javelin | FIS

Creating a Digital Portrait to Prevent Omnichannel Fraud

WHITEPAPER | JUNE 2023

Table of Contents

Foreword 3
Overview....3
Key Findings....4
Recommendations 6
Account-Based Fraud: The Realization of a Major Problem 7
Fraud Alerts: A Necessary Tool Provides Consumer Security 9
Account-Based Alerts: Giving the Brush and Palette to the Accountholder....10
Reducing Fraud: The Digital Portrait 11
Technology is the Glue Holding the Multiple Pieces Together 12
Appendix 13
Endnotes 15
Methodology 15
About FIS....15

Table of Figures

Figure 1. Fraud Losses by Typology....7
Figure 2. What Criminals Take Over Most Frequently 8
Figure 3. Consumers' Satisfaction Regarding Fraud Alerts 9
Figure 4. Suggested Ways to Enhance Client Notifications....10
Figure 5. Consumer Comfort Level with Banks Using Personal Data Elements to Prevent Fraud 11
Figure 6. The Necessity of a 360-Degree View 12
Figure 7. Consumers Acknowledge Receipt of Automated Alerts....13
Figure 8. The Reasons Consumers Did Not Respond to Automated Fraud Alerts....13
Figure 9. Account-Based Changes and New-Account Alerts....14

javelin

Meet the Author

John Buzzard
Lead Analyst,
Fraud & Security

John is a Lead Analyst of Javelin's Fraud & Security practice. He is a nationally recognized financial industry fraud and security expert, and has influenced the card fraud, risk and security services for financial institutions throughout the United States through research, writing whitepapers, public speaking and consulting.

Foreword

This report, sponsored by FIS, explores the next step in controlling and reducing account-based fraud by using advanced technology and procedures that include a deeper understanding of each accountholder and data element.

This report was adapted from "The Butterfly Effect," published by Javelin Strategy & Research in March 2023. Javelin Strategy & Research maintains complete independence in its data collection, findings, and analysis.

Overview

As identity fraud losses continue to escalate across the financial services industry, increased attention is required in terms of technology and overall day-to-day procedures. Financial service providers and their vendor-partners need to press forward in developing an innovative series of solutions that will help stabilize the erosion of consumer trust that has been slipping with so many incidents of identity fraud—now an annual $43 billion problem.

javelin

Key Findings

Organized criminal activity is systematically targeting multiple verticals to evade detection. Organized criminals are not operating in an unorganized or manual way today, so it makes perfect sense that defenders of sensitive financial information develop some rapid changes.

Success in fraud prevention is a combination of technology and automation. A more sensible approach to tackling so many business verticals is technology and automation. Every facet of the business should be contributing to a larger pool of actionable data that helps to accomplish several initiatives, such as preventing or confirming fraud at the accountholder level, providing a strong and automated response to the growing demands of the investigative side of the business, and providing an insightful digital portrait of the accountholder relationship.

Identity fraud losses totaled a combined $43 billion (USD) in 2022. That was the combined total of Javelin-tracked categories. Despite the staggering total, this represented a wholesale decline of $9 billion from the previous Javelin study period.

There were 40 million combined identity fraud victims in 2022. That's the number experiencing identity fraud in some form, representing traditional identity fraud and identity fraud scams.

Traditional identity fraud losses in 2022 totaled $20 billion. The impact reflects a decline of $4 billion (15%) from the previous Javelin study period. The average loss per victim in 2022 was $1,311, a drop of $240 per victim (16%).

Traditional identity fraud affects 6% of U.S. adults. A total of 15.4 million U.S. adults were affected by identity fraud in 2022. The victim total for 2021 was 15.3 million. This increase of less than 1% underscores the fact that U.S. adults are still experiencing identity fraud without relief despite the small decrease in the overall loss per victim.

In 2022, identity fraud scam losses eclipsed those related to traditional identity fraud. The $23 billion impact of identity fraud resulting from scams reflects a decline of $5 billion (17%) from the previous Javelin study period. Despite the respectable decline, this Javelin-tracked fraud category still managed to eclipse the $20 billion lost to traditional identity fraud types. The average loss per identity fraud scam victim in 2022 was $915, representing a decrease of $114 per victim (11%) from the previous study period.

Risk for existing accountholders occurs quite often when criminals open unauthorized accounts where the consumer primarily banks. Efforts at preventing new-account fraud can benefit from alerts based on the originations of loans and new demand deposit accounts (DDA). Criminals prefer to open fraudulent accounts where identity fraud victims already have well-established relationships, so it makes perfect sense to notify accountholders when other loans and accounts are opened, using a combination of procedures dictated by regulations and compliance.

Account takeover fraud (ATO) losses barely changed, topping out at $11 billion. There was a decline of almost 4% in losses from the previous study period ($11.4 billion). This minor decline also affected the ATO victim count, which fell by 13% (approximately 4.5 million U.S. adults).

Criminals focus on access to funds and merchandise in ATO targets. Checking and savings accounts (36%) and credit cards (22%) are consistently favored by criminals every study period. Merchant accounts such as those with Amazon or Walmart (21%) represent new opportunities for criminals to order high-value goods for resale or personal gain.

Recommendations

Notify existing accountholders when new accounts are opened in their name. Cross-referencing and comparing information across old and new accounts to detect anomalies should be standard practice. Existing accountholders should also be notified when their personally identifiable information is used to open additional accounts in their name—especially when the accounts are not linked.

Mandate multifactor authentication (MFA). Consumer accounts, customer contact sessions, and in-person branch transactions can benefit from leveraging MFA when additional step-up authentication is required. MFA protocols should be automatically activated as soon as an account is established. Consumers should still be permitted to opt out of MFA notifications upon request.

Enhance alerting capabilities by notifying accountholders when tokens are requested. Unauthorized enrollment in digital wallets is a problem across all account-based fraud. Existing accountholders should be notified through existing alerting functionality whenever a token request is received.

Monitor and interpret how unauthorized non-monetary account changes can result in identity fraud. Criminals make significant changes to account details to evade accountholder detection. It is important to develop fraud strategies for account-based changes to prevent fraud related to loans, credit, or funds transfers.

Leverage omnichannel data to improve fraud rates. Reduce fraud by unifying data from multiple sources into a single view.

Detect organized crime faster using data from multiple verticals. Part of the challenge in realizing that organized criminals are targeting the organization is having access to data from multiple verticals on a continuous basis.

Empower fraud investigations using real-time data. Real-time data should flow freely through the fraud investigation process to permit faster identification of outcomes and sustain lower losses from a faster turnaround time.

Enable a one-voice approach to organizational fraud communication. Organizations can directly benefit by converting fraud intelligence into a singular view that facilitates a “one-voice /one-source” fraud mentality by extracting omnichannel fraud data across the entire protected enterprise.

Maintain existing fraud decision strategies with a renewed focus on cross-organizational efficiency. Financial institutions depend on a strong fraud analytics program. Practitioners should also consider the benefits of combining omnichannel data and fraud investigation outcomes into a single organizational view.

Automate Know Your Customer (KYC) compliance. Organizations cannot depend on a highly trained workforce as the only methodology for administrating strong KYC practices. Tokenized data, real-time updates to regulations, and versatility via international and domestic channels are essential elements to be considered.

Account-Based Fraud: The Realization of a Major Problem

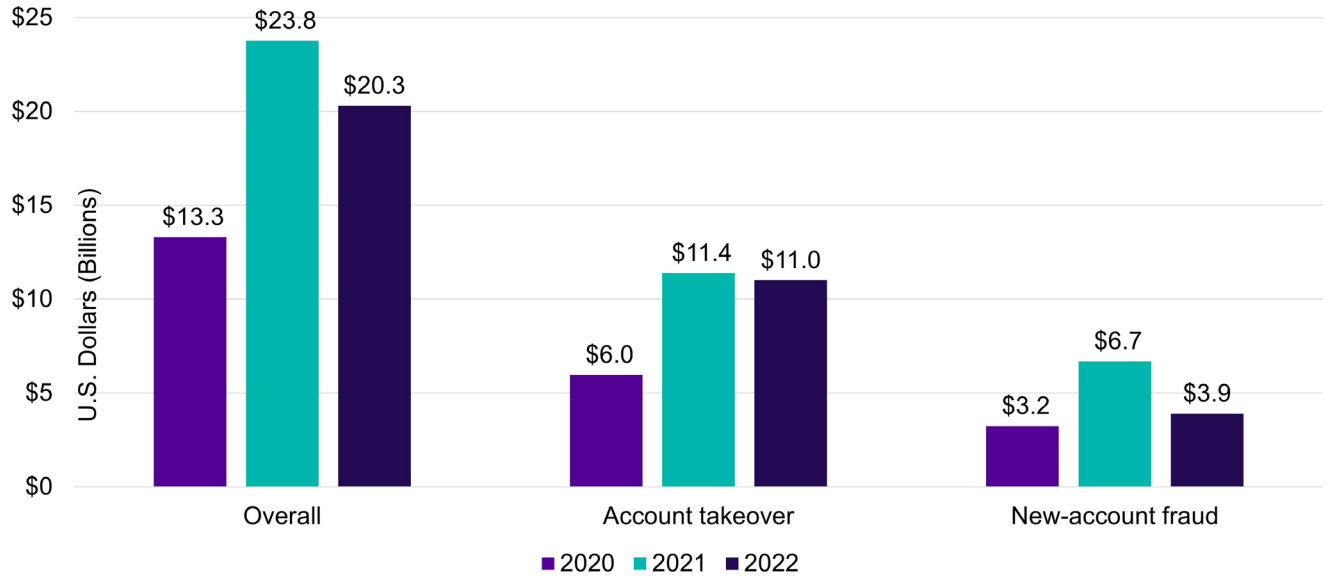
Javelin cited a $43 billion combined loss for identity fraud in its annual identity fraud report, titled *The Butterfly Effect*.[1] Account-based fraud continues to be a major problem, with $11 billion in losses affecting consumers. As financial service providers make consumers whole again from most of these losses, the cost simply shifts over and directly affects financial institutions, credit card issuers, and payment industry businesses.

One of the most startling conclusions published by Javelin was that account takeover fraud (ATO) remained virtually identical for two consecutive research periods. This means that losses remained unchanged amid so many opportunities to improve the landscape. Interestingly, new-account fraud (NAF) losses dramatically dropped—by 42%—from an all-time high reported by Javelin in 2022, when NAF losses increased by 109%. Part of the problem here is that one fraud typology should not suffer increased or sustained losses because practitioners focused on everything else.

A holistic and comprehensive plan is required to uniformly achieve reductions in all fraud categories. This requires using a mix of updated operational plans as well as some enhancements to existing technological tools. Organized criminals are not operating in an unorganized or manual way today, so it makes perfect sense that defenders of sensitive financial information enact some rapid changes.

Account-Based Fraud Continues to Be a Major Challenge

Figure 1. Fraud Losses by Typology



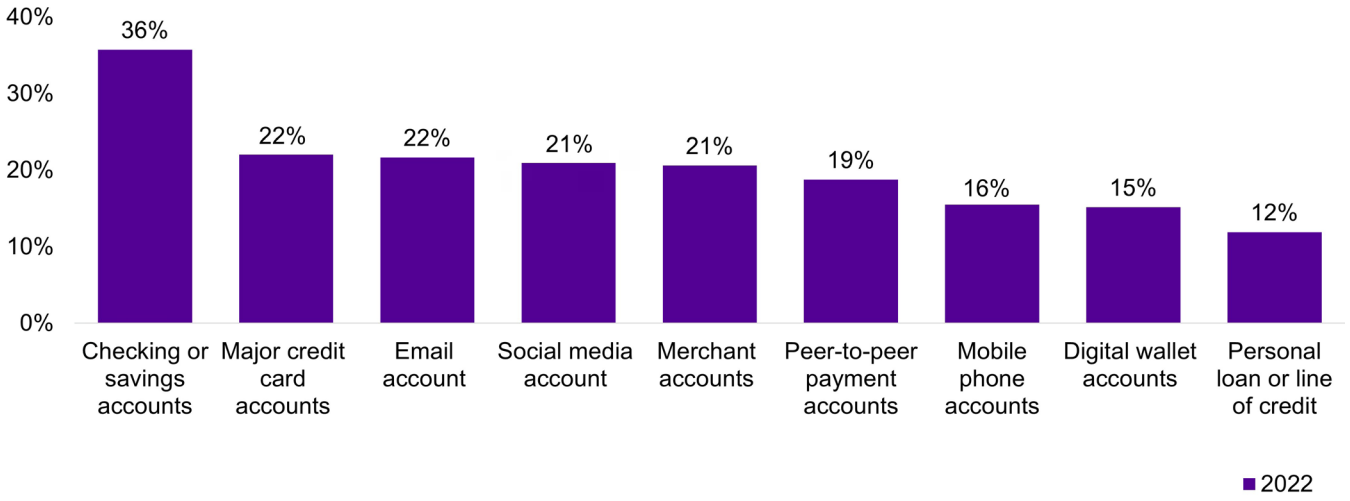
Source: Javelin Strategy & Research, 2023

javelin

Account takeover targets favored by criminals are a combination of things that provide access to financial accounts such as checking or savings accounts and user-credential-oriented information that allow a criminal to gain domain over email and mobile devices.

Account Takeover Targets Popular in 2023

Figure 2. What Criminals Take Over Most Frequently



Source: Javelin Strategy & Research, 2023

One of the primary issues financial institutions face on a daily basis is collecting data that can then be analyzed across the entire business enterprise.

As organizations continue to grow, there are natural business verticals that are managed by different leaders specialized in addressing key components of the business. This doesn't mean that cross-organizational communication and data mining are more optimized; it's just that there simply isn't time to rely on standard communication to sufficiently scale so many areas of concern.

A more sensible approach to tackling so many business verticals rests with technology and automation. Every facet of the business should contribute to a larger pool of actionable data that helps accomplish several initiatives, such as preventing or confirming fraud at the accountholder level, providing a strong and automated response to the growing demands of the investigative side of the business, and providing an insightful digital portrait of the accountholder relationship.

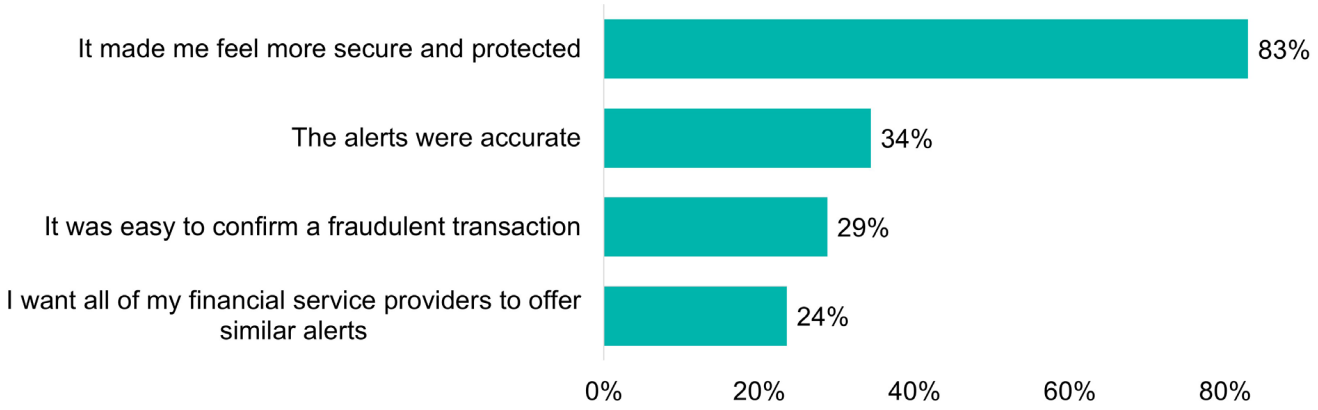
javelin

Fraud Alerts: A Necessary Tool Provides Consumer Security

Most financial institutions today offer a combination of fraud alerts (alerts sent to accountholders to confirm unauthorized transactions based on a decision engine score) and optional account-based alerts (alerts an accountholder can select and enable during a secure online banking session). Fraud alerts are essential to the everyday rhythm of managing transactional-based scoring and fraud prevention by permitting the actual accountholder to validate potentially risky transactions as fraud or non-fraud.

83% of Consumers Felt More Secure Upon Receiving an Automated Fraud Alert

Figure 3. Consumers' Satisfaction Regarding Fraud Alerts



Source: Javelin Strategy & Research, 2023

The organizational value in automated fraud alerts has a fruitful side effect: —higher degrees of satisfaction at the accountholder level. Among consumer respondents, 83% indicated a feeling of security and protection each time they received an automated fraud alert via SMS or email.

About one-third of respondents find fraud alerts accurate in identifying transactions that were highly suspicious or fraudulent. The ease with which consumers interact with SMS and email in their daily lives translates to comfort when they respond to alerts, as 29% indicate an easy experience providing responses to their financial service provider. Javelin also asked consumers to confirm whether they have ever received an automated fraud alert (51% have; see Figure 7 in the Appendix).

A very small margin of consumers refrained from engagement with a fraud alert (8%) citing such reasons as concern that the alert was actually a scam (55% of the original 8%), and 32% of the original 8% of consumers indicated that they had chosen to call their financial institution instead of responding to the alert. All of these reasons (see Figure 8 in the Appendix) are addressable with increased messaging and education. Consumers simply need to understand the value proposition in responding to alerts even if they performed the transaction in question.

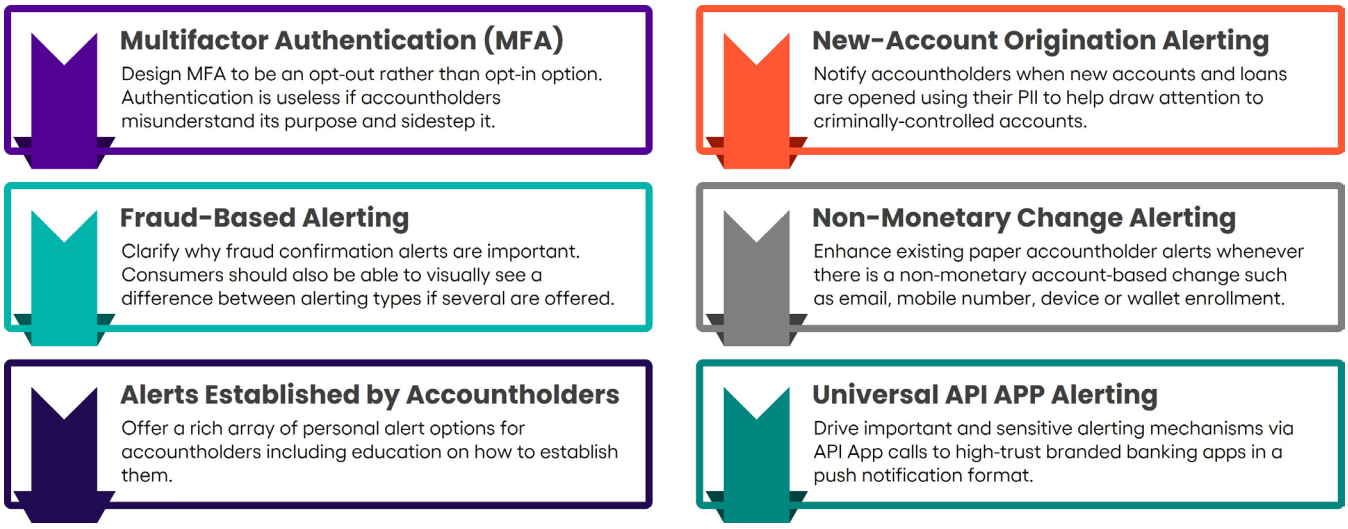
javelin

Account-Based Alerts: Giving the Brush and Palette to the Accountholder

Account alerts, common in most banking circles, represent an enormous opportunity to further engage accountholders in collaborating on fraud detection, simply by virtue of how account-based alerts can provide early warnings to accountholders when anomalies occur. Accountholders should be provided with a wide array of triggers to select from to maximize the efficacy of an alerting program. Customization should be woven into the offering as consumers seek more options from their primary financial institutions. All of these actions should be supported by continuous authentication via multifactor authentication. (Note: Javelin recommends that MFA notifications are automatically established with every new account relationship. If consumers wish to opt out of MFA, they can easily do so in a similar way that any automated alert can be stopped upon request.)

Essential Enhancements to Outbound Accountholder Alerts

Figure 4. Suggested Ways to Enhance Client Notifications



Source: Javelin Strategy & Research, 2023

Risk for existing accountholders occurs quite often when criminals open unauthorized accounts where the consumer primarily banks. Efforts at preventing new-account fraud can benefit from alerts based on the originations of loans and new demand deposit accounts (DDA). Criminals prefer to open fraudulent accounts where identity fraud victims already have well-established relationships, so it makes perfect sense to notify accountholders when other loans and accounts are opened using a combination of procedures dictated by regulations and compliance.

Another regular criminal occurrence pertains to changes to non-monetary accounts. Changes to email and mobile numbers and a combination of credentials have served as early fraud indicators for years. Advancements in technology can now alert accountholders to non-monetary changes as other forms of notification, such as letters and emails, are delivered through the traditional channels.

Reducing Fraud: The Digital Portrait

Financial institutions should be encouraged by Javelin's recent research findings that consumers are more accepting of data usage when it comes to fraud prevention. Combined, 62% of consumers expressed a general acceptance of data usage for fraud prevention purposes (a neutral response is considered a soft yes), with another 19% of consumers indicating that they were very comfortable with personal data such as mobile device IDs and geolocations being used to keep their personal financial accounts safer. Consumers are equally comfortable with advanced authentication methods such as facial liveness (selfies) and document verification commonly referred to as identity proofing.

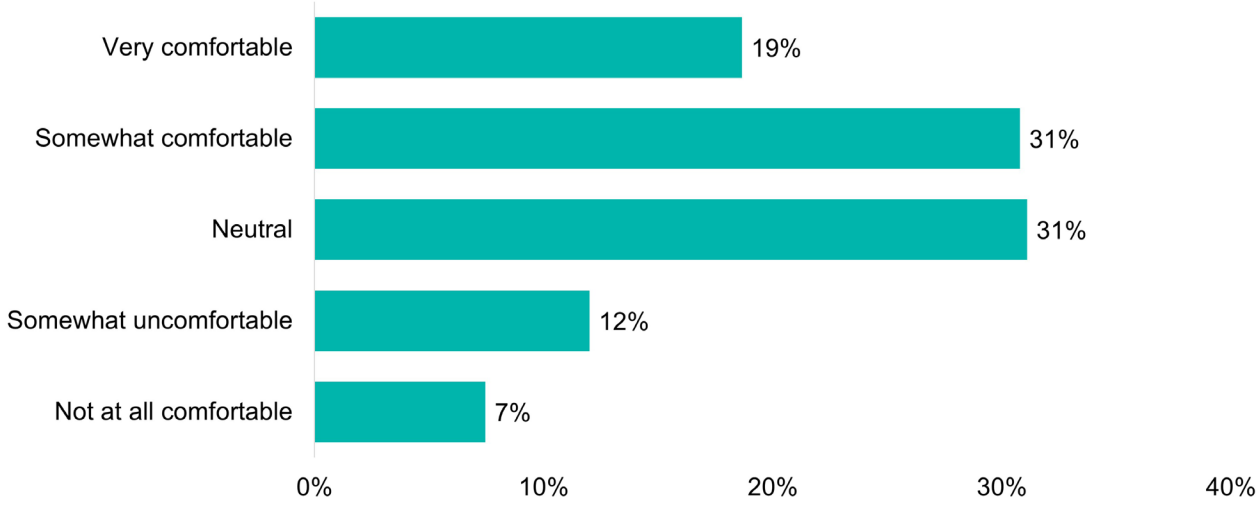
There is a tremendous benefit to financial service providers in realizing that consumers are far more accepting of technology and data in matters of fraud prevention. Consumers are already interacting with technology within smartphone apps that triangulate locations and use repeated behaviors to generate offers and suggestions.

These societal shifts are primary examples of why financial institutions must take the lead in providing enriched experiences that help consumers to visualize their personal financial circumstances—including the early detection of suspicious transactions.

Insightful information such as credit scores, the addition of new accounts, and credit bureau activity are perfect areas to expand upon as financial institutions further engage with their accountholders in a meaningful way that expedites the delivery of information that might otherwise be available only through other diverse, time-consuming channels.

More Than Half of Consumers Accept the Usage of Their Data for Fighting Fraud

Figure 5. Consumer Comfort Level with Banks Using Personal Data Elements to Prevent Fraud (1=Not to 5=Very)



Source: Javelin Strategy & Research, 2023

javelin

Technology is the Glue Holding the Multiple Pieces Together

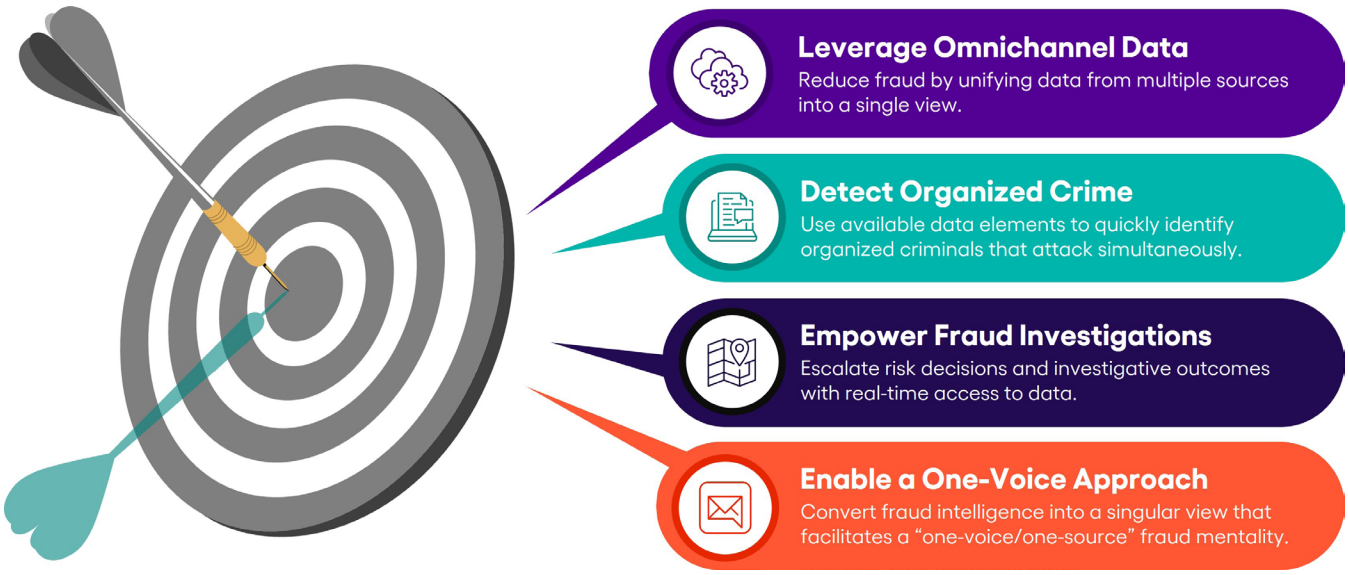
Fraud investigations are often hampered by fragmented data and conclusions that are not always accessible across the business enterprise. A huge and perennial challenge is making solid decisions that positively affect accountholders in good standing. The objective: Inconvenience the criminal through stronger insights that also create a barrier against future attacks from the same actors.

The challenge, as always, is the inability to connect multiple data sources into a single point of view. The uphill battle to rank accountholder risk and manage payment card activity along with a wide array of other transactions, such as wires and ACH payments, can require dozens of tools—none of which have any interoperability. Javelin recommends that financial institutions focus on technology that is capable of unifying multiple fraud prevention tools without compromising on the individual performance of each tool.

As fraud investigators become less attainable in the highly competitive employment marketplace, many organizations are facing a "do more with less" staffing model out of necessity. The implications of operating on such a thin scale without optimizing fraud investigation and prevention efforts leave the entire organization exposed to the risk of a higher incidence of fraud. Anti-money-laundering efforts can also suffer through the current employment shortages without the proper attention to compliance and the investigations required to be successful. A unified approach through the use of technology tools and some strategy to acquire more highly specialized fraud investigators will be the only way to properly execute a cross-organizational fraud prevention program.

Gaining Domain Over Omnichannel Fraud

Figure 6. The Necessity of a 360-Degree View



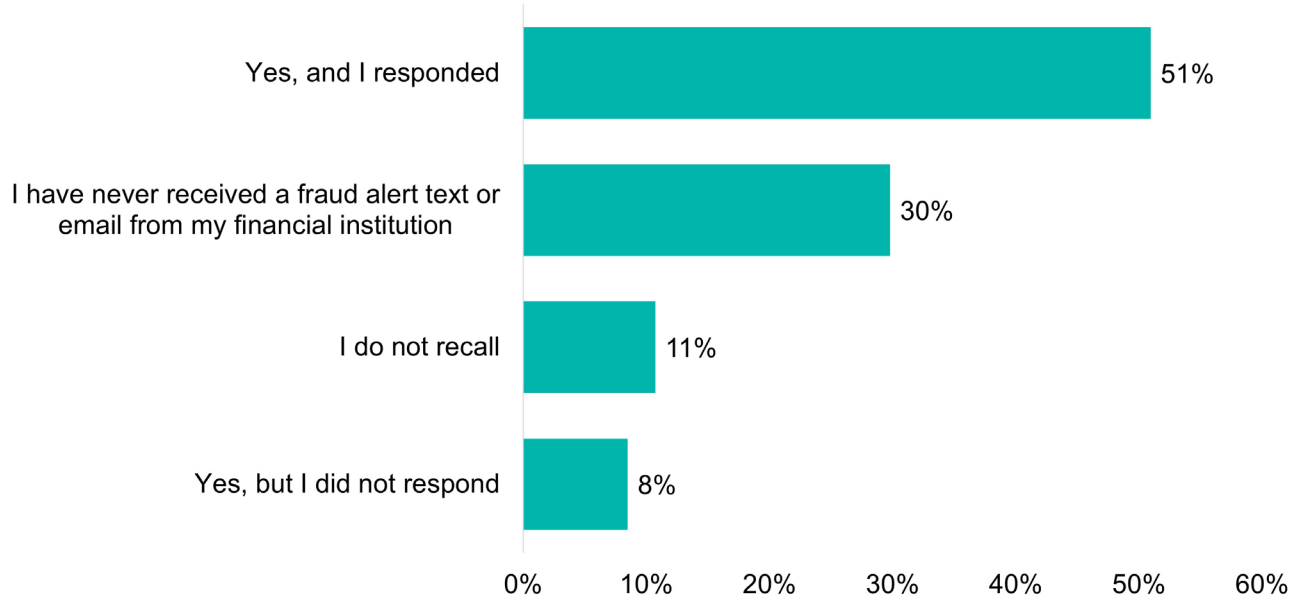
Source: Javelin Strategy & Research, 2023

javelin

Appendix

51% of Consumers Know What Fraud Confirmation Alerts Are

Figure 7. Consumers Acknowledge Receipt of Automated Alerts



Source: Javelin Strategy & Research, 2023

Consumers' Fear of Scams and Malware Inhibit Their Engagement

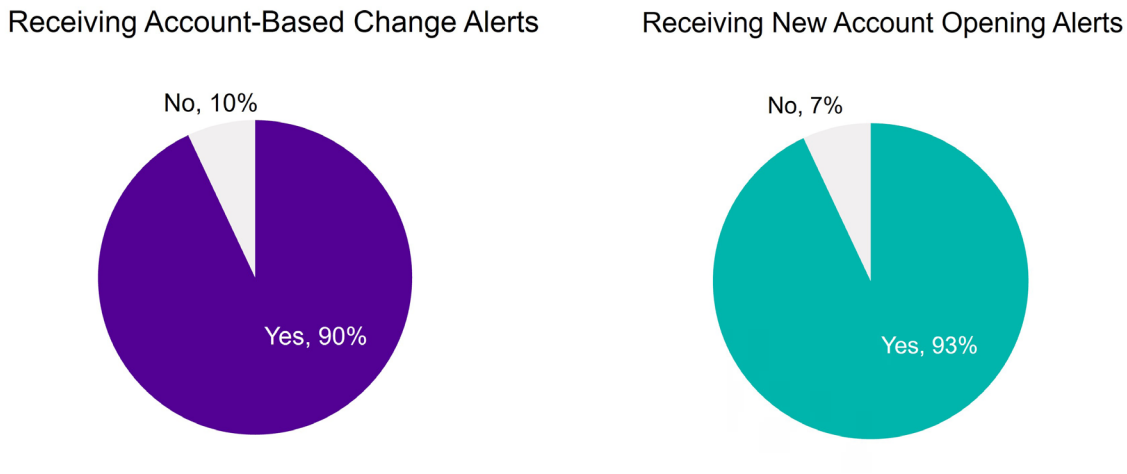
Figure 8. The Reasons Consumers Did Not Respond to Automated Fraud Alerts

Source: Javelin Strategy & Research, 2023

javelin

High Consumer Approval for Any Helpful Alerting

Figure 9. Account-Based Changes and New-Account Alerts



Source: Javelin Strategy & Research, 2023

Endnotes

1 Javelin Strategy & Research "The Butterfly Effect." Published March 2023.

Methodology

The Javelin 2023 Identity Fraud 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 from Nov. 7 through Nov. 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.

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 the final results.

About FIS

FIS is a leading provider of technology solutions for merchants, banks and capital markets firms globally. Our employees are dedicated to advancing the way the world pays, banks and invests by applying our scale, deep expertise and data-driven insights. We help our clients use technology in innovative ways to solve business-critical challenges and deliver superior experiences for their customers. Headquartered in Jacksonville, Florida, FIS ranks #241 on the 2021 Fortune 500 and is a member of Standard & Poor's 500® Index.
To learn more, visit www.fisglobal.com. Follow FIS on Facebook, LinkedIn and Twitter (@FISGlobal).

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
Twitter and LinkedIn

javelin