javelin | PrivacyGuard

Fraud Resolution:
Harnessing the Power of the White Glove

WHITEPAPER | AUGUST 2024

Table of Contents

Table of Figures

© 2024 Escalent and/or its affiliates. All rights reserved.

javelin

Meet the Author

Jennifer Pitt
Senior Analyst, Fraud & Security

Jennifer Pitt is a senior analyst in Javelin's Fraud & Security practice. She analyzes data and trends and provides recommendations to financial professionals regarding best practices for fraud prevention and cybersecurity.

Foreword

This report, sponsored by PrivacyGuard, explores the immediate and long-term risks associated with identity fraud and account takeover fraud for organizations and consumers and establishes a case for employing a guided, white-glove approach to fraud protection and resolution.

This report was adapted from the 2024 Identity Fraud Study: Resolving the Shattered Identity Crisis, published by Javelin Strategy & Research in April 2024. Javelin Strategy & Research maintains complete independence in its data collection, findings, and analysis.

Overview

As identity fraud and account takeover fraud losses sharply increase, fraud victims are left wondering how to resolve complex fraud incidents and how to prevent them from happening again. Fraud resolution can be an overwhelming and time-consuming process, and many victims are not sure where to start. Financial service providers must lend support to fraud survivors and potential victims. A white-glove approach to fraud protection and resolution will be the key to keeping customers and building trust. This more hands-on, guided approach will require that FIs provide consumer alerts in near real time, prompt consumer discussions about fraud trends and typologies, engage in early transparency about the fraud resolution process, and leverage the enlistment of dedicated fraud resolution specialists who can guide fraud victims through the entire resolution process.

© 2024 Escalent and/or its affiliates. All rights reserved.

Executive Summary

Traditional identity fraud losses in 2023 totaled $22.8 billion, an increase of 13% from 2022. Among those identity fraud losses, account takeover fraud accounted for more than half of the loss, at $12.7 billion[1]. Account takeover fraud is prolific because of the number of linked accounts, which are usually more heavily funded than new accounts. Financial service providers must anticipate additional fraud on compromised accounts and protect their customers' accounts from future fraud.

43% of fraud victims who were victimized in the past 12 months suggested that their FI improve its resolution processes by providing a fraud resolution representative. Fraud victims have stated that, in general, they want more support during the reporting and resolution processes. Enlisting the help of dedicated fraud resolution specialists can help reduce the number of resolution hours victims are required to spend. This guided, customer-oriented approach can also assist in empowering victims.

The majority (70%) of fraud victims did not have an active identity protection service at the time of their fraud incident. IDPS products can be instrumental in detecting, preventing, and resolving fraud by offering a suite of monitoring and alerting tools and dedicated fraud resolution specialists. This customer base without IDPS services is a gap that can be closed by FIs that partner with IDPS providers to offer free or discounted services to their customers.

Average out-of-pocket costs for fraud victims rose by 70% in 2023. The costs, which rose from an average of $119 in 2022 to an average of $202 in 2023[2], included unreimbursed fraudulent transactions and miscellaneous expenses like overdraft and late fees. Though a few hundred dollars may not seem like a lot of money for out-of-pocket costs, the amount could be devastating for victims who are on a fixed income.

Fraud victims make major financial changes after their victimization. Almost one third (30%) of fraud victims with a household income of $50,000 to $99,000 now avoid certain merchants, 19% closed the account where the fraud occurred, and 21% now spend less money. Identity fraud victims who do not feel they've experienced top-tier fraud prevention and resolution are not afraid to overhaul their financial portfolios to ensure the security of their accounts and identities.

Older consumers want automatic fraud alerts from their FIs. Though consumers of all ages value automatic alerts from their FIs, older adults especially value several types of automatic alerts. In fact, 81% of consumers 55 and older would feel more protected from identity fraud if their bank automatically alerted them when personally identifiable information was exposed in a data breach. And nearly three-quarters of consumers 55 and older reported that they would feel more protected from identity fraud if their FI automatically alerted them of any new financial accounts opened using their personal information.

Victims struggle emotionally because of fraud. Fraud victims—who are often unsure exactly how their information or accounts were compromised—are left wondering how to resolve complex fraud incidents and how to prevent them from happening again. Fraud resolution can be a difficult and daunting process, and many victims feel paralyzed by time-consuming resolution processes that they are often left to navigate on their own. Fraud victims often feel helpless and alone, and they need a dedicated fraud resolution professional as an advocate.

Financial service providers face repercussions when they fail to prevent or resolve fraud. FIs and other organizations not only lose money because of fraud and lackluster resolution but also can lose customers. FIs with inadequate fraud prevention and resolution processes can also be subject to consent orders, fines, or civil actions, which can lead to additional regulatory oversight and audits as well as the added time and cost of hiring personnel to remedy the situation.

© 2024 Escalent and/or its affiliates. All rights reserved.

Recommendations

Provide guided, white-glove fraud resolution solutions. Victims often feel heavy emotional burdens from their experiences with fraud. Resolution processes are complex, and victims are unsure how to navigate the process on their own. With the plethora of resources available online, often with conflicting information and differing guidance, fraud victims are not sure what advice to follow. Fraud victims need someone in their corner who can guide them through the entire resolution process. FIs should become a lifeline for fraud victims.

Encourage customers to set accountholder-initiated alerts. Members should understand the benefits of setting transaction or location limits and alerts on their accounts. These limits (which would essentially block transactions) or alerts can be easily updated by the customer.

Alert customers to account, user, and transaction changes in real time. Consumers should automatically be alerted to any changes to their user credentials, account profile, authorized users, and transaction patterns, and those changes should be subject to their approval. Alerting customers to these changes in real time will help reduce account takeover fraud.

Empower consumers to be in control of their financial well-being. Fraud victims often feel helpless and alone. By keeping customers informed (from the beginning) about fraud red flags and typologies, how to access and make the best use of educational resources, and how to navigate fraud resolution processes, FIs will help empower consumers to better detect and prevent future suspicious activity.

Partner with identity protection service providers. IDPS providers offer comprehensive fraud solutions and dedicated fraud resolution specialists. By using such partnerships to provide consumers with free or discounted IDPS services, FIs can help combat fraud and build customer trust.

© 2024 Escalent and/or its affiliates. All rights reserved.

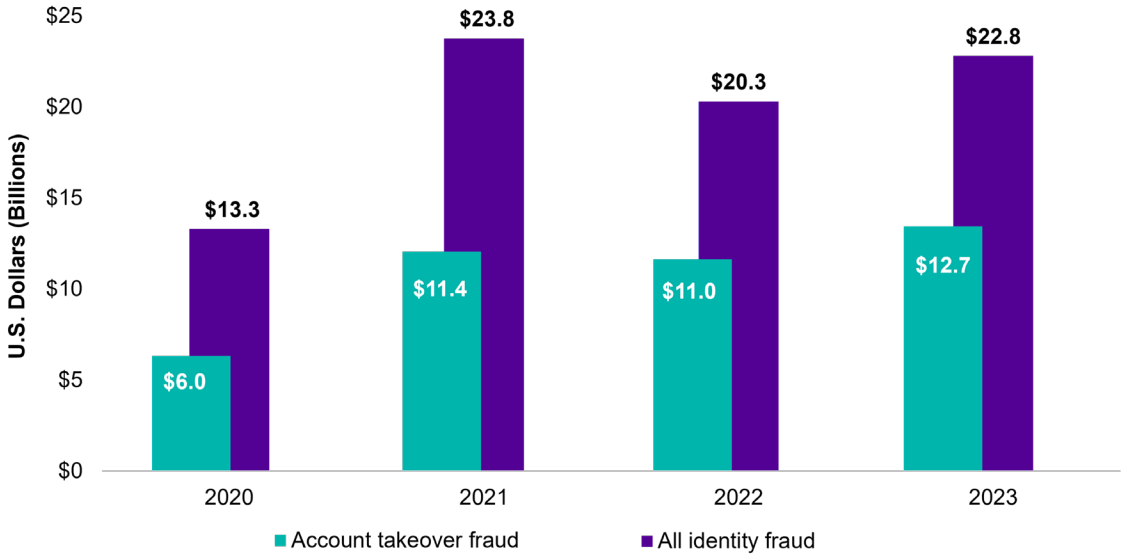
Fraud Costs More Than Just Money

As fraud and cyberattacks increase, consumers continue to become identity fraud victims, and they are often in shock that they have become "part of the statistic." Fraud victims—who are often unsure exactly how their information or accounts were compromised—are left wondering how to resolve complex fraud incidents and how to prevent them from happening again. Fraud resolution can be a difficult and daunting process, and many victims feel paralyzed by time-consuming resolution processes that they are often left to navigate alone. Financial institutions must become a lifeline for fraud survivors and consumers who may become fraud victims in the future. FIs can do this by implementing a guided, white-glove approach to fraud prevention and resolution that will ultimately empower consumers.

Although the number of victims stayed fairly consistent in 2023, identity fraud losses sharply increased. Traditional identity fraud losses in 2023 were $22.8 billion, an increase of 13% from 2022. Among those identity fraud losses, account takeover (ATO) fraud accounted for over half of the overall loss, at $12.7 billion (an increase of 15% over the previous year)[3]. What's more, ATO fraud losses accounted for nearly half of all identity fraud losses from 2020 to 2023, which showcases the devastating effects of account takeover.

Account Takeover Fraud Accounts for Nearly Half of All Identity Fraud Losses

Figure 1. Dollar Loss of Account Takeover Fraud vs. All ID Fraud (from 2020-2023)



Source: Javelin Strategy & Research, 2024

One of the reasons ATO fraud accounts for so much of total identity fraud is that established accounts—which have already gone through rigorous onboarding and know-your-customer processes—typically contain more funds than new accounts. Additionally, existing accounts are already linked to a variety of financial and non-financial accounts, including checking and savings, credit cards, utilities, email, and social media. This gives criminals ample opportunity to more easily take over a variety of linked account types.

© 2024 Escalent and/or its affiliates. All rights reserved.

javelin

Unfortunately, many financial service providers address only the current fraud and compromised accounts; they do not anticipate future fraud with linked information or accounts, and they typically do not advise their customers on how to protect non-compromised information or accounts. Financial service providers and fraud victims must assume that if one piece of victim information or one account has been compromised, others have already been compromised (or will be in the future). To distance themselves from the fraud, criminals do not always use all the stolen information immediately. Instead, they often keep some of the stolen information for years before using it. Many fraud professionals suggest that consumers simply change the information that has been affected by fraud, but that is not always realistic and does not always prevent additional fraud. Though account numbers, email addresses, and phone numbers can be changed, information like Social Security numbers and dates of birth cannot be changed under most circumstances.

Financial service providers must provide a white-glove approach to fraud resolution. This consists of guidance through the fraud resolution process, during which dedicated resolution specialists can assist consumers in understanding fraud red flags and walk consumers through the fraud resolution process, which includes critical steps such as implementing fraud prevention and data security methods as well as contacting reporting agencies.

With white-glove fraud resolution, dedicated fraud resolution specialists can assist with ensuring that all linked accounts and information are protected from current and future fraud. Though nothing is truly fraud-proof, credit freezes and locks, monitoring of all linked accounts, and real-time alerts can be utilized to help prevent future fraud on victims' accounts.

© 2024 Escalent and/or its affiliates. All rights reserved.

Victims And Businesses Feel Significant Impacts From Fraud

Unfortunately, many fraud victims fail to report their fraud incidents. This can be attributed to several factors. In the case of scams, victims may feel embarrassed or ashamed that they "fell for it" (though anyone can be a victim and there's no reason for shame). But in the case of non-scam-related identity fraud, victims usually do not feel the same sense of embarrassment or shame. Their information was taken by these cybercriminals without the victim's authorization or assistance. Yet many still fail to report fraud, mainly because the reporting and resolution process is too difficult and too time-consuming. And many fraud victims are not even sure whom to contact.

Depending on the information that was compromised, the fraud reporting and resolution process often involves separate communications to several entities, including banks, credit card companies, credit bureaus, law enforcement, the Department of Motor Vehicles, the Social Security Administration, and the Federal Trade Commission. Because many organizations do not cross-report or efficiently share information, fraud victims are left to contact each organization. Because of this, it is often easier for these victims (and many FIs) to simply take the loss and chalk it up as "a learning experience" or "the cost of doing business."

And oftentimes, victims who do report their fraud incidents disclose feelings of additional stress because of the difficulties with the reporting and resolution processes and the sheer number of organizations they must contact. Repeatedly rehashing details of the fraud incident often leaves fraud survivors feeling frustrated and re-victimized.

Fraud victims have stated that, in general, they want more support during the reporting and resolution processes. In fact, 43% of fraud victims who reported fraud to their FI suggested that their FI and other service providers improve their fraud resolution processes by providing a dedicated fraud resolution representative, a role typically associated with a white-glove fraud resolution experience.

Identity fraud resolution can be a daunting task and require countless dedicated hours of document collection, phone calls, or online reporting. In 2023, the average number of hours fraud victims spent resolving fraud incidents hit 10 hours, a rise from six in 2022[4]. This could be because fraud is becoming more complex, resolution processes are complicated and involved, and consumers are beginning to take control of their own financial well-being.

In addition to the increase in the average number of resolution hours, the average out-of-pocket costs for fraud victims also rose. These costs rose from an average of $119 in 2022 to an average of $202 in 2023 (a 70% increase)[5]. Most of these incurred costs for 2022 and 2023 included unreimbursed fraudulent transactions and miscellaneous costs like overdraft and late fees. Although $200 may not seem like a significant amount of money, for those on a fixed income or living paycheck-to-paycheck, such costs may not be bearable. White-glove fraud resolution services can be employed to cover or help recover these costs for victims.

© 2024 Escalent and/or its affiliates. All rights reserved.

In addition to financial loss, fraud victims suffer a heavy emotional burden and extreme physical stress. Surprisingly, financial stress was not reported as the biggest impact of being a fraud victim. More fraud survivors reported suffering from emotional stress after becoming a victim. In fact, in 2023, 69% of fraud victims reported being emotionally stressed because of their fraud incident, whereas 56% reported being financially concerned.

Emotional Burdens Carry Heaviest Victim Impact

Figure 2. Percentage of Fraud Victims Who Report Severe Impacts of Fraud Victimization (by Stress Type)

Source: Javelin Strategy & Research, 2024

Many fraud victims say fraud has made them feel violated and paranoid that it will happen again. Because of that, victims often take steps—like activating fraud alerts—to help combat future fraud victimization.

After a fraud incident, victims change their spending habits and adjust whom they do business with.

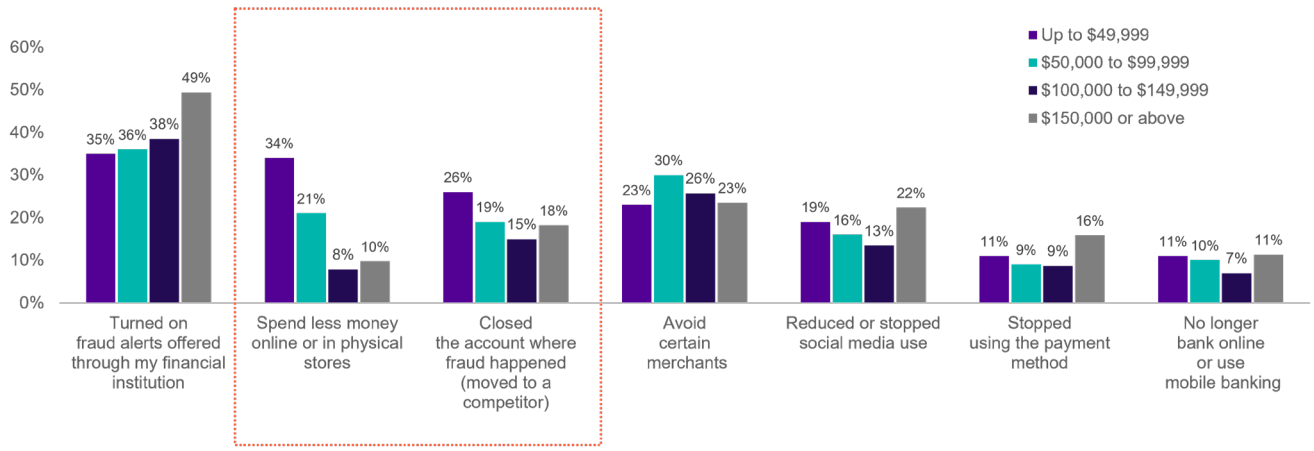
In 2023, 26% of fraud victims report avoiding certain merchants after a fraud incident, and 20% of fraud victims in 2023 closed their accounts and went to a competitor[6], with both percentages increasing from 2022. This staggering data shows that FIs and other organizations are not immune to losing customers because of fraud incidents. In fact, some consumers who experience fraud hold their FI accountable and will not hesitate to switch to a different bank, one they feel will protect their information and help them avoid fraud victimization.

© 2024 Escalent and/or its affiliates. All rights reserved.

Surprisingly, responses to fraud vary depending on household income. After fraud victimization, higher income consumers tend to rely more on implementing fraud alerts, while lower-income to average-income consumers tend to make significant financial changes (like spending less money and closing accounts where the fraud occurred), while. Of fraud victims with an annual household income of less than $50,000, 26% closed the fraud-related account, and 34% spend less money because of being a fraud victim. For those fraud victims with a household income of $50,000 to $99,000, 30% avoid certain merchants, 19% closed the account where the fraud occurred, and 21% spend less money.

Responses to Fraud Vary With Income

Figure 3. Steps Taken by Fraud Victims After a Fraud Incident (by Income Level)



Source: Javelin Strategy & Research, 2024

Such consumers do not have as much discretionary income and therefore must take every possible step to increase savings and reduce fraud. On the other hand, consumers with higher discretionary incomes tend to believe it is easier just to take the financial loss than it is to move accounts to another provider and change spending habits.

Consumers are not the only ones who suffer because of increased fraud and poor resolution practices; businesses also bear a burden. FIs and other organizations not only lose money because of fraud and lackluster resolution but also can lose customers. Consumers continue to report poor treatment and insufficient resolution from fraud professionals.

When asked how identity fraud has affected their lives, victims noted that fraud resolution was difficult. They could not use their bank accounts until resolution was completed.

And they lost all faith in the fraud investigation and resolution processes.

© 2024 Escalent and/or its affiliates. All rights reserved.

javelin

If financial service providers fail to prevent or detect fraud, or if they fail to adequately and easily resolve fraud, customers will choose different providers. Consumers lose trust in FIs that fail to remedy fraud situations or those that provide poor customer service during fraud investigation and resolution processes. Poor contact center support is a top reason fraud victims will consider closing all accounts at their primary financial institution. In fact, 37% of fraud victims will consider leaving their financial institution just because of poor customer service experiences. And 30% of fraud victims would consider leaving their financial institution just because of the fraud experienced on their account.

Additionally, if financial service providers fail to adequately prevent, detect, investigate, or resolve fraud, they can also be subject to consent orders, fines, or civil actions. These actions can directly result from failure to adequately educate consumers about fraud, failure to implement sufficient controls and security measures necessary to prevent and detect fraud, and failure to resolve or reimburse fraud.

In January 2024, the New York Attorney General's Office filed a civil lawsuit, citing Citibank's failure to protect and reimburse fraud victims, which ultimately led to millions of dollars in out-of-pocket costs for New York-based Citibank accountholders. The lawsuit further notes that these victims lost their hard-earned savings because of lax data security, ineffective fraud monitoring systems, failures of real-time fraud detection and response, lackluster fraud investigations, and an outright refusal to reimburse victims. The New York Attorney General's Office is asking that Citibank be required to reimburse all affected fraud victims and implement robust fraud and security controls to mitigate future fraud and security incidents[7].

Civil suits like this can be detrimental to many financial service providers and can lead to additional regulatory oversight and audits as well as the added time and cost of hiring personnel to remedy the situation. Situations like these can not only result in steep fines to the organization but also put the reputations of FIs and other organizations at risk. No one wants to do business with a company that allows fraud or will not help anyone resolve fraud. And continued fines and lawsuits could repel investors and ultimately lead to shuttering of the business. Investment in a white-glove fraud resolution experience will ultimately prevent exorbitant fines incurred from regulatory and legal action, as well as prevent the loss of consumers and investors.

© 2024 Escalent and/or its affiliates. All rights reserved.

White-Glove Fraud Services Empower Consumers

Because of the severe financial, emotional, and physical impacts of fraud, victims need an advocate in their corner, an expert who can walk with them through the entire resolution process. Victims want to feel like they are not alone. The best way to do that is to provide a white-glove, guided approach to fraud prevention and resolution. White-glove experiences are typically associated with high-end luxury services that go out of their way to provide a superb customer experience. White-glove experiences can be implemented into any type of service, including fraud prevention and resolution.

White-glove fraud services should encompass fraud prevention—which includes educational resources and fraud alerts—as well as guided resolution. Unfortunately, white-glove-style fraud prevention and resolution are not offered by every financial service provider.

Fraud prevention education needs improvement–many financial institutions provide resources that are too long and ineffectual. Fraud and cyber-related educational materials must be easier to find and digest. Instead of just placing fraud educational resources on the organization's website in only a few formats—mostly lengthy, hard-to-find articles—fraud prevention education should be provided on various channels in interactive and engaging formats, like assessments, quizzes, and games. Consumers should be provided information at account opening on where to find educational resources. Additionally, bespoke fraud red-flag notifications should be sent to consumers so they are aware of the warning signs before the fraud occurs. These notifications (which differ from fraud alerts) should be tailored specifically to a consumer's behavior, transaction activity, and/or demographic. For example, if a customer transacts regularly using P2P payments, a notification about P2P fraud should be delivered. If a consumer is older, a notification about scams targeting older adults should be communicated. These notifications will help empower consumers to better detect and prevent future suspicious activity.

CONSUMERS WANT TO BE ALERTED TO FRAUD

In addition to education, fraud alerts are valuable for fraud prevention and detection. In fact, 77% of consumers who signed up for fraud alerts find them helpful. Unfortunately, not all consumers are utilizing these alerts. Nearly one-quarter (23%) of consumers are not signed up for or do not remember if they are signed up to receive fraud alerts from their financial institution.

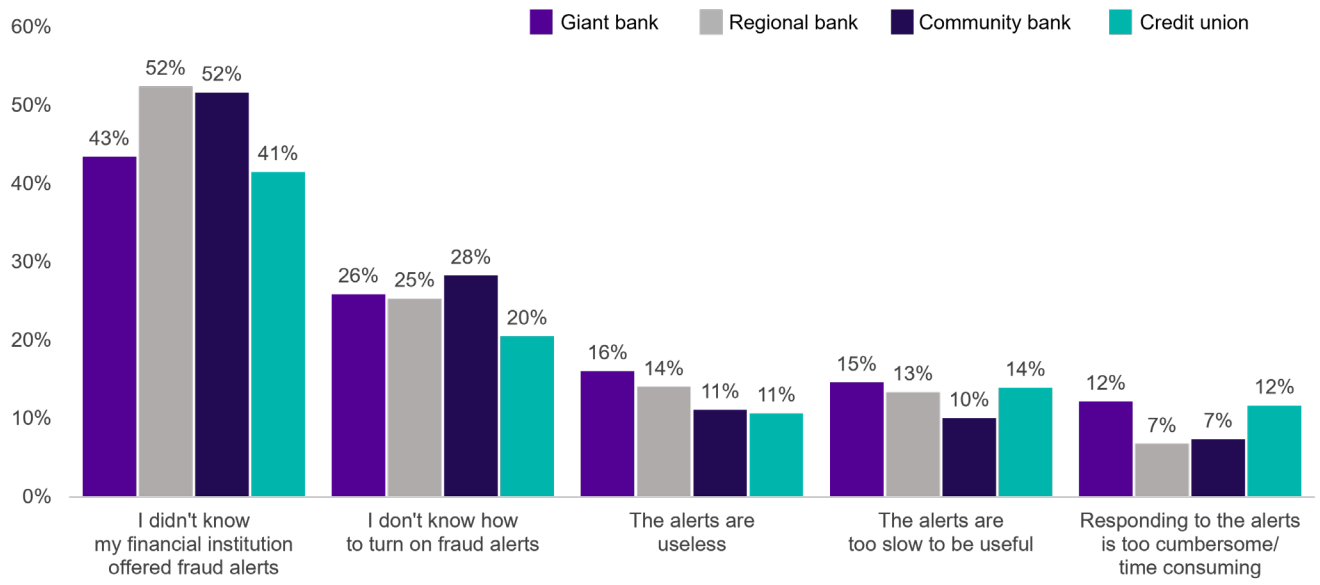
Many consumers are not aware how to turn on fraud alerts, and some consumers are not even aware that their FI offers such alerts. In fact, of those consumers who have not signed up for fraud alerts, 27% said they did not know how to turn on the alerts. This number does not differ much among accountholders at financial institutions of various sizes.

Additionally, 48% of consumers who have not signed up for fraud alerts noted that they were unaware their FI even offered the alerts. Interestingly, this number does vary among consumers who bank at different types of financial institutions. Around 40% of consumers who bank with either credit unions or giant-sized banks report that they did not know their FI even offered fraud alerts, whereas more than 50% of consumers who bank at community or regional banks reported the same.

© 2024 Escalent and/or its affiliates. All rights reserved.

Lack of Awareness Tops the Reasons for Activating Fraud Alerts

Figure 4. Reasons for Not Signing Up for FI Fraud Alerts (by Bank Size)



Source: Javelin Strategy & Research, 2024

Although we often assume community banks are better at providing more hands-on guidance and personal experience with their members, giant banks clearly are doing a bit better at socializing their customers to alerts.

But these staggering figures show that financial institutions of all sizes still have a long way to go with informing their members about fraud alerts, their benefits, and how to effectively use them. All FIs should consider reevaluating their budgets to include fraud and account alert education and awareness campaigns.

FIs that employ a white-glove experience ensure that their customers are well-informed about fraud alerts at account opening and throughout the account lifecycle. The guided, customer-oriented approach can also be implemented to help consumers understand the type of alerts offered and how these alerts can help prevent and detect fraud.

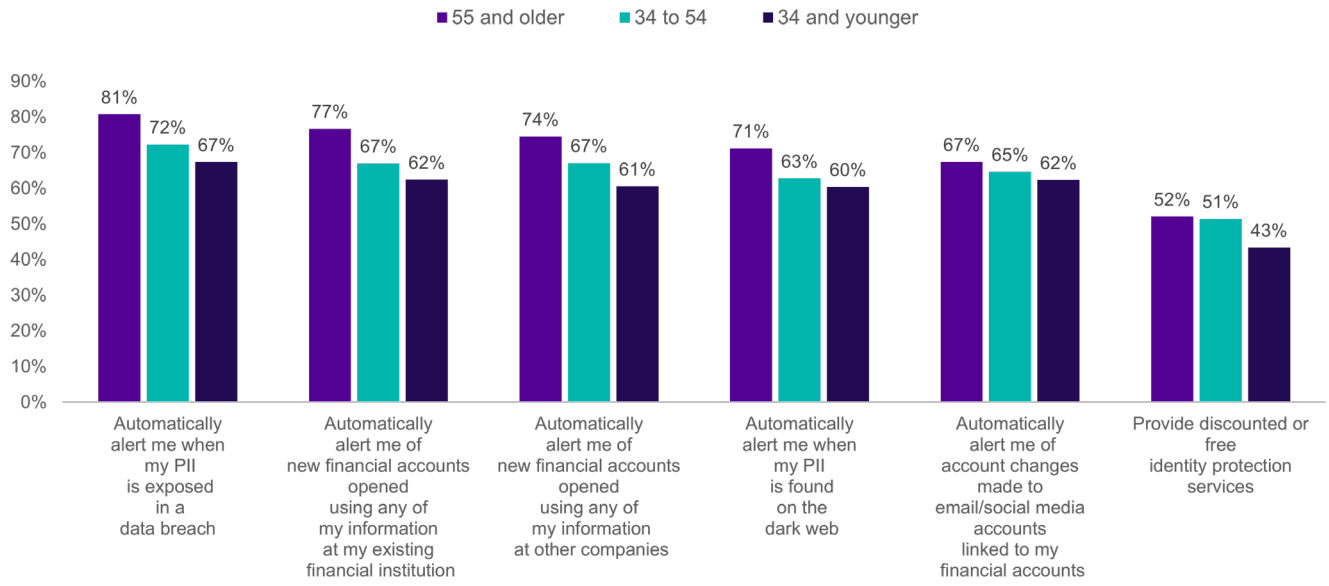
Even though some consumers are not aware of the presence of fraud alerts or how they work, most consumers concerned about identity fraud say they would feel more protected if their FI automatically alerted them to account changes or exposed personal information. Older consumers tend to value automatic alerts more than younger consumers. In fact, 81% of consumers 55 and older would feel more protected from identity fraud if their bank automatically alerted them when PII was exposed in a data breach, whereas only 67% of consumers 34 and younger would feel more protected if they were given the same alert. Additionally, around 75% of consumers 55 and older reported that they would feel more protected from identity fraud if their FI automatically alerted them about any new financial accounts opened using their personal information, whereas around 61% of consumers 34 and younger would feel the same.

© 2024 Escalent and/or its affiliates. All rights reserved.

javelin

Consumers Feel More Protected With Automatic Alerts

Figure 5. Ways to Make Consumers Feel More Protected from Identity Fraud (by Age)



Source: Javelin Strategy & Research, 2024

Consumers want their FIs' assistance in detecting fraud and alerting them to it. But FIs must close the age gap on the use of automatic alerts. Automatic alerts are critical in understanding what information has been compromised and where the information was found. FIs must assure younger consumers that, although addressing identity fraud in the current landscape of excessive data breaches may seem like a losing battle, using automatic alerts may help mitigate the degree of successful fraud.

As ATO victims find that criminals most often change their passwords and email addresses, any detected account changes and user changes—like changes in login credentials, personal and contact information, and the addition of users—should be sent as real-time automatic security alerts that customers can also address in real time. By providing automatic alerts to consumers of all ages for various changes to their user information, accounts, or transactional behavior, consumers will be empowered to engage in their own identity and account security, and the burden to detect fraud will not lie entirely with them.

In addition to automatic security alerts, accountholder-initiated alerts are valuable. White-glove fraud prevention experiences provide users the option to set limits on transaction amounts, types, locations, and merchant types. Some users who very rarely engage in specific types of transactions (like wires) might want to set an alert or limit on wire transfers. Allowing consumers to set and change these transaction alerts empowers consumers to take control of their financial well-being. These alerts should be offered on various channels (via push notification through the app, SMS text, email, and phone call).

© 2024 Escalent and/or its affiliates. All rights reserved.

CONSUMERS WANT GUIDED FRAUD RESOLUTION

Financial service providers should provide a quick, high-level overview of the fraud resolution during onboarding, before fraud occurs, so fraud victims know how the process generally works. Even though the internet contains vast fraud prevention and resolution resources, it is difficult for victims—who are in shock amid a fraud incident—to determine which resolution strategies are the most effective and efficient. Victims are left frustrated and often paralyzed about what steps to take. It is often difficult to know whom to ask for help, and sometimes it is difficult to even ask for help in the first place. No one wants to be a victim. But everyone needs help sometimes. Fraud resolution processes are often confusing and time-consuming, and victims are often left to fend for themselves in figuring out how to resolve their incidents.

Many FIs still do not even educate their customers on fraud resolution processes. And those that do typically point fraud victims to a link or site containing resolution steps that are not accompanied by explanations of why these steps need to be taken or how long each step will take. And unfortunately, many FIs often require the victim to complete these time-consuming resolution steps on their own.

Through field research, Javelin discovered that, unsurprisingly, many FIs feel that consumer satisfaction remains low with regard to fraud resolution, causing customers and members to leave their institutions because of it. Several FIs are attempting to increase customer satisfaction with fraud resolution by restructuring their fraud and customer service teams and cross-training employees on fraud and customer service. But many FIs still struggle with successfully implementing customer-oriented fraud resolution programs. FIs still grappling with this issue should implement a true white-glove experience with dedicated fraud resolution specialists. These specialists can advocate for victims by joining them for the entire resolution journey.

White-glove resolution services should include a fraud toolkit—essentially a packet of information provided to and reviewed with the victim, including a high-level fraud process overview, a list of next steps, a list of organizations to contact, a fraud checklist (detailing information and documents needed from the victim about the fraud incident), and fraud and cyber prevention educational resources to help customers avoid becoming a victim again. Dedicated fraud resolution specialists will assist victims with understanding the overall fraud resolution process, aid in completing fraud resolution steps, inform victims of the expected timeframes of each step, and help victims gather necessary documentation. Dedicated resolution specialists will also assist with contacting agencies and organizations, keep victims informed about the status of any investigation, and help secure and protect victims' information from future fraud.

Rather than simply signing a temporary or limited power of attorney to allow the financial service provider to resolve fraud without involvement from the victim, consumers should be involved in the entire resolution process. Even though the process may be simpler with a power of attorney in place, it is never the best idea to give financial power of attorney to an unknown person. Though it may be rare for financial professionals to exploit being granted financial power of attorney, it does happen. Additionally, there may be something the consumer needs to add or clarify, as well as information the consumer might recall only after going through the resolution process with a professional.

Being assigned a dedicated fraud resolution specialist will help victims feel empowered and not alone.

© 2024 Escalent and/or its affiliates. All rights reserved.

IDPS SERVICES ARE INVALUABLE IN THE FIGHT AGAINST FRAUD

Consumers can become fraud victims in several ways, including being manipulated and socially engineered by scammers or experiencing the theft of their credentials or information in hacks and data breaches.

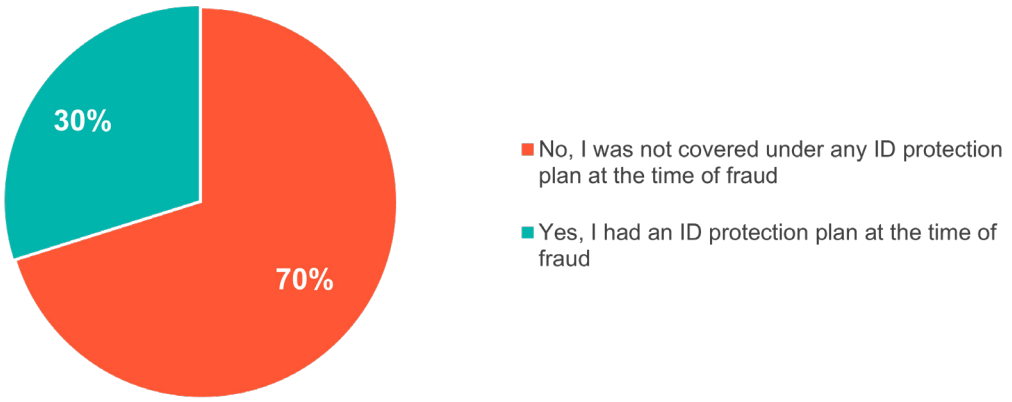
Sadly, the number of data breaches and leaks continues to increase, and consumers are left to figure out how to protect their information from further misuse through fraud. According to the Identity Theft Resource Center, there were 3,205 data compromises—which includes company data breaches and leaks—in 2023 (a drastic increase from the 1,801 data compromises in 2022), affecting more than 353 million consumers. The financial service industry experienced the second-highest number of data compromises, with 744, behind only the healthcare industry. In 2023, sensitive personal information was the most compromised type of information[8].

With the high number of data breaches and leaks, consumers must protect and secure their information. Identity protection services (IDPS) can be invaluable in fraud detection, prevention, and resolution. IDPS service providers are instrumental in not only assisting consumers in avoiding fraud (by being educated and alerted to suspicious account activity) but also in resolving fraud through a white-glove, guided approach. Comprehensive IDPS solutions often include a suite of fraud protection and resolution services, including credit monitoring, dark web scanning, bank account monitoring, Social Security number and driver's license monitoring, secure browsers, identity theft insurance, and a dedicated fraud resolution specialist.

Even though IDPS services are useful in preventing and detecting fraud, the majority (70%) of fraud victims did not have an active IDPS service at the time of their fraud incident.

Most Fraud Victims Lacked IDPS Coverage

Figure 6. IDPS Coverage at the Time of the Fraud Incident



Source: Javelin Strategy & Research, 2024

The large gap in IDPS coverage speaks to why account takeover and other fraud typologies continue to increase. Without the support of expert practitioners such as IDPS providers, account and PII abuse run rampant. FIs can help close this gap not only by informing their customers about the need to subscribe to IDPS services but also by partnering with IDPS providers to offer free or discounted services to FI customers. Consumers must be made aware of the benefits of IDPS services and how they can help reduce fraud.

© 2024 Escalent and/or its affiliates. All rights reserved.

Combatting fraud is not easy. But by implementing guided white-glove services, like those often provided by IDPS providers, consumers can be empowered to prevent and resolve fraud without feeling overwhelmed by the process.

All financial service providers should offer their members a white-glove fraud prevention and resolution experience. This will require FIs and other organizations to keep consumers informed and included in the process from the beginning, starting with the account opening.

Methodology

The Javelin Identity Fraud Study provides businesses, financial institutions, government agencies, and other organizations with an in-depth and comprehensive examination of identity fraud and the success rates of methods used for prevention, detection, and resolution.

SURVEY DATA COLLECTION

Consumer data in this report is based on information gathered from Javelin's 2023 Identity Fraud Survey, which was conducted online among 5,000 U.S. adults over the age of 18; this sample is representative of the U.S. Census demographics distribution. Data collection took place from Oct. 23 to Nov. 28, 2023. 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 errors, the percentages on graphs may add up to 100% plus or minus 1%. To preserve the independence and objectivity of this annual report, the sponsors of this project were not involved in the tabulation, analysis, or reporting of final results. The ID Fraud Study estimates key fraud metrics for the current year using a base of consumers who have experienced identity fraud in the past six years. Other behaviors are reported based on data from all identity fraud victims in the survey (i.e., fraud victims experiencing fraud up to six years ago) as well as total respondents, where applicable. For questions answered by all 5,000 respondents, the maximum margin of sampling error is +/-1.41 percentage points at the 95% confidence level. For questions answered by all identity fraud victims, the margin of sampling error is +/-3.3 percentage points at the 95% confidence level.

Consumer data in this report is also based on information gathered from Javelin's 2022 Identity Fraud Survey. This survey was conducted online among 5,000 U.S. adults over the age of 18; this sample is representative of the U.S. Census demographics distribution. Data collection took place Nov. 7-21, 2022. 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. The Identity Fraud Study estimates key fraud metrics for the current year using a base of consumers experiencing identity fraud in the past six years. Other behaviors are reported based on data from all identity fraud victims in the survey (i.e., fraud victims experiencing fraud up to six years ago) as well as total respondents, where applicable. For questions answered by all 5,000 respondents, the maximum margin of sampling error is +/-1.41 percentage points at the 95% confidence level. For questions answered by all identity fraud victims, the maximum margin of sampling error is +/-3.22 percentage points at the 95% confidence level.

© 2024 Escalent and/or its affiliates. All rights reserved.

Endnotes

1 Javelin Strategy & Research, "2024 Identity Fraud Study: Resolving the Shattered Identity Crisis." Published April 10, 2024; accessed June 21, 2024.

2 Ibid.

3 Ibid.

4 Ibid.

5 Ibid.

6 Ibid.

7 New York State Attorney General, "Attorney General James Sues Citibank for Failing to Protect and Reimburse Victims of Electronic Fraud." Published Jan. 30, 2024; accessed June 20, 2024.

8 Identity Theft Resource Center, "2023 Data Breach Report." Published January 2024; accessed June 24, 2024.

About Privacyguard

PrivacyGuard gives businesses the power to quickly add an end-to-end managed ID Protection program. PrivacyGuard is a comprehensive identity and privacy protection service that helps consumers to proactively protect their personal and financial information, monitor their credit and receive support if they experience identity theft.

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

© 2024 Escalent and/or its affiliates. All rights reserved. This report is licensed for use by Javelin Strategy & Research Advisory Services clients only. No portion of these materials may be copied, reproduced, distributed or transmitted, electronically or otherwise, to external parties or publicly without the permission of Escalent Inc. Licensors may display or print the content for their internal use only, and may not sell, publish, distribute, re-transmit or otherwise provide access to the content of this report without permission.

javelin