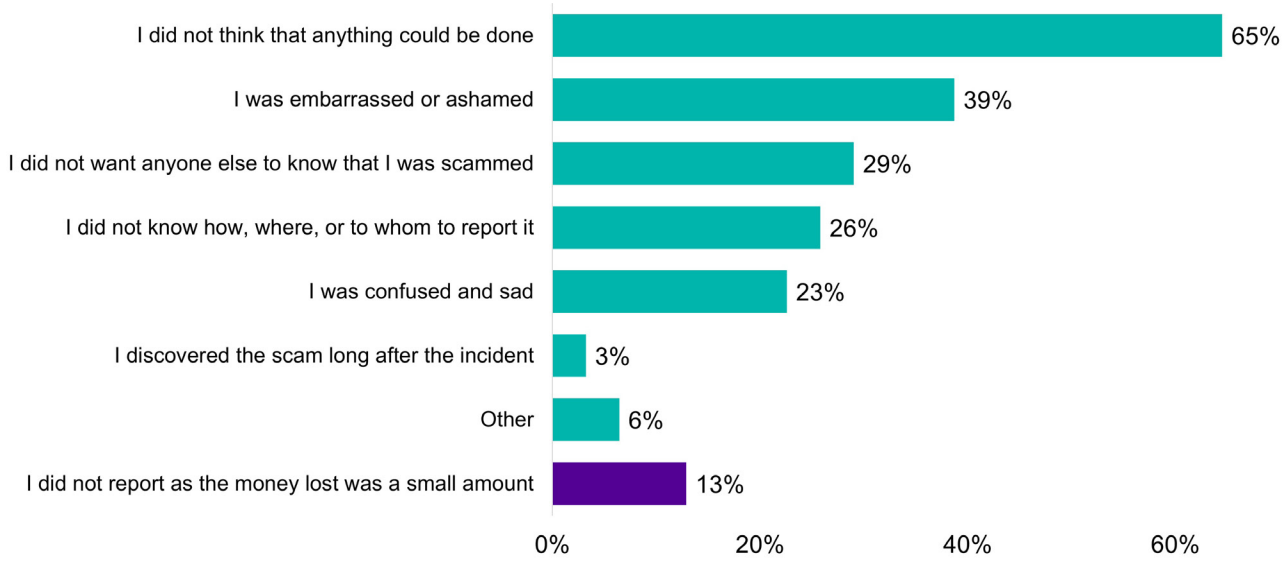
Source: Javelin Strategy & Research, 2024

Encouraging is the small number of scam victims who chose not to report the scam, with Javelin research showing that only 6% of victims didn't report the crime, but it's important to note, nonetheless. Consumer advocacy groups and financial institutions are working to create a more empathetic environment where victims feel they can come forward and report without judgment or shame, but the negative stigma and psychological effects of scams persist, leaving some scam victims resistant to reporting the crime. In an ideal world, every victim would report their scam interaction.

Despite the small number of victims who chose not to report, feelings of helplessness, shame, and embarrassment are leading reasons for remaining silent after a scam. Slightly less than two-thirds (65%) of victims felt as though the damage was irreparable, with 39% saying they felt ashamed or embarrassed and opted not to report.

Scam Victims Skip Reporting for Fear of Irreparable Damage and Negative Perceptions

Figure 10. Scam Victims' Reasons for Not Reporting Scams



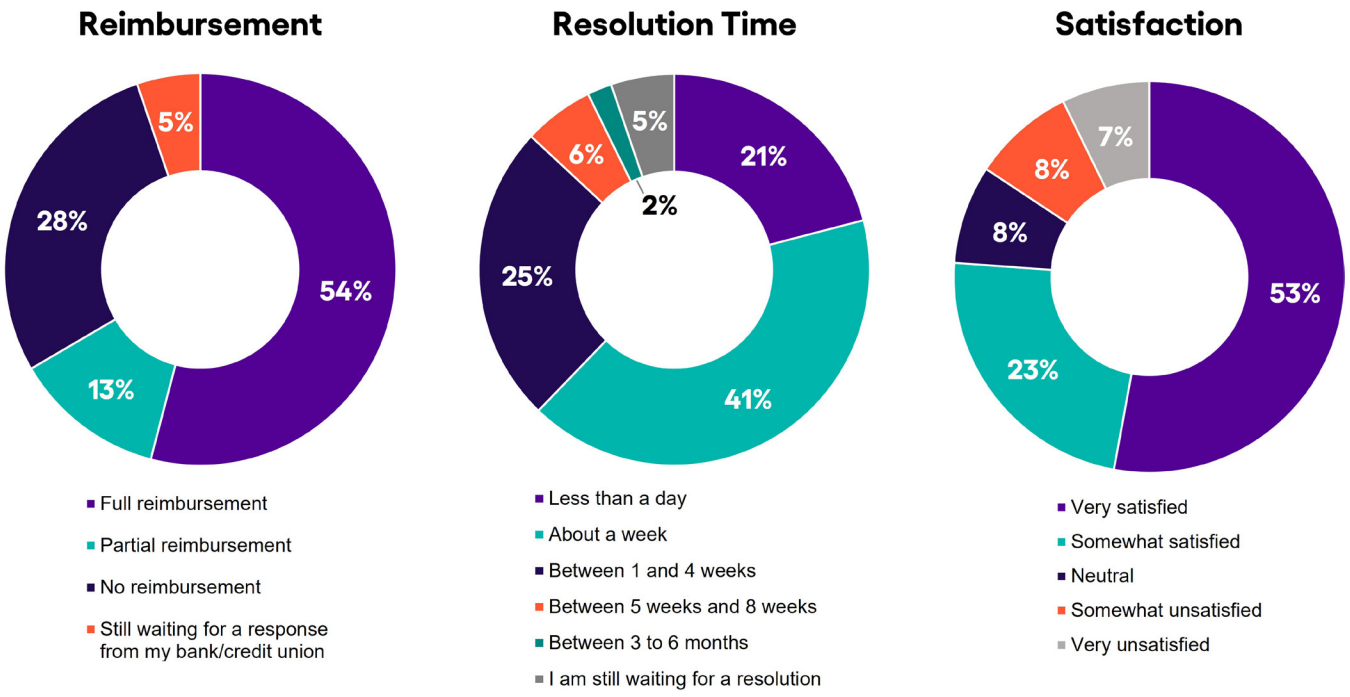
Source: Javelin Strategy & Research, 2024

Illustrating the importance of banks in consumers' lives, FIs have an opportunity to vastly improve the victim experience. With one-quarter (26%) of victims not knowing to whom they should report their scam interaction, FIs should reassess their policies and procedures, ensuring that steps post-scam are fully detailed and easily accessible through their online banking experience, as well as optimized for those who default to mobile banking.

Generally, victims who reported their scam interactions to their financial institutions are satisfied with the experience they receive. This is likely linked to the rate at which they are reimbursed and how much time is spent on the resolution of their issues. A significant number of scam victims, 54%, report getting a full reimbursement of their lost funds from their financial institution, with 13% receiving partial reimbursement, 5% waiting for a response from their financial institution, and the remaining 28% receiving no reimbursement. Overall U.S. scam reimbursement rates somewhat align with U.K. reimbursement rates for APP scams. According to the 2023 UK Finance annual fraud report, 62% of money lost to APP scams was reimbursed to the victims.[3]

Reimbursement Rates and Resolution Times Suggest Satisfaction with Financial Institutions

Figure 11. Scam Victims' Experiences with Reimbursement, Resolution Response, and Overall Satisfaction with Assistance



Source: Javelin Strategy & Research, 2024

If FIs are to continue increasing satisfaction rates among their customers who become scam victims, reimbursement policies must be reassessed, as reimbursement clearly plays a significant role in overall satisfaction in a banking relationship. Along with provisional credit offerings, FIs should use historical transaction activity and account status to earn and uphold the trust and satisfaction of the affected customer, which is critical in maintaining a long-standing financial relationship.

Currently, FIs are not required to reimburse victims for monetary losses associated with scams. However, that's not the case in every country. Scam loss liability has been a hot-button issue in the United States, especially as other regions start shifting liability from consumers to banks for certain kinds of scams. This can be challenging for many FIs. For larger banks, reimbursing scam losses (within reason) may not have much effect on their annual financial performance, but for smaller community banks and credit unions, reimbursement can have considerable impact. This should be a leading motivator for FIs to make sure real-time scam detection and prevention measures are in place to keep pace with criminal activity.

Although 21% of scam victims are hearing back from their FI in less than a day after initially reporting their scam, there is major room for improvement in reducing resolution times for victims and effectively reducing the amount of time FI employees spend resolving cases. Four in 10 scam victims are waiting one week, and another 25% of victims waiting

one to four weeks for resolution of their scam case. It's no secret that the longer a scam goes unresolved, the worse the situation can get for a victim, whether simply through the financial aftereffects of losing money or through further criminal exploitation and additional financial crimes perpetrated by using critical victim PII gleaned from the initial scam.

So, what's behind the lagging resolution times for scam victims? For one, scams lack any sort of industry standard for categorization and official reporting, thus leaving any decisioning in the hands of individual financial institutions, and often it comes down to the customer service representative or resolution case manager to make those important distinctions. Because there is no legal requirement to reimburse scam victims, FI employees must manually review each case, often requiring managerial approval for reimbursement. This proves costly for financial institutions in terms of time and in hiring expertly trained staffers to efficiently manage scam caseloads.

The Federal Reserve's FraudClassifier model[4] provides FIs with guidance for classifying different fraud types, but it largely excludes assistance in classifying most scams, with the exception of authorized payment fraud driven by impersonation schemes. Given the rising threat of scams every year, it would serve financial institutions well to know what kinds of threats their customers and members face, especially if FIs are going to eventually be legally required to resolve scam issues and reimburse victims. It's time to push for industry-wide clarity for scams.

The Role of Financial Institutions and Technology

We may never know the full scale of losses stemming from scams. With the lack of industry-wide classification and categorization for scam losses, the limitations financial institutions face in resolution time and expert staffing, and the ever-present stigma against scam victims that results in a lack of reporting, it's difficult for the financial services industry to gain full visibility into the damage caused by scams. But FIs aren't powerless in protecting their customers and members against the threat of scams. Technology providers are capitalizing on the rapid advancement of artificial intelligence and machine learning by developing solutions that play a critical role in detecting and preventing scams. The first step in effectively using innovation to lessen the impact of scams is to understand what victims would find useful within the scope of their own accounts.

Scam victims find tools and features that aid in the confirmation of all aspects of the payment process incredibly useful in preventing scams. Tools that verify the authenticity of communication (in all forms) from their bank (86%), pop-up messages before a payment is finalized (81%), and verify new payee information (78%) all rank high on the priority list of scam victims. As bank impersonation scams continue to trouble consumers,[5] FIs must regularly confirm with consumers the authentic ways they may establish contact through information that is easily accessible and posted prominently on the website and readily available when a customer is logged into an online or mobile banking session. This should include reasons the institution may contact customers and members, as well as the email addresses and text numbers from which communication may come. Scam victims also place a high value in customer service support that offers guidance in times of need (84%).

Scam Victims Want Preventive Measures In Place

Figure 12. Tools and Actions Scam Victims Find Useful in Protecting Accounts, by Percentage

Source: Javelin Strategy & Research, 2024

javelin

Particularly noteworthy is the drop-off in interest in preventive measures that may result in payment lags. Daily limits for all kinds of payments (61%) and payment holds for up to 48 hours (58%) don't possess the same value that scam victims find in features that would be helpful before a payment is actually made. FIs must find the balance of friction and convenience in minimizing scams, and that includes injecting a reasonable amount of optimal friction—the friction that a consumer might expect and often desire—in the examples above.

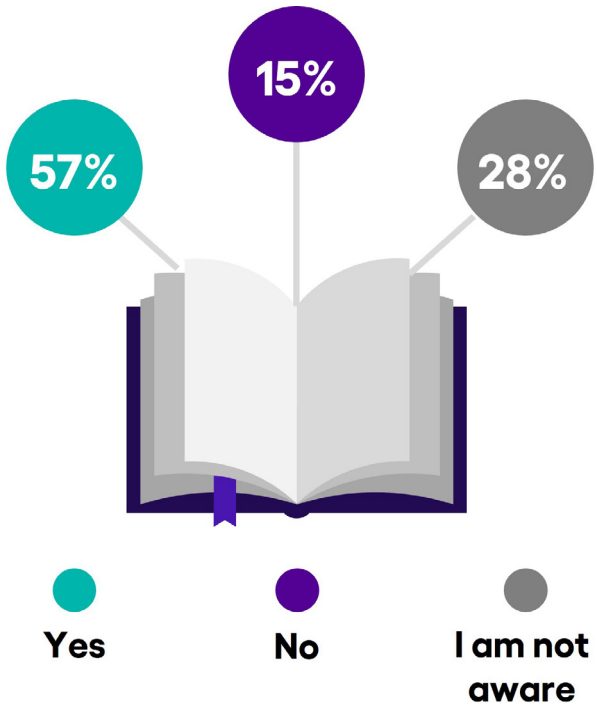
Payment prompts and warning messages injected into the pre-payment flow are an effective precautionary method by which FIs assist consumers in determining the risk of sending a payment, affording the customer much-needed time to recognize red flags with suspicious transactions before completing a payment. National Australia Bank has saved its customers more than $50 million in potential scam transactions,[6] demonstrating the value of appropriately placed alerts before the completion of a transaction. Technology that uses a data-driven approach in detecting scams by using key aspects of a consumer's profile—such as historical account data as well as behavioral biometrics and device intelligence—can determine the risk level of a transaction in real time, saving the potential scam victim and the FI from a costly headache.

Education continues to play a vital role in the fight against scams. FIs that expose their customers to regularly updated scam education provide a stronger foundation in detecting suspicious behavior and preventing illegitimate transactions. Scam victims' awareness of education provided by their FI is shockingly low, with just over half (57%) of victims reporting that their FI's website and mobile app house scam-related education. Of the remaining 43% of scam victims, more than one-quarter (28%) are not aware of any scam education provided by their FI. Because of the plethora of scam-related education from various sources across the web, FIs should consider personalizing education in online and mobile app banking sessions, creating targeted lists of pertinent articles and tips for each customer based on demographics and spending habits.

Financial institutions are highly trusted by consumers, so they have an opportunity to make or break the experience for scam victims. Consumers place an immense amount of trust in their FI, entrusting banks with their livelihoods and personal information, and it is incumbent upon FIs to uphold and build on that trust. Removing unnecessary burdens of scam detection, treating victims with empathy, and protecting customers with innovative scam detection technology can turn the negative experience of a scam victim into a positive outcome for the victim, drastically alleviating the long-lasting financial and emotional impact of scams.

Too Many Scam Victims Are Unaware of FI-Provided Scam Education

Figure 13. Awareness of Scam Education Provided by Financial Institution



Source: Javelin Strategy & Research, 2024

Methodology

The Javelin Strategy & Research 2024 Scam and Financial Loss survey was conducted online among 500 U.S. adults, over the age of 18, who were victimized by at least one scam resulting in monetary loss in the past two years; this sample is representative of the U.S. Census demographics distribution. Data collection took place in May 2024. Data is weighted using 18-plus U.S. population benchmarks on age, gender, race/ethnicity, education, census region, and metropolitan status from the most current CPS targets. Due to rounding, the percentages on graphs may add up to 100% plus or minus 1%.

To preserve the independence and objectivity of this report, sponsors of this project were not involved in the tabulation, analysis, or reporting of the final results.

Endnotes

1 Empower, "37% of Americans can't afford an emergency expense over $400." Published July 2, 2024; accessed July 2, 2024

2 Finextra, "Banks to be given more time to investigate APP fraud." Published March 12, 2024; accessed June 26, 2024

3 The Banker, "Card ID theft on the rise in the UK." Published May 2024; accessed June 28, 2024

4 Federal Reserve, "FraudClassifier Model." Accessed July 1, 2024

5 Federal Trade Commission, "New FTC Data Analysis Shows Bank Impersonations Most Reported Text Message Scam." Published June 8, 2023; accessed July 2, 2024

6 News.com.au, "NAB customers 'abandoned' $50m in possibly fraudulent sales." Published Nov. 29, 2023; accessed July 3, 2024

About BioCatch

BioCatch stands at the forefront of digital fraud detection, pioneering behavioral biometric intelligence grounded in advanced cognitive science and machine learning. BioCatch analyzes thousands of user interactions to support a digital banking environment where identity, trust, and ease coexist. Today, more than 30 of the world's largest 100 banks and 196 total financial institutions rely on BioCatch Connect™ to combat fraud, facilitate digital transformation, and grow customer relationships. BioCatch's Client Innovation Board – an industry-led initiative featuring American Express, Barclays, Citi Ventures, HSBC, and National Australia Bank – collaborates to pioneer creative and innovative ways to leverage customer relationships for fraud prevention. With more than a decade of data analysis, 92 registered patents, and unmatched expertise, BioCatch continues to lead innovation to address future challenges. For more information, please visit www.biocatch.com.

About Javelin

Javelin Strategy & Research, part of the Escalent family, helps its clients make informed decisions in a digital financial world. It provides strategic insights to financial institutions including banks, credit unions, brokerages and insurers, as well as payments companies, technology providers, fintechs and government agencies. Javelin's independent insights result from a rigorous research process that assesses consumers, businesses, providers, and the transactions ecosystem. It conducts in-depth primary research studies to pinpoint dynamic risks and opportunities in digital banking, payments, fraud & security, lending, and wealth management. For more information, visit www.javelinstrategy.com.

Follow us on
X and LinkedIn

javelin