FIS

ADVANCING THE WAY THE WORLD PAYS, BANKS AND INVESTS™

RISING THREATS:
HOW IDENTITY FRAUD AFFECTS THE DIGITAL CHANNEL

JULY 2022

PART OF THE ESCALENT FAMILY

JAVELIN

TABLE OF CONTENTS

TABLE OF FIGURES

FOREWORD

This report, sponsored by FIS, will examine how identity fraud affects digital channels. The compilation of issues ranges from the ever-changing regulatory environment to how financial institutions deal with the increasingly sophisticated financial crime tactics perpetrated by criminals. Javelin recently published its 2022 Identity Fraud Study, titled The Virtual Battleground. The study concluded that in 2021 alone 42 million U.S. adult consumers were victimized by identity fraud, resulting in a collective $52 billion financial impact on the financial service industry. The overwhelming losses have long-range effects on the client experience, know-your-customer (KYC) standards, and a variety of compliance and regulatory obligations.

As financial institutions recalibrate the client experience to be friction-free and appealing, there are also regulations and compliance-driven dynamics such as the KYC process that must constantly be taken into consideration.

This report was adapted from the 2022 Identity Fraud Study, The Virtual Battleground, published by Javelin Strategy & Research in March 2022. Javelin Strategy & Research maintains complete independence in its data collection, findings, and analysis.

OVERVIEW

Financial institutions are facing rising incidents of account-based fraud. The steep acceleration of identity fraud and criminals' ability to extract excessive amounts of personally identifiable information (PII) using sophisticated techniques and social engineering have weaponized information in the digital channel. The expenses associated with these schemes are shouldered to varying degrees by consumers and their financial service providers. Additional complications are also born out of the ever-present need to adhere to compliance and due-diligence requirements without compromising the client experience. Despite numerous challenges, technology and improved business processes are still the essential ingredients required for protecting the digital channel and beyond.

EXECUTIVE SUMMARY

Identity fraud losses increased by 79% in 2021. Javelin recently published its annual 2022 Identity Fraud Study, titled *The Virtual Battleground*. The study concluded that in 2021 alone 42 million U.S. adult consumers were victimized by identity fraud, resulting in a collective $52 billion financial impact on the financial service industry.

Identity fraud methods mimic pre-pandemic characteristics. The astounding increases in traditional identity fraud categories such as new-account fraud (NAF) and account takeover fraud are byproducts of sophisticated criminal attacks similar to those of the pre-pandemic era before 2020.

Personally identifiable information (PII) continues to be monetized by criminals and used to execute account-based fraud. As criminals perpetrate multiple identity fraud schemes that steal consumers' PII, they are conscious of the fact that information always has a price—especially when it's sold on the dark web or bartered or bartered for other illegal goods and services.

Synthetic identities continue to represent risks to a wide variety of organizational siloes. Synthetic identity fraud easily links to various account-based fraud. Criminals are eager to open valuable new financial accounts using any information that passes the scrutiny of the financial institution, as with NAF. Synthetic fraud can also be associated with first-party fraud in the sense that the fraud actor may open a new account using a synthetic identity (or a stolen legitimate identity) to extract a maximum return on investment in a variety of account-based frauds, including credit accounts, loans, and online merchant accounts.

Consumer-owned digital accounts take a throttling, with one million additional victims. Javelin's findings conclude that one million additional new consumer-owned digital accounts were taken over when compared with the previous Javelin research period. Merchant accounts and delivery services like Instacart provide immediate access for criminals to acquire goods and services.

Account-based fraud increased as much as 109% in 2021. Account-based fraud categories saw rises, such as NAF, which had a 109% increase in just one year.[1] One of the largest financial losses cited in the report pertained to account takeover fraud, which increased 90% and came to $11 billion in losses. It's important to note that most of these losses must be absorbed by financial institutions in an attempt to make the accountholder whole again and to align with banking regulations pertaining to account-based fraud.

Criminals are embracing automation as a means of garnering more victims. Criminals are exercising their options for automation every day by harnessing artificial-intelligence-powered bot networks and leveraging other schemes, such as card enumeration attacks.

Know Your Customer standards remain a constant challenge for financial institutions. The increase in identity fraud and synthetic identities presents an overabundance of potentially fraudulent information that has to be validated pursuant to KYC standards.

RECOMMENDATIONS

Recommendations: Account-Based Fraud

Enable multifactor authentication (MFA). One-time passcodes, for example, should be used in tandem with a variety of other fraud prevention tools to further secure the enterprise from criminal account takeovers.

Monitor card velocity to help identify spikes in unusual transaction patterns. Card velocity is still a valuable indicator that unusual transactions are being executed. Card issuers or their third-party vendors should execute fraud strategies that take into consideration a variety of card velocity parameters.

Verify card verification values. CVX values help to identify unauthorized activity, including payment cards that have been compromised during counterfeit card-skimming scenarios and phishing attacks.

Offer automated fraud alerts that are triggered by account-based changes. Financial service providers should send out automated fraud alerts to verify unusual account-based activity via SMS texts and email. Accountholders can also benefit from fraud alerts when they are customizable and offer the cardholder an opportunity to be alerted on a wide array of card statuses.

Recommendations: Card Enumeration Attacks

Randomize card number issuance and expiration dates. To avoid rampant losses stemming from card enumeration attacks, issuers must revise certain archaic practices that help to proliferate card enumeration or BIN attacks, such as issuing payment cards and expiration dates in sequential order.

Scrutinize card verification value denials as a means of early attack detection. Card verification (CVV and CVC) denials should be scrutinized closely to help identify emerging enumeration attacks.

Embrace 3D Secure technology. To help stabilize the card authorization process, card issuers need to fully embrace 3D Secure technology to increase the efficacy of card authorizations.

Establish revised daily card limits. Daily limits established by issuers—including those on the number of allowable transactions—should be conservative and appropriate for the demographic.

Segment card BINs by affluence levels when possible. Card issuers should segment BINs based on accountholder affluence. This helps issuers adjust daily spending limits and manage risk more effectively.

Incorporate velocity-based rules into your daily monitoring strategies. In addition to leveraging a predictive neural work that includes machine learning capabilities, incorporate velocity-based rules that prohibit authorization behavior indicative of bot attacks.

Recommendations: Know Your Customer

Use a single-platform API offering when possible to maximize interoperability. Business enterprises should seek options that may reside on a single platform, enabling a layered plug-and-play product acquisition to be deployed as the needs of the organization expand.

Import global watchlist data directly into the KYC decisioning process. Watchlist information such as Office of Foreign Assets Control (OFAC) should be importable into a single KYC platform to maximize efficiency.

Deploy device and behavioral biometrics. Due diligence for KYC can be greatly enhanced through the adoption of biometrics that help determine if a device and the associated accountholder behaviors match the true accountholder.

Encrypt sensitive biometric data. Biometric images and data should be highly encrypted or tokenized to increase security.

THE CRIMINAL MASQUERADE: ACCOUNT-BASED FRAUD

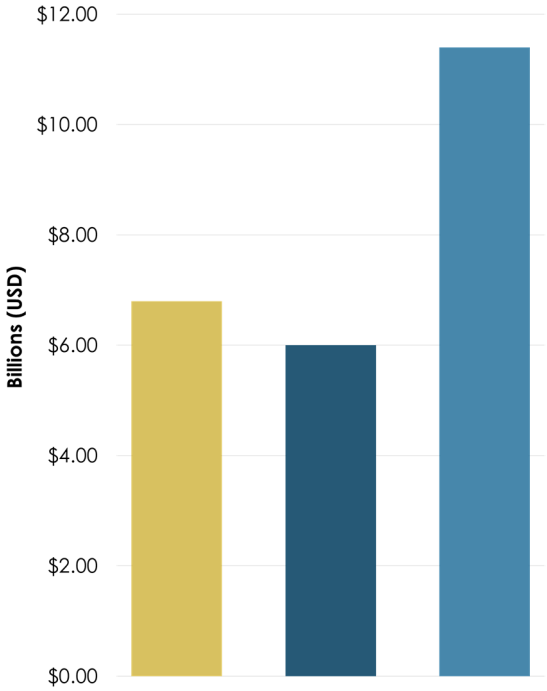
Javelin published the latest edition of its annual Identity Fraud Study, titled *The Virtual Battleground*, in March 2022. The study findings included some shocking increases in categories such as new-account fraud, which had a 109% increase in just one year.[2] One of the largest financial losses cited in the report pertained to account takeover fraud, which increased 90% and totaled $11 billion in losses. It's important to note that most of these losses must be absorbed by financial institutions in an attempt to make the accountholder whole again and to align with banking regulations pertaining to account-based fraud. The astounding increases in such traditional identity fraud categories as new-account fraud and account takeover fraud are byproducts of sophisticated criminal attacks that are similar to those of the pre-pandemic era before 2020.

The steady need for consumer goods and services and the wide variety of payment options that have flourished in recent years have provided a fantastic convenience for consumers. That same convenience also benefits the criminal manifesto. As criminals perpetrate multiple identity fraud schemes that steal consumers' PII, they are conscious of the fact that information always has a price—especially when sold on the dark web or bartered for other illegal goods and services.

One of the final, and most damaging, aspects of identity fraud is how losses affect a wide range of industries, including e-commerce merchants, retailers, financial service providers, and a host of gig economy workers and micro industries. While the consumer, in many cases, is made financially whole again, the service provider might not be so lucky. There are also many occasions when lines are blurred as one form of criminal activity gets confused or miscategorized because it shares characteristics with other fraud types. Synthetic identity fraud is an excellent example.

Account Takeover Fraud Is Now An $11 Billion Dollar Problem

Figure 1. Account Takeover Fraud, 2019-2021



Source: Javelin Strategy & Research, 2022

The Federal Reserve recently defined synthetic identity fraud and classified a wide variety of common uses that propel synthetic identities across the realms of credit repair, housing and government services, payments, and other criminal activity.[3]

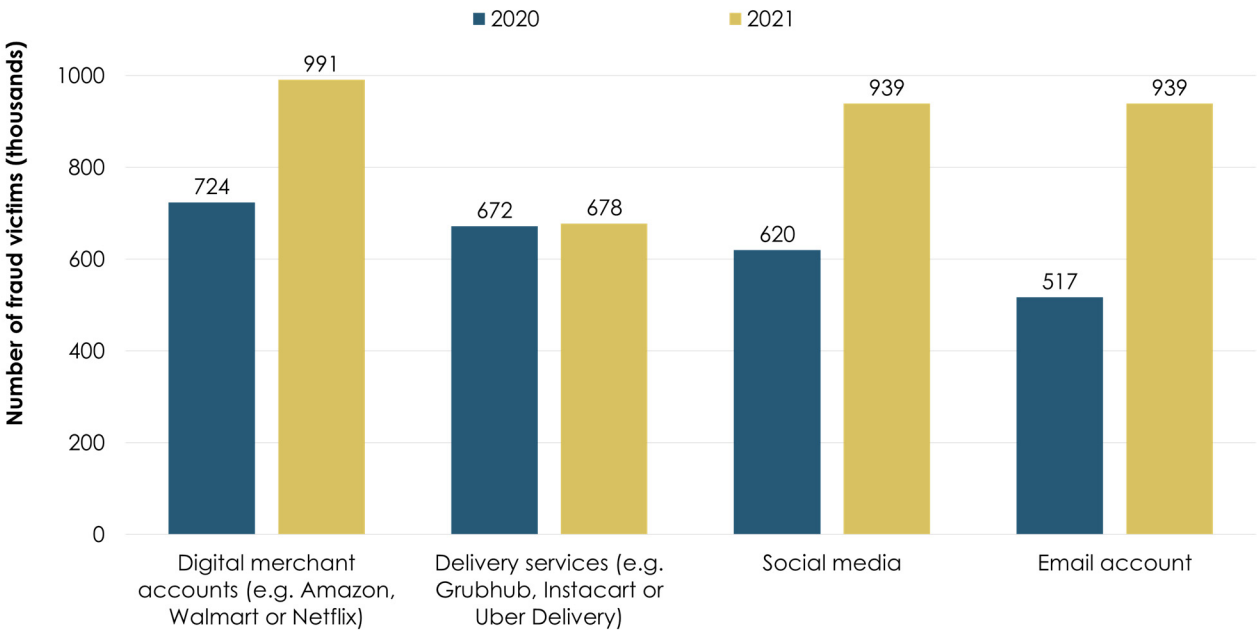
Synthetic identity fraud easily links to various kinds of account-based fraud. Criminals are eager to open valuable new financial accounts using any information that passes the scrutiny of the financial institution, as with NAF. Synthetic fraud can also be associated with first-party fraud in the sense that the fraud actor opens a new account using a synthetic identity (or a stolen legitimate identity) to extract maximum ROI in a variety of account-based frauds involving credit accounts, loans, and online merchant accounts. The a is essentially the same since the criminal has no intention of repaying any debts while applying laser-focused attention to the acquisition of funds and high-value goods and services.

Javelin's findings also conclude that one million additional new consumer-owned digital accounts were taken over in 2021 when compared with the previous Javelin research period. Merchant accounts and delivery services like Instacart provide immediate access for criminals to acquire goods and services.

Social media and email accounts, once taken over, represent part of the process criminals will use to gain unfettered access to valuable personal contacts and other identifying information that can unlock the information needed to overcome basic challenge questions. Email takeover also means that valuable account change email notifications are often deleted by the criminal and therefore unread by the consumer.

Victim Counts Increase by 1 Million Consumers

Figure 2. Top Digital Channels Taken Over by Criminals, 2020-2021



Source: Javelin Strategy & Research, 2022

THE TOTAL DIGITAL TAKEOVER

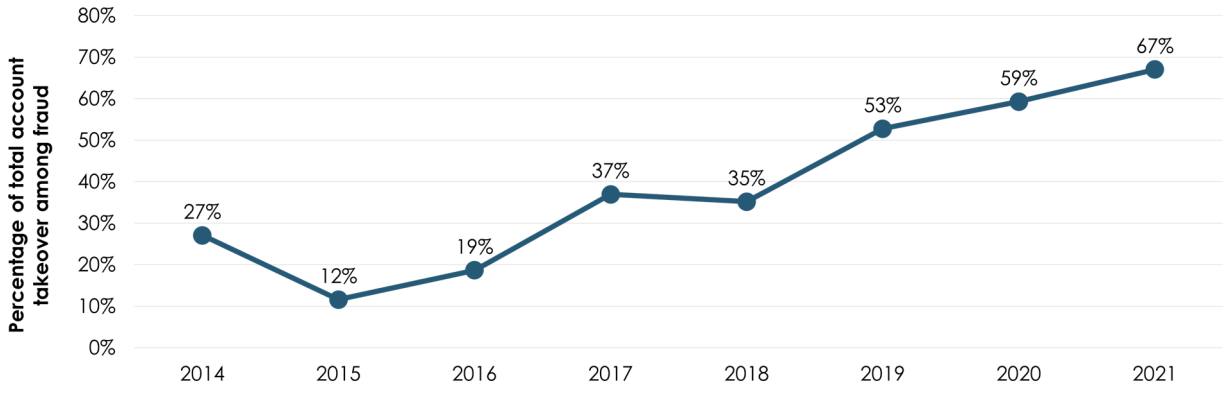
Consumers are leading lives that increasingly involve digital interaction. Tech-savvy consumers, in particular, often use multiple digital platforms that represent a wide variety of applications ranging from social media to sensitive financial apps for banking and retirement or investment activities. The importance placed on immediate access to social media and financial information may not always be met with the same level of security-mindedness. Consumers may neglect to deploy a variety of usernames and passwords, thus leaving their personal accounts vulnerable to a complete takeover by a criminal who simply needs to gain knowledge of one username and password to be successful. Javelin's research findings indicate that consumers in growing numbers have lost complete and total control over multiple digital accounts since 2018.

As total account takeover fraud reached 67% of fraud incidents in 2021, it has become apparent that consumers are not equipped to protect themselves without assistance from their primary financial institution (PFI) and other business partners. In addition to aggravation and upheaval suffered by consumers who are victims of fraud, the loss of personal accounts often translates to substantial financial losses that may have to be restored back to consumers by their PFIs.

Knowing that consumers are vulnerable to criminal attacks can lead to better circumstances at the financial institution level when fraud prevention tools and procedures are aligned to ensure that strong authentication is combined and layered into an existing fraud prevention program that includes decision engine strategies as well as adherence to regulations and compliance.

Criminals Continue to Take Over the Entire Digital Lives of Consumers

Figure 3. Full Account Takeover Fraud, 2014-2021



Source: Javelin Strategy & Research, 2022

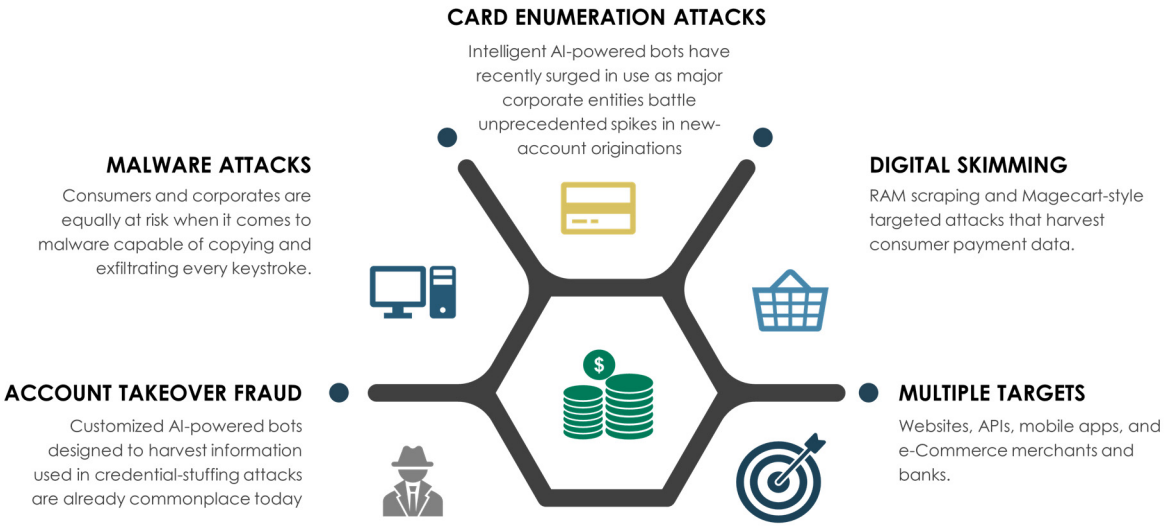
THE DANGER OF AUTOMATED THREATS

Automation is not exclusive to legitimate business concerns. The concept of achieving more net results with lesser or lower-cost efforts has universal appeal. Criminals are exercising their options for automation every day by harnessing AI-powered bot networks and leveraging other schemes, such as card enumeration attacks. Card enumeration attacks have been a staple tactic for criminals for many years. Long-term fraud prevention professionals may also refer to such attacks as "credit master" or "BIN" attacks. Card enumeration attacks usually begin when a criminal gains access to random merchant payment processing accounts through various means. Single cards or large batches of test transactions are then performed, with the criminals using each card number to ascertain which cards return a valid authorization. Cards that demonstrate a successful authorization are often used immediately by criminals for fraudulent purchases or wholesale barter with other criminal carders for digital currency or other items of value. Card issuers should be sensitive to repeated card value verification failures as a key indicator that a card enumeration attack may be occurring.

The appeal for most criminals is the ability to extend the life of consumer PII by automating multiple facets that use stolen information. Digital skimming, for example, is an automated RAM-scraping malware attack designed to evade detection while exfiltrating large amounts of stored payment and customer data into the hands of cyber criminals from millions of website shopping carts and poorly secured online payment checkouts.[4]

Criminal Automation Extends the Shelf Life of Stolen PII

Figure 4. The Danger of Automated Threats



Source: Javelin Strategy & Research, 2022

HOW WELL DO YOU KNOW YOUR CUSTOMER?

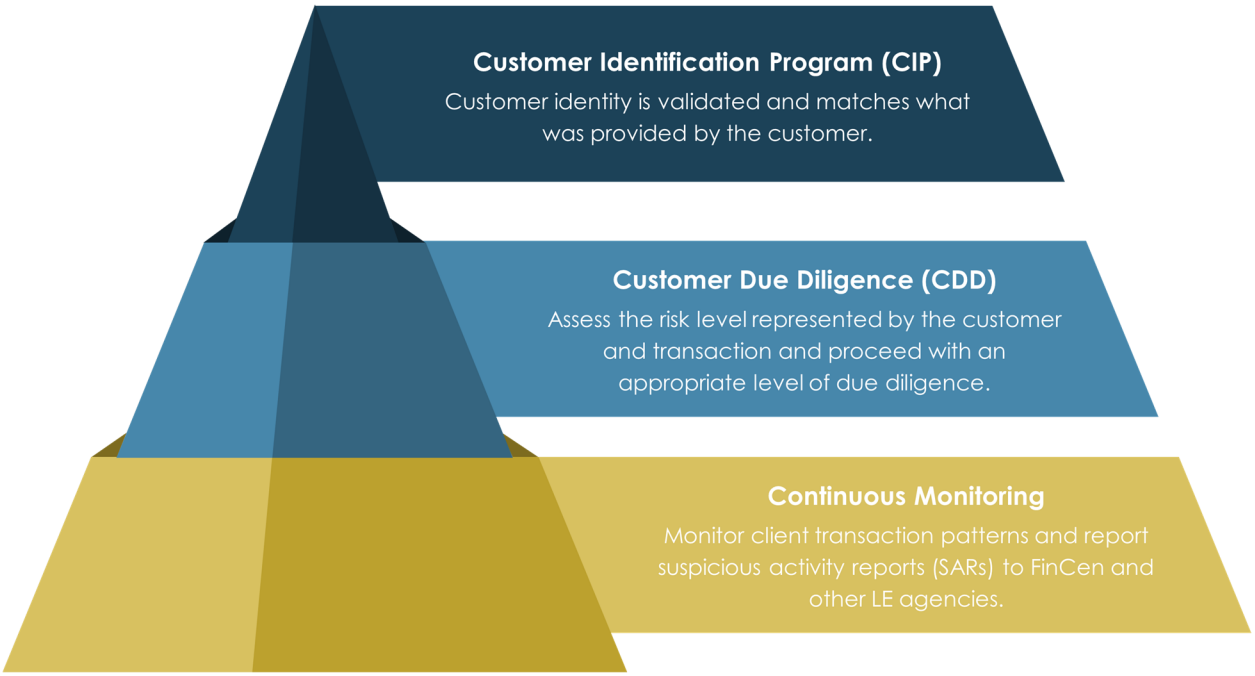
Identity fraud can also complicate how financial service providers conduct business with unknown entities who request products and services that require a deeper understanding of the identity of the requestor.

The increase in identity fraud and synthetic identities presents an overabundance of potentially fraudulent information that must be validated pursuant to KYC standards. The sweeping Patriot Act of 2001 helped to usher forward KYC standards to help protect financial service providers from fraud, money laundering, corruption, and other illegal financial activity, such as terrorism.

A risk-based approach with KYC can help to eliminate fraudulent activities and ensure a better customer experience by creating fraud strategies that continuously monitor and adapt rules specifically to the needs of the organization. As requirements change, the organization can also adapt quickly to scale.

KYC Standards Continue to Expand and Change

Figure 5. The Basic Tenets of KYC Today



Source: Javelin Strategy & Research, 2022

Executing KYC in an efficient, cost-effective manner can be complicated by extraneous issues such as outdated legacy systems, poorly designed data storage, and regulatory requirements that vary from country to country. Provisioning to the scale and needs of the business can start to feel more challenging than the task at hand.

The approach to solving KYC constraints starts with the lightness that an API provides when one API call can leverage a wide variety of validation tools such as behavioral biometric solutions, global watchlists, and decision engines.

It is also necessary that critical vendors are ready to accept the new ISO 27001 requirements to ensure high levels of security and stronger messaging across international business channels. The risk of identity fraud and imposters should also compel organizations to leverage identity-proofing techniques such as selfies or videos as part of the requirements of a customer identification program (CIP).

Information security should also be top of mind, as sensitive data and images are used as part of any KYC program. Tokenized biometrics, when available, can optimally protect a wide range of biometric images and calculations so that, for example, fingerprints or facial recognition images are unreadable and obfuscated to protect sensitive information from being stolen and repurposed by criminals.

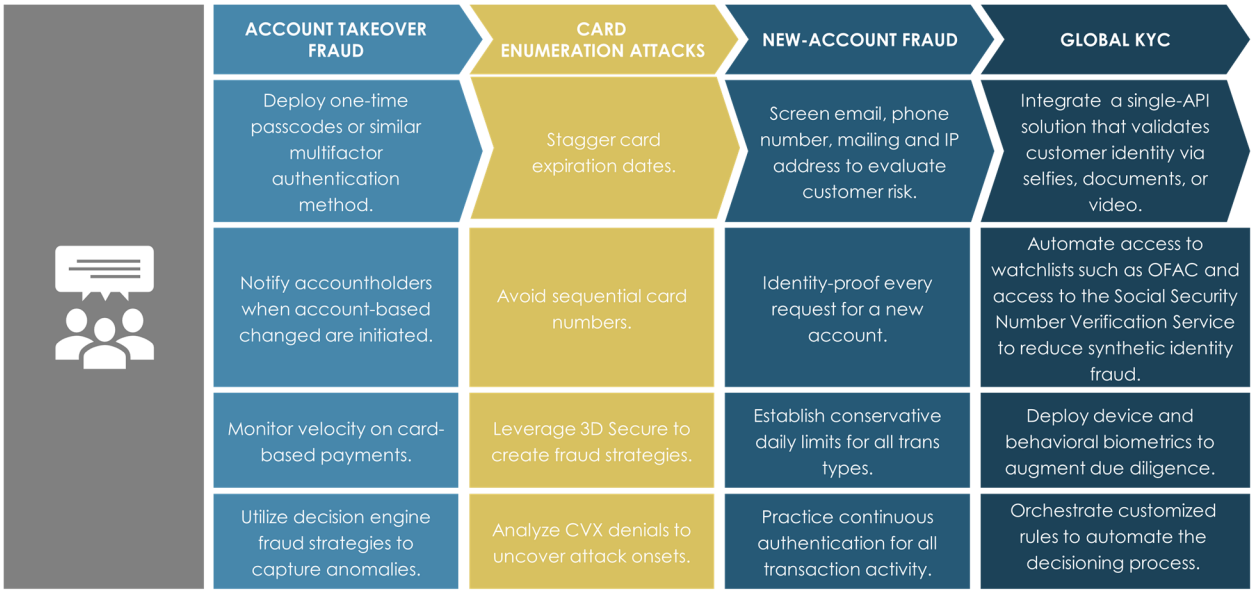
SCALING FUNDAMENTALS ACROSS THE BUSINESS ENTERPRISE

Alleviating the rising threat of identity fraud across the digital channel will always involve a multilayered approach. The abundance of organizational siloes and vast array of consumer product offerings require specialized treatment. The good news here is that many fraud prevention tools and practices can perform double duty, lessening the need for continuous investments. Business enterprises should also seek options that may reside on a single platform, enabling a layered plug-and-play product acquisition to be deployed as the needs of the organization expand.

Old-school card enumeration attacks have gained power as criminals leverage automation to execute attacks that are faster and more accurate. To avoid rampant losses stemming from card enumeration attacks, issuers must revise certain archaic practices that help to proliferate these attacks, such as issuing payment cards and expiration dates in sequential order. Card verification (CVV and CVC) denials should be scrutinized closely to help identify emerging enumeration attacks. To help stabilize the card authorization process, card issuers need to fully embrace 3D Secure technology.

Alleviating the Rising Threat of Identity Fraud Across the Digital Channel

Figure 6. Final Recommendations



Source: Javelin Strategy & Research, 2022

This can be achieved with a strong focus on APIs that provide single-call access to a wide variety of product modules. Identity-proofing techniques remain a constant staple across account, card, and KYC channels. The driving demand for identity verification is increasing, and therefore organizations should deploy products that not only identify the customer with a selfie but also then serve in the same capacity during step-up authentication across multiple verticals. As criminals continue to manipulate consumers with socialized scams, multifactor authentication methods such as one-time passcodes remain essential as elements that help to identify, protect, and provide access to legitimate accountholders.

ENDNOTES

1. **2022 Identity Fraud Study: The Virtual Battleground**, Javelin Strategy & Research, March 2022.
2. Ibid
3. https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/synthetic-identity-payments-fraud/synthetic-identity-fraud-defined/. Accessed May 31, 2022.
4. https://www.darkreading.com/attacks-breaches/magecart-how-its-attack-techniques-evolved. Published Sept. 14, 2021; accessed May 31, 2022.

METHODOLOGY

The Javelin 2022 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 Oct. 30 through Nov. 16, 2021. 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%.

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 THE AUTHOR

John Buzzard
Lead Fraud & Security Analyst

CONTRIBUTORS:

Suzanne Sando
Senior Analyst, Fraud & Security

ABOUT JAVELIN STRATEGY & RESEARCH

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