EQUIFAX®

THE IDEAL CRIMINAL TARGET:
NO ONE IS IMMUNE

OCTOBER 2022

PART OF THE ESCALENT FAMILY

JAVELIN

TABLE OF CONTENTS

TABLE OF FIGURES

ABOUT THE AUTHOR

Suzanne Sando
Senior Analyst,
Fraud & Security

CONTRIBUTORS:

John Buzzard
Lead Analyst, Fraud & Security

Alexander Franks
Analyst, Fraud & Security

FOREWORD

This report, sponsored by Equifax, explores the widespread effects of identity fraud on consumers, regardless of age or socioeconomic status, and the importance of taking advantage of fraud detection and prevention services. This report is derived 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

Consumers of all kinds are ideal targets for cybercriminals. As losses from traditional identity fraud and identity fraud scams increase, consumers cannot let down their guards for a moment, because all it takes is that one moment for a criminal to steal an unsuspecting consumer's identity. Criminals are constantly refining their tactics to capitalize on exploiting as many consumers as they can, leaving no one behind. Factors such as age, income, and education level do not concern a cybercriminal who is selecting the next target for identity fraud. No one is off-limits.

Consumers must be equipped with tools and education to safeguard their identities from the criminals who are launching constant attacks. Moreover, organizations must provide services and amenities that assist with identity protection and remove the sole responsibility for preventing identity fraud from consumers. Layering comprehensive education with innovative technology will aid in mitigating the threat of identity fraud.

JAVELIN

KEY FINDINGS

Although the ways consumers are targeted by cybercriminals may vary, no one is impervious to the threat of identity fraud. The effects of identity fraud are wide-reaching, regardless of income, education, or generation. Each group may be targeted in a slightly different way as criminals adapt to factors such as consumer habits and device use behaviors, but criminals do not discriminate when choosing a target for identity fraud. The ultimate goal for a criminal is to quickly acquire fast cash, and it likely doesn't matter how that fast cash is obtained. Whether a criminal is working alone or as part of a larger network or organization, any consumer with a digital footprint and available funds and accounts is up for grabs.

Consumers of all generations are experiencing increases in unwanted communication. Consumers across the board noted surges in unsolicited communication such as robocalls, spam texts, and emails, as well as social media requests from strangers. Criminals have modified strategies for each generation, attempting to trick consumers by using the communication method most familiar to and generally used by each generation. Nearly 7 in 10 Baby Boomers (65%) noted an increase in robocalls, while nearly half of Gen Z (46%) and Millennials (46%) perceived a surge in unwelcome social media requests from strangers.

Identity fraud is not a one-and-done situation—consumer identities can live on the dark web forever. Once victimized by identity fraud, some consumers might not realize that a criminal can continue to use and abuse their personally identifiable information (PII) as long as it goes undetected or unresolved. If the victim doesn't take any action or has no monitoring or detection in place, it's simple for a criminal to continue the exploitation of a stolen identity. Moreover, victims' PII may be sold on the dark web, available for further manipulation by other cybercriminals, in ways that are often difficult to detect. Legitimate PII may be used to create synthetic identities, which are not tied to real consumers (although they contain real parts of consumer data).

Not enough consumers take advantage of tools designed to prevent and detect identity fraud. Many consumers who haven't been victimized by identity fraud may not feel these tools and services are necessary to protect their information, and unfortunately, many won't recognize the value until it's too late. Nearly six in 10 consumers (58%) do not use an identity protection service, and that's just the beginning of the neglect. Over half of consumers aren't reaping the benefits from tools and services such as security freezes, virtual private networks (VPN), or password managers. Relying on fraud detection and prevention technology frees up precious time for consumers to focus on their day-to-day lives.

Education is on the minds of consumers. Consumers want to be able to protect themselves from identity fraud. Over half of consumers (54%) believe a fraud prevention resource center would be useful in educating them about fraud prevention. Additionally, consumers find value in educational videos about staying safe from fraud (49%) and online quizzes with fraud prevention strategies (44%). It's up to financial institutions and identity protection providers to make fraud prevention educational materials readily available and easily accessible so consumers can educate and empower themselves.

RECOMMENDATIONS

Emphasize the importance of a proactive stance in identity protection and fraud prevention. Consumers are creating opportunities for criminals to steal their identities by not using tools and services such as security freezes on credit, virtual private networks on devices like a laptop or a phone for personal use, and identity protection services. Financial institutions and identity protection providers must highlight how much easier it is to mitigate identity fraud attempts with proactive measures rather than reactive scrambling.

Highlight safe digital banking and internet use habits. Consumers who regularly practice good cyber and digital banking hygiene will undeniably experience a diminished threat of future encounters with identity fraud. Organizations should highlight what constitutes good cyber and digital banking hygiene so consumers know the habits they need to make or break. Using a password manager to generate and securely store strong passwords will cut down on password reuse by consumers who tend to spread those usernames and passwords across multiple accounts. Consumers should also get in the habit of using a VPN on their personal devices. Additional safeguards—such as fraud alerts and security freezes on credit reports—significantly reduce the chances that a criminal will be able to further exploit consumer PII exposed on the dark web.

Maintain a centralized current and trending scam hub that is easily accessible by consumers. Consumers should have access to up-to-date information and educational materials on current and trending scams to empower them to recognize potential identity theft and prevent it. Well-informed consumers have a keen sense of awareness and will be more perceptive of scam threats, which will translate into a stronger identity fraud defense.

Layer education and advanced fraud detection and prevention technology together to maximize identity protection. Relying on consumers to be well-informed of scam and identity fraud threats is critical to a robust fraud defense, but it is not enough to thwart every fraud attempt. Maximum protection for consumer identities means weaving fraud prevention and detection technology with comprehensive educational tools. Identity protection requires effort from consumers and providers alike. Organizations must emphasize the importance of consumer education while also providing fraud detection and prevention tools needed to protect consumers' identities.

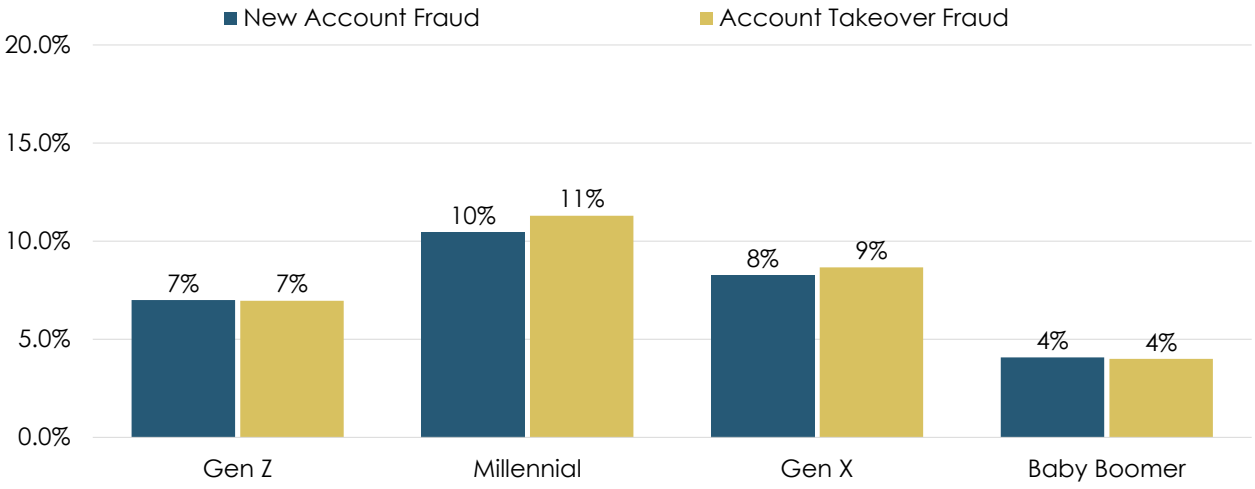
Remove sole responsibility for detecting and preventing identity fraud from consumers. Identity protection doesn't require constant vigilance on the part of the consumer—plenty of tools can be employed in the background to relieve a large portion of the burden from the consumer. Organizations have the capability to handle many of the tasks involved in fraud detection and prevention that are often left to consumers. Assuming the responsibility of constant credit and account monitoring is a great start toward freeing up consumers' time.

IDENTITY FRAUD LANDSCAPE: THE WHO AND THE HOW

Identity fraud losses again reached incredible heights in 2021, with consumers of all ages and socioeconomic backgrounds falling victim. Identity fraud losses reached $52 billion across 42 million U.S. adult consumers.[1] There were significant increases across all account-based fraud categories tracked by Javelin, such as new-account fraud (up 109%) and account takeover fraud (up 90%). Not all fraud victims are unsophisticated targets lacking technical savvy. More and more, criminals are pursuing victims of all kinds through a variety of methods, casting a wide net in hopes of catching large numbers of victims and thus making every consumer a viable option for untapped revenue. Although criminals vary their tactics by generation, no one is immune to the threat of identity fraud. Criminals had a tendency to target younger generations through new-account fraud and account takeover fraud at higher rates than older consumers (see Figure 1). In general, Millennials have a greater propensity than their older counterparts to own more accounts of all types, ranging from merchant to P2P to social media, creating a larger digital footprint and more opportunities for criminal exploitation. Of Millennials who were victims of identity fraud, 21% were specifically targeted through new-account fraud (10%) and account takeover fraud (11%), compared with only 8% of Baby Boomers who were specifically targeted through new-account fraud (4%) and account takeover fraud (4%). But identity fraud still presented a challenge for all consumers, with criminals shifting gears for each victim they pursued.

Identity Fraud Threats Differ Across Generations

Figure 1. New-Account Fraud and Account Takeover Fraud Incidence Rates, by Generation



Source: Javelin Strategy & Research, 2022

[1] Javelin Strategy & Research. https://javelinstrategy.com/2022-Identity-fraud-scams-report. Published March 29, 2022; accessed June 2022.

JAVELIN

Many consumers experienced an exorbitant amount of unsolicited spam communication in 2021, from robocalls to spam texts to emails with suspicious links or attachments. Criminals seemed to shift their tactics by targeting specific consumers based on their age and what types of communication were assumed to be the most common among that age group. This was undoubtedly done with the hope that the communication would be considered legitimate by a potential victim.

A larger portion of older consumers, such as Baby Boomers, experienced an increase in robocalls compared with their youngest counterparts, Gen Z (see Figure 2), as older consumers are more likely to regularly receive—and answer—phone calls. Conversely, more Gen Z and Millennial consumers experienced a significant surge in unwanted social media requests from strangers in comparison with their older counterparts, likely because they have a greater presence on social media and a higher comfort level with engaging via chat mechanisms.

Criminals Adjust Their Tactics for Each Generation

Figure 2. Increases in Unwanted Communication in 2021, by Generation

	Robocalls	Unusual Text Messages	Emails with Suspicious Links	Social Media Requests from Strangers	Emails with Suspicious Attachments	Chatbots
Gen Z	52%	52%	39%	46%	29%	18%
Millennials	60%	53%	46%	46%	36%	24%
Gen X	59%	53%	50%	44%	43%	22%
Baby Boomers	65%	46%	45%	31%	37%	14%

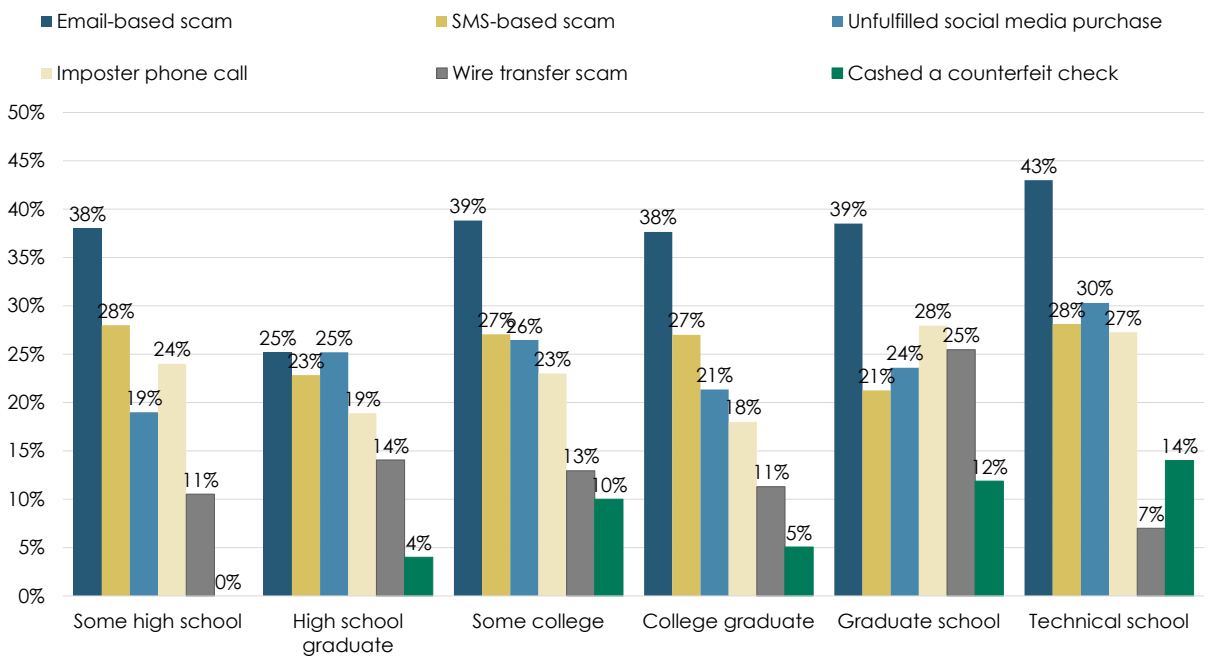
Source: Javelin Strategy & Research, 2022

Identity fraud does not discriminate. Almost every consumer is considered fair game to a criminal. Although factors like income may affect the amount of illegally obtained funds fraud actors are able to get their hands on, not much separates one consumer from the next regarding how criminals choose to target their victims. Formal education is not necessarily indicative of a consumer's ability to detect and prevent a scam, nor is a lack of it an indicator of naiveté. Advanced levels of formal education do not automatically make one consumer any safer than another from the threat of identity fraud scams.

In comparing consumers with varying levels of formal education, Javelin discovered somewhat similar efficacy of scams, regardless of the consumer's highest level of education completed (see Figure 3). Email-based scams were the most effective way for criminals to deceive consumers, whether the consumer held a high school diploma (25%) or a college degree (38%). Fraud actors recognize how prevalent email use is across all consumers. One would be hard-pressed to find a consumer without an email address—whether the mail account was initiated by the consumer or was automatically provided through work, school, or even as a part of cable, internet, or mobile services. Check fraud, such as counterfeit checks, victimized fewer consumers across education levels with physical check usage declining in favor of faster forms of payment.

Every Consumer Is Fair Game to a Cybercriminal

Figure 3. Scam Methods Used to Victimize Consumers in 2021, by Highest Level of Education Completed



*Respondents could select multiple options

Source: Javelin Strategy & Research, 2022

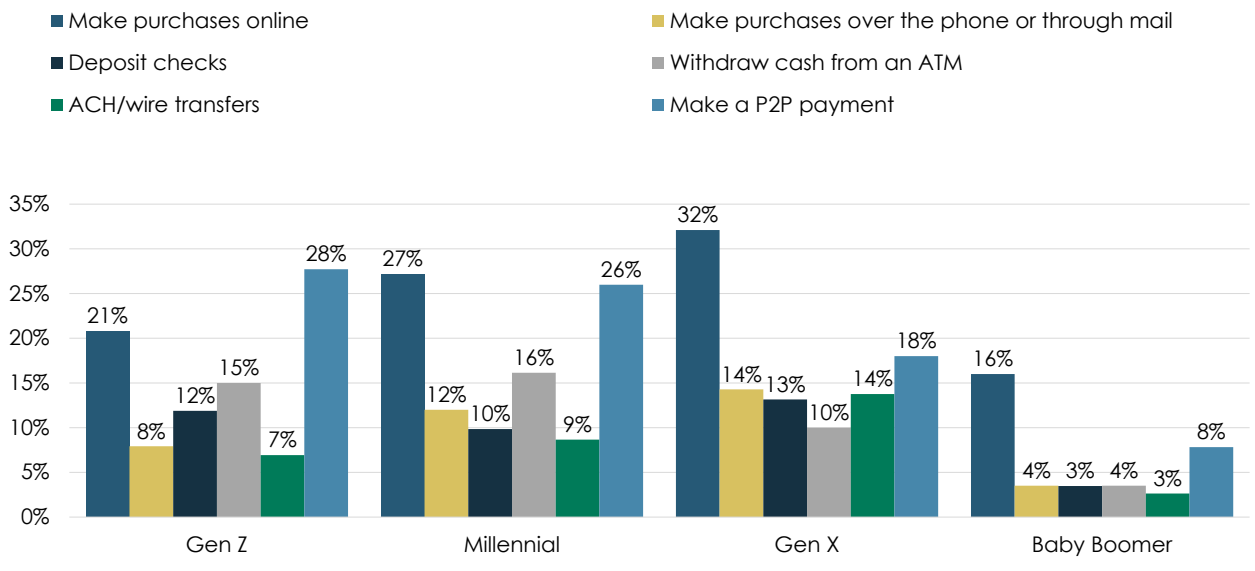
A similar parity exists among the specific actions different generations of consumers were persuaded by criminals to perform, resulting in a loss of funds (see Figure 4). Although the efficacy of each scam action varies slightly across all groups, criminals were able to pinpoint the most successful schemes and stick to them, regardless of generation.

Persuading consumers of all ages to make purchases online and make person-to-person (P2P) payments proved to be lucrative for criminals. Conversely, actions such as persuading a consumer to make a purchase over the phone or through mail and ACH/wire transfers were not as successful, in general. The most successful and prolific scams focus on extracting enough PII from the consumer to perpetrate a multitude of schemes quickly using electronic means. This is why corporate entities should devote consistent messaging about financial crime vulnerability to their consumer audiences.

Knowing how they may be targeted by criminals builds a strong foundation for consumers in preventing identity fraud. Consumers should have access to up-to-date information and educational materials on current and trending scams to empower them to recognize potential identity theft and prevent it. Well-informed consumers have a keen sense of awareness and may be more perceptive of scam threats. Although the responsibility of preventing and detecting identity fraud should not be fully on the shoulders of consumers, they serve an important role in mitigating future fraud.

Scams Are Effective, Regardless of Generation

Figure 4. Scam Loss Types, by Generation



Source: Javelin Strategy & Research, 2022

REACTING TO IDENTITY FRAUD: PLAYING FROM BEHIND

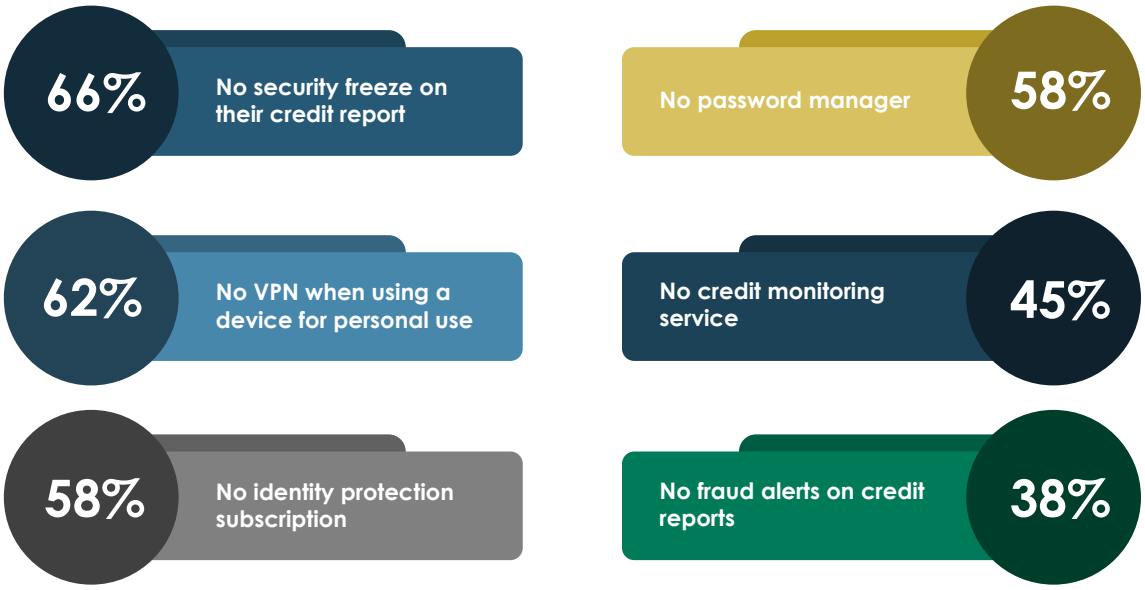
Consumers may not realize that criminals can continue to use and abuse victims' PII as long as it goes undetected or unresolved. If the identity fraud victim doesn't take any action or has no monitoring or detection in place, it's simple for a criminal to continue exploiting a stolen identity. Moreover, victims' PII may be sold on the dark web, available for further manipulation by other cybercriminals, in ways that are difficult to detect.

Legitimate PII can be used to create synthetic identities, which are not tied to real consumers (though they contain real parts of consumer data). Identity fraud is not a one-and-done situation-—consumer PII can live on the dark web forever. And though it's virtually impossible to remove PII for sale on the dark web, consumers can take plenty of steps to prevent cybercriminals from taking advantage of information that's out there. That's where it becomes critical for consumers to be proactive about establishing a strong identity fraud defense.

Too many consumers are missing the opportunity to utilize the options available to them to prevent and detect identity fraud (see Figure 5). Consumers are creating opportunities for criminals to steal their identities by not employing tools and services such as security freezes on credit (66%), VPNs when they use devices like a laptop or phone for personal use (62%), and identity protection services (58%).

Many Consumers Don't Take Advantage of Existing Tools

Figure 5. Consumers Who Do Not Use Available Identity Protection Tools



Source: Javelin Strategy & Research, 2022

Nearly half of consumers (45%) do not use a credit monitoring service, arguably one of the most effective and uncomplicated ways to keep an eye on not only financial fitness but also unexpected or unauthorized activity on existing or new accounts.

Some consumers who haven't been victimized by identity fraud may not feel these steps are necessary to protect their information and identities, and unfortunately, many won't recognize the tools' value until it's too late and their identities have already been compromised.

Consumers and organizations must recognize that effective fraud prevention and detection goes beyond resolution. It's not enough to simply resolve a singular instance of identity fraud. The prevalence of consumer PII on the dark web has made that abundantly clear.

Without concrete measures to lock down their identity, the likelihood that consumers find themselves in a fraud situation down the road is incredibly high (see Figure 6). Criminals can reuse a fraud victim's information as many times as they want as long as the fraud goes undetected.

Consumers may find themselves in situations where new accounts are fraudulently opened in their name or a fraud actor assumes control of legitimate accounts using stolen PII. Once criminals gain access to PII on the dark web, they will squeeze whatever mileage they can out of victims' identities.

Identity Fraud Resolution Should Be Immediate

Figure 6. Missed Opportunities Pressurize Identity Fraud Losses

Source: Javelin Strategy & Research, 2022

WHAT CONSUMERS— AND ORGANIZATIONS—SHOULD BE DOING

With the ever-growing threat of identity fraud coming from all sides, it's never been more essential for consumers to be aware of how they may be targeted by cybercriminals and to have the right precautions in place to prevent identity fraud altogether. Consumers need to understand how much easier it is to mitigate identity fraud attempts when their approach is proactive rather than reactive.

The good news is that education is on the minds of consumers. Over half of consumers (54%) believe a fraud prevention resource center would be useful in educating them about fraud prevention. Additionally, consumers find value in educational videos about staying safe from fraud (49%) and online quizzes with fraud prevention strategies (44%). It's up to financial institutions and identity protection providers to make fraud detection and prevention educational materials readily available and easily accessible for consumers to educate and empower themselves.

Those who practice good cyber and digital banking hygiene will undeniably experience a diminished threat of future encounters with identity fraud. Organizations should highlight what constitutes good cyber and digital banking hygiene so consumers know the habits they need to make or break. Consumers can take numerous actions to protect their identities and PII.

Using a password manager to generate and securely store strong passwords will cut down on password reuse by consumers who consistently recycle usernames and passwords across multiple accounts. Consumers should also get in the habit of using a VPN on their personal devices. Additional safeguards—such as fraud alerts, credit locks, and security freezes on credit reports—significantly reduce the chances that a criminal will be able to further exploit consumer PII exposed on the dark web. Identity protection service providers must provide access to these kinds of features, and consumers should take full advantage of the tools available to them in order to prevent unauthorized access to their credit.

What's more, consumers who entrust an identity protection service to protect them from identity theft are relieved of a sizable responsibility of constant vigilance of their accounts (financial and non-financial), their credit, and their general digital footprint. The removal of this burden frees up consumers to empower themselves with education on how to detect and prevent scam and identity fraud attempts. Concentrate on demonstrating the value of a comprehensive fraud defense that uses existing identity protection tools and services woven together with consistently updated education on current consumer threats.

METHODOLOGY

The 2022 ID 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 EQUIFAX

At Equifax (NYSE: EFX), we believe knowledge drives progress. As a global data, analytics, and technology company, we play an essential role in the global economy by helping financial institutions, companies, employers, and government agencies make critical decisions with greater confidence.

Our unique blend of differentiated data, analytics, and cloud technology drives insights to power decisions to move people forward. Headquartered in Atlanta and supported by more than 13,000 employees worldwide, Equifax operates or has investments in 25 countries in North America, Central and South America, Europe, and the Asia Pacific region. For more information, visit Equifax.com.

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.