JAVELIN

A ZERO-DAY MISSION TO REDUCE ACCOUNT-BASED FRAUD

OCTOBER 2021

PART OF THE ESCALENT FAMILY

TABLE OF CONTENTS

TABLE OF FIGURES

FOREWORD

This report, sponsored by Neustar, explores how advanced authentication practices can help financial services providers differentiate between threat actors and legitimate accountholders without compromising the legitimate client's access to accounts and services.

This report was adapted from the 2021 Identity Fraud Study Shifting Angles, published by Javelin Strategy & Research in March 2021. Javelin Strategy & Research maintains complete independence in its data collection, findings, and analysis.

OVERVIEW

Treating every new client as a potential criminal is no way to begin a long and fruitful business relationship. Advancements in technology should empower rather than hinder new account openings and long-term fraud detection practices that help capture account-based fraud without a dependency on massive data collection practices that can take time to establish.

EXECUTIVE SUMMARY

Client experience is a continual balancing act for most financial institutions. When net new consumers present themselves during an account-opening session, the focus should really be devoted to expediting the account-opening process by placing the most inconvenience on fraud actors who fail to adequately pass authentication.

67% of consumers received a one-time passcode as the only form of validation for account opening in 2020. Part of the problem that most companies face is a lack of contemporary and scalable authentication methods for new accounts. During the early stages of the COVID-19 pandemic, consumer authentication was often relegated to remote verification steps that were not always accurate.

46% of consumers were asked to provide a photo selfie in 2020. Requests for photo selfies indicate the usage of some advanced forms of identity-proofing practices, which also help support new customers who rely heavily on mobile devices and branded banking apps for conducting important financial transactions.

Financial institutions still need to solve for the permanency of remote financial transactions. 45% of consumers in 2020 made visits to a physical location to complete verification for a new account application. As consumers adopt more digital habits, there must be provisions for seamlessly handling identity validation during the origination process without requiring the account holder to show up at a physical location.

Consumers are leveraging mobile apps and mobile chat capabilities to perform account changes. 30% of legitimate consumers used mobile banking apps for initiating account changes in 2020, and 13% indicated using mobile banking app chat features to perform similar tasks. This diverse usage across digital amenities necessitates the need for constant monitoring across the business enterprise for device IDs, IP addresses, and other unique identifiers. Those unique identifiers can help detect potentially fraudulent usage.

Detecting account-based fraud has become an endurance contest that requires long-term monitoring. Financial services providers need to be able to continually monitor account-change events for classic examples of synthetic identity fraud such as *piggybacking,* in which the criminal adds an authorized user to an account that is in good credit standing.

Thin files are not always the calling card of criminal impostors. Thin files are not always a harbinger of fraud, but the mere lack of available public information pertaining to a new account requester should signal the

need for additional validation of identity. That validation should examine a combination of elements, such as name, phone number, physical location, and device identity.

Account takeover fraud detection has to evolve past KYC challenge questions. Criminals often deploy elaborate scams that allow them to deceive consumers into divulging their personally identifiable information (PII) and, in addition to PII, consumers often disclose extraneous personal information that criminals use to overcome *know your customer* (KYC) challenge questions, ultimately rendering those questions useless.

There is a particular rhythm to account takeover tactics. It comes as no surprise (see Figure 4) that criminals have certain tasks they need to perform to execute a smooth account takeover, and the patterns of activity are quite revealing. For example, 24% of criminals change the payment card PIN, enabling them to smoothly facilitate ATM and POS cashback transactions. Passwords, contact phone numbers, and new debit card requests occur in 22% of ATO cases, because criminals want a physical card with a new PIN to speed the process of draining accounts.

RECOMMENDATIONS

Use technology that has the ability to analyze diverse data points. The decision process should not hinge entirely upon forcing legitimate consumers to prove their identity. As more consumers present personas that lack mature data points, keep in mind that the objective should be focused on step-up authentication, to ensure faster account access for legitimate customers.

Perform identity-proofing exercises for all government-issued forms of identification. Financial services providers have to leverage technology that allows them to authenticate forms of identification with the purpose of isolating counterfeits. Identity-proofing practices usually involve third-party vendor technology that not only scans the identity document for validity but also requires some form of selfie image to confirm the *liveness* of the individual applicants.

Improve remote account origination processes to help prevent account-based fraud. Consumers have firmly adopted a variety of online habits that will most likely increase. This shift in consumer behavior has strong implications for growing incidents of fraud if identity-proofing tactics are not embedded into a seamless and efficient process that includes face-to-face and remote digital customer interactions.

Focus on a combination of identifiers from multiple sources to make stronger decisions. Consumers have multiple identifiers that should be evaluated in addition to government-issued IDs. Mobile devices and IP and email addresses can all come together to form a much stronger decision during the origination process, especially when biometrics are layered in to help authenticate the customer.

Monitor the account life cycle by continuously authenticating a variety of elements. The importance of monitoring changes in account behavior over a period of time will help to quickly detect account-based fraud across synthetic and traditional identity fraud scenarios.

Analyze credit utilization across the account life cycle. Criminals realize their actions are being watched over a much longer period for signs of potentially fraudulent behaviors. Sudden increases in overpayments and rapid utilization of available credit should be accounted for via stringent monitoring to help reduce account bust-out fraud.

Understand how account changes help to serve as an early warning sign for fraudulent activity. It would be impossible to monitor and account for every account change without a fraud-detection solution

capable of analyzing account changes 365 days a year. The key is combining the findings more contextually so that faster decisions can be executed to detect and reduce fraud.

Notify existing accountholders when new accounts are opened in their names. Criminals have already demonstrated how easy it is to open new accounts at financial institutions where their victims already own accounts. Notifying consumers about the presence of new accounts that match their PII should be standard practice, especially when mailing addresses and other identifiers are not used to create the new accounts. There may be occasions in which where separate accounts are created for non-fraudulent purposes, but their creation should still involve some written form of communication that confirms the account-opening event.

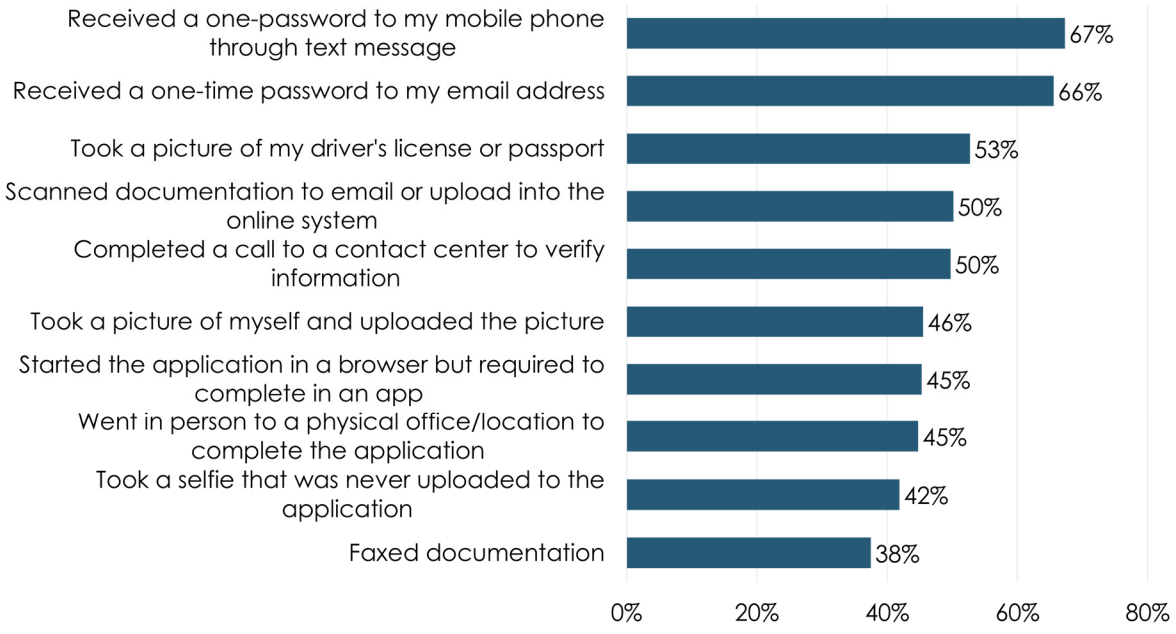
NEW ACCOUNT FRAUD: SEPARATING LEGITIMATE INTERACTIONS FROM POTENTIAL FRAUD

Serial criminals spend a great deal of time focusing on how to blend in. When net new consumers present themselves during account-opening, the focus should be on expediting the account-opening process for validated customers while applying more friction to suspected fraud actors when their credentials appear questionable. The camouflage of choice for an experienced criminal might involve a counterfeit government identification card that includes a photograph of the criminal imposter, and, in some cases, backup documents, such as forged leases, fake utility bills, and altered employer W-2s.

Every organization should have step-up authentication processes for handling documentation problems to address these issues. The step-up processes should include strong identity-proofing biometrics that help to identify counterfeit government-issued forms of identification. Regardless of whether career criminals are arming themselves with a battery of forged documents or stolen true identities, the

Authentication Methods Need to Be More Consistent

Figure 1. Variety of New Account Authentication Methods Executed by Consumers in 2020



Source: Javelin Strategy & Research, 2021

emphasis should still remain squarely on how to grant account access and enhance the experience of legitimate customers while keeping criminals at bay.

Part of the challenge faced by most companies is a lack of contemporary and scalable authentication methods for new accounts. Financial institutions should focus more attention toward the validation of IP location to help counteract criminals who operate outside the U.S. and/or outside the location where the true customer is expected to be. Device ID, when monitored, can help to corroborate the overall identity of the customer by comparing the device ID and mobile carrier data to help establish global trust based on potentially fraudulent events that have occurred elsewhere.

Authentication can also shift from digital to physical (see Figure 1). 45% of consumers said they were forced to make visits to a physical location to provide authentication for a new account application amid work and social isolation during the early stages of the COVID-19 pandemic contributing to less-than-accurate results when untrained personnel were forced to evaluate government-issued identification and other supporting documentation that was required as part of an account origination procedure.

Consumers also snapped pictures of their government-issued identification (53%) indicating the presence of more advanced identity-proofing measures that may have been in practice at various financial service providers. The more troubling authentication methods in 2020 leaned too heavily on scanned documents (50%) that could be counterfeits, while another 50% of consumers answered authentication questions via a contact center interaction that naturally would have been predisposed to errors as call center staffing levels plummeted and hold times increased.

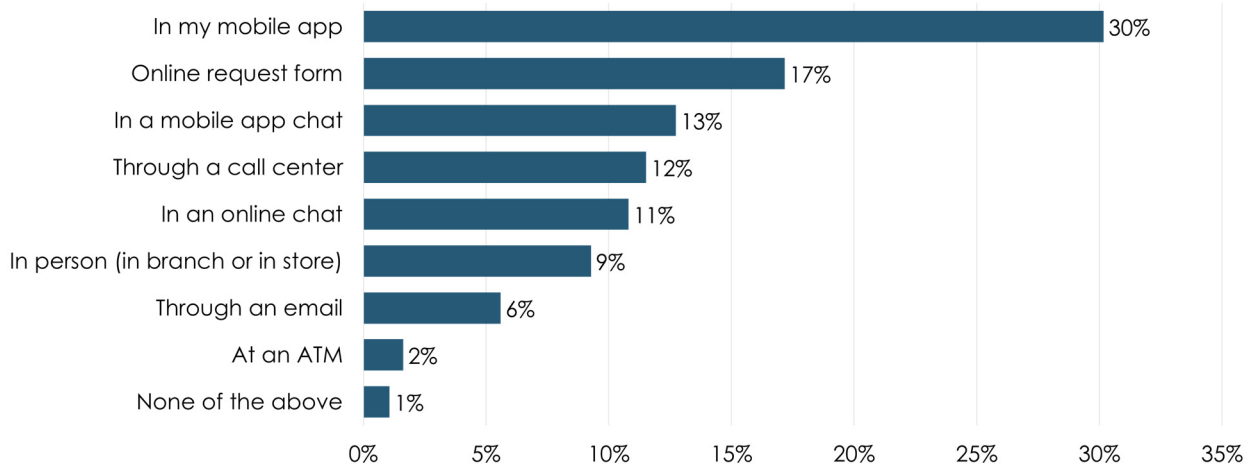
While the methods used by consumers to help authenticate their identities were not mutually exclusive to just one thing in 2020 (see Figure 1), it remains evident that some authentication practices relied too much on human visual comparison when stronger forms of identity-proofing technology could have performed a more accurate appraisal resulting in less fraud.

SYNTHETIC IDENTITY FRAUD: THE CRIMINAL LONG GAME

Synthetic identity fraud can often seem like a paradox because it has lacked a proper definition for many years. Estimates suggest that synthetic identity fraud has cost U.S. lenders up to $6 billion (USD), and that the financial losses account for 10% to 15% of charge-offs in a typical unsecured lending portfolio.[1] The Federal Reserve recently defined synthetic identity fraud as "The use of a combination of personally identifiable information to fabricate a person or entity in order to commit a dishonest act for personal or financial gain."[2] The Federal Reserve's intention in defining synthetic identity fraud was to draw attention to the pernicious growth of synthetic fraud. Additionally, with a universal definition of synthetic identity fraud, industry stakeholders are better equipped to develop metrics for tracking and detecting synthetic personas. New account fraud (NAF) presents a major problem that requires additional identity-proofing to limit criminal success rates. As criminals cultivate newly opened accounts for fraud, they often synthesize normal activity such as balance inquiries and simple account changes that help them establish a pattern of trust that elongates the account aging process. It is important for financial service providers to have a baseline idea of normal usage patterns for existing accountholders. For instance, 30% of consumers in 2020 used mobile banking apps for making account changes (see Figure 2), while 17% of consumers demonstrated their digital virtuosity by leveraging online request forms. While these activities seem subtle,

Consumer Behavior Is Not One-Size-Fits-All

Figure 2. 30% of Consumers Initiated Change Requests in 2020 Using a Mobile App



Source: Javelin Strategy & Research, 2021

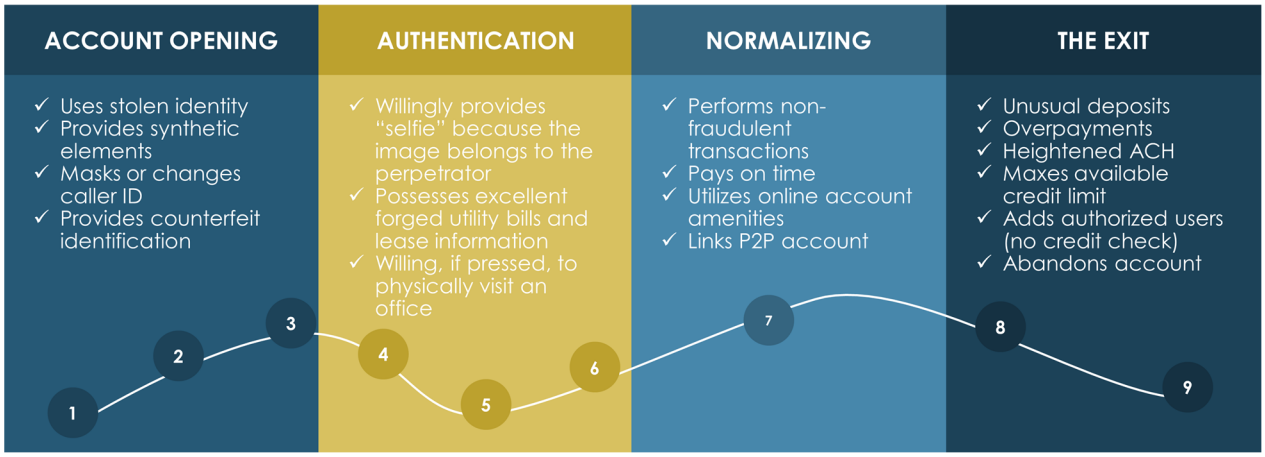
they are key indicators of how consumers conduct their personal business today and represent an important baseline that can be used to detect potentially fraudulent activity that could be hiding in plain sight.

The importance of monitoring changes in account behavior over a period of time adds clarity to the question of how to detect synthetic identity fraud before substantial losses occur. Financial services providers need to be able to continually monitor account changes for classic examples of synthetic identity fraud, such as piggybacking, in which the criminal adds an authorized user to an account that is in good credit standing. Authorized users are rarely validated against credit bureau information and thus present a significant threat due to the unevenness of the vetting process. The other challenge in managing NAF pertains to the account life cycle. There should be more emphasis placed on account activity during a much longer maturation period, as criminals open new accounts with the intent to nurture them to evade fraud detection. During the account-opening process, the absence of credit information or corroborating identifiers is often referred to as a thin file. Thin files are not always a harbinger of fraud, but the mere lack of available public information pertaining to a new-account requester should signal the need for additional validation. That additional validation of identity should include a combination of elements, such as name, phone number, physical location, and device identity. Simply validating a bevy of key identity elements will not eliminate sophisticated synthetic identity fraud, especially when criminals have, for example, cultivated email addresses that are accepted as legitimate due to a lack of technology that specializes in global trust scores for email and mobile numbers.

NAF and subsequent bust-out fraud (account abandonment) represents a virtual powder keg (see Figure 3) of bad debt hiding in plain sight across loans, credit cards, and demand deposit accounts (DDAs) when there is a lack of continuous authentication across identity and accountholder behavior. A lack of controls can enable criminals to suddenly

A Powder Keg Hiding in Plain Sight

Figure 3. Bust-Out Fraud: How Criminals Cultivate New Account Fraud with Synthetic Identities



Source: Javelin Strategy & Research, 2021

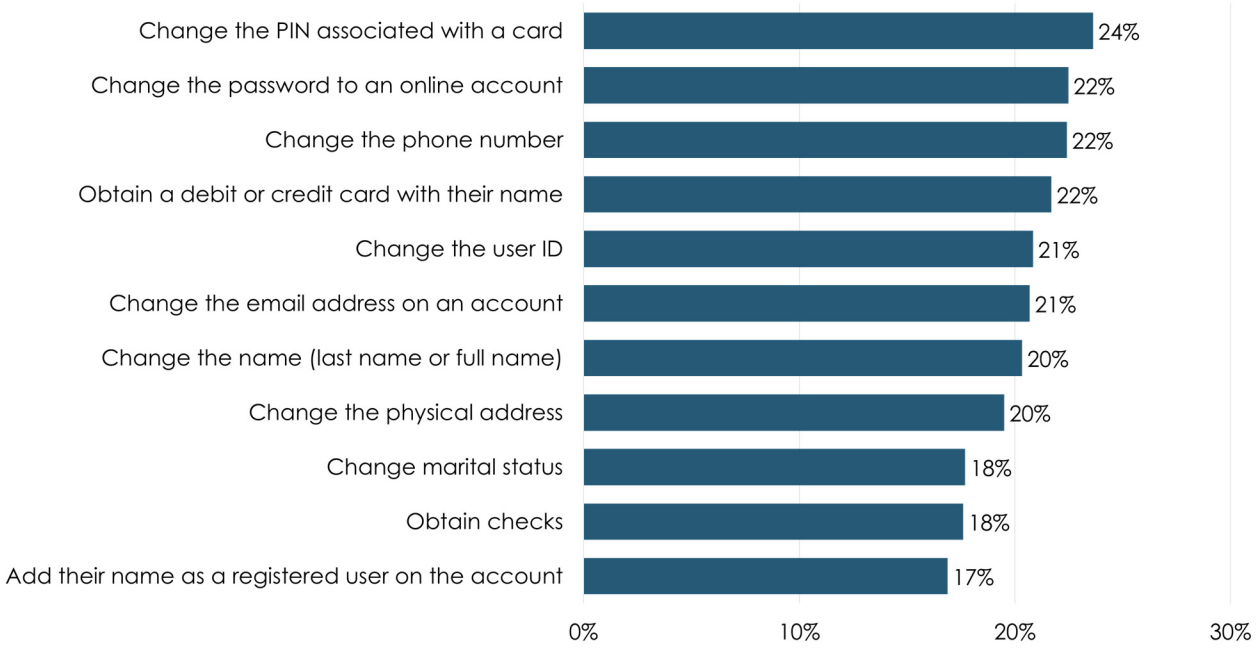
maximize credit lines, leaving a trail of unpaid debt that will eventually need to be charged off as the result of a classic bust-out fraud scenario. Losses can multiply quickly when criminals deploy mules who open multiple accounts via organizations where lax account-opening practices exist. Financial services providers should monitor account activity (and credit utilization) throughout the entire account life cycle to help reduce losses attributable to account-based and synthetic identity fraud.

DIGITAL BREADCRUMBS: USING TECHNOLOGY TO DETECT ACCOUNT TAKEOVER FRAUD

Criminals often deploy elaborate scams that allow them to deceive consumers into divulging their personally identifiable information (PII). In addition to PII, consumers also often disclose extraneous personal information about themselves, either directly to the criminal or by way of social media, that enables criminals to overcome know your customer (KYC) challenge questions. Technology is then used by criminals to mask their activities by obfuscating caller ID information via call spoofing and using a masking VPN that obscures their true geographic location. SIM-card swaps (mobile device takeovers) further add to criminals' Machiavellian tactics to take control of SMS capabilities and email accounts that typically reside within most mobile devices. Email and SMS-capable devices are primary endpoints or

Criminals Leave a Trail of Digital Breadcrumbs

Figure 4. Actions Criminals Perform After Taking Over an Account



Source: Javelin Strategy & Research, 2021

tools used today to verify financial account changes. It comes as no surprise (see Figure 4) that criminals have certain tasks they need to perform to execute a smooth account takeovers (ATOs), and the patterns of activity are quite revealing. For example, 24% of criminals change payment card PINs, which allows them to more easily conduct ATM and POS-cashback transactions. Passwords, contact phone numbers, and new debit card requests occur in 22% of ATO cases, because criminals want a physical card with a new PIN to speed the process of draining accounts. User ID credentials and email addresses (both 21%) help partition the consumer's ability to log in to own accounts, thereby interfering with the criminal activity taking place. Shockingly, criminals may even elect to add their own names as registered users to an account (17%) in order to help them circumvent other obstacles, like mismatched identification or additional account-change requests.

THE MODEL FOR SUCCESS: COMBINING DATA POINTS

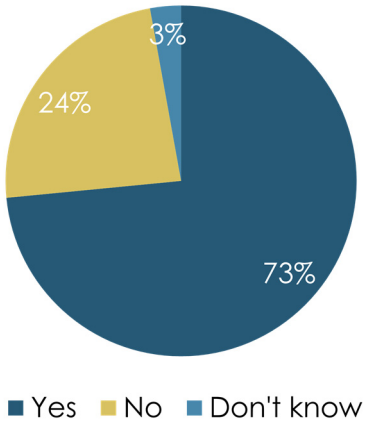
The only way to successfully reduce the threat of ATO fraud is to apply real-time analysis across account behavior, device identifiers — like IP address — and through the verification of biometric data, which can range from facial scanning to fingerprint and voice authentication. Financial services providers should focus on incorporating as many tactics as possible through a federated score of multiple data points. Doing so will help the organization make better decisions in real time. Avoiding the compromise of existing accountholders should also be a major focus for organizations that desire higher levels of consumer trust in their brands.

In 2020, 73% of new accounts were opened at the same financial institution where the victim already maintained active accounts. Criminals have realized for some time now that opening accounts using credentials that belong to existing bank customers is the easiest way to scale over fraud detection practices. It makes perfect sense that when consumers are not properly notified that additional accounts have been opened in their name, they immediately lose trust in their primary financial institution where the fraudulent activity took place. A general lack of trust can often lead to attrition as consumers are left pondering whether other unidentified problems exist beneath the surface. To counteract this issue, financial institutions should follow up every account opening with a combination of compliance letters, automated SMS (or email) alerts, and clearer visibility to all known accounts via online banking.

As organizations work toward a zero-day capability to reduce identity fraud, client experience has to remain a primary focus. Rewarding legitimate customers with less friction as they passively meet validation across user credentials and multiple data points such as mobile carrier information, device ID, and IP address provides a way for organizations to increase fraud detection without diminishing consumer trust or experience.

Undetected Criminal Activity Jeopardizes the Trust of Existing Customers

Figure 5. New Accounts Opened by Criminals Where the Victim Already has Accounts Established



Source: Javelin Strategy & Research, 2021

METHODOLOGY

In October 2020, Javelin conducted a nationally representative online survey of 5,000 U.S. consumers to assess the impact of falling victim to identity fraud, uncover where criminals are making progress, explore consumers' actions and behaviors, and identify segments of consumers most affected by fraud.

ENDNOTES

1. https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/synthetic-identity-fraud-definition/. Accessed Aug. 25, 2021.
2. https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/synthetic-identity-payments-fraud/synthetic-identity-fraud-defined/. Accessed July 25, 2021.

ABOUT NEUSTAR

Neustar is an information services and technology company and a leader in identity resolution providing the data and technology that enable trusted connections between companies and people at the moments that matter most. Neustar serves more than 8,000 clients worldwide, including 60 of the Fortune 100.

ABOUT THE AUTHOR

John Buzzard
Lead Analyst, Fraud & Security

CONTRIBUTORS:

Jacob Jegher
President

Tracy Kitten
Director, Fraud & Cybersecurity

Suzanne Sando
Sr. Analyst, Fraud and Security

Crystal Mendoza
Production Manager

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