IDology
a GBG company

Research Paper

Eighth Annual Fraud Report

The Beginning of a New Chapter: COVID, the Rush to Digitization, and the Impact on Fraud

Table of Contents

We've Never Been Here Before, But the Future Looks a Little Brighter

By now, you've likely probably read countless articles and reports that attempt to make sense of 2020 and put the year in perspective. Without a doubt, the COVID-19 pandemic changed many aspects of society for good. The virus forced companies and consumers to accelerate their digitization existence, sometimes in life-or-death circumstances, and what would have taken years to accomplish took place in months. How firms and humans interact has been transformed and to some extent permanently. And with it, the fundamental benefits of digital benefits will be reaped.

The pandemic served as an existential threat and unsettling daily deadly event throughout the year, as it does today. It scared people, forcing them to make previously unimaginable changes in their work and personal life. At the same time, criminals and nation-states that intended to do harm wasted little time in taking advantage of the global crisis.

We saw governments approve massive aid packages to mitigate the economic effects of the virus, while many organizations adopted work from home (WFH) arrangements. Unfortunately, confining employees to their homes provided a fertile hunting ground for fraudsters. Not surprisingly, the online and mobile channels continued to sit firmly in the crosshairs of criminals. Synthetic fraud continued to grow and inflict losses across the economy as well. This will undoubtedly remain the case in 2021 and beyond.

Executive Findings

- In 2020, fraud attempts sharply increased – companies reporting fraud attempts increased compared to the prior year by 53%
- Online and especially the mobile channel experienced dramatic increases in reported fraud as businesses across the world shifted to digital distribution, with one in three experiencing an increase of 50% or more in digital migration since the pandemic began among participating surveyed companies
- Businesses are forecasting surges in fraud in 2021
- Identity verification is now the number one challenge for businesses in addressing fraud
- Businesses are increasingly weighting the balance of fraud and friction towards optimizing and easing the customer experience
- To mitigate fraud risk and remove customer friction, businesses report best practices of omni-identity verification with data source diversity and multiple layers of attributes with international reach
- Synthetic identity fraud grows in prevalence and concern to an all-time high
- Businesses view the mobile channel as especially vulnerable in the near term with virtually all types of mobile fraud surging

History & Purpose

Now in its eighth year, IDology's annual Fraud Report measures fraud trends across a variety of industries in order to better understand the identity and fraud landscape, identify emerging trends, and offer insight for businesses.

Methodology

The survey was fielded September 16 – October 23, 2020 resulting in 314 business and fraud respondents across multiple industries including financial services, healthcare, insurance and e-commerce. Position titles of respondents include senior leadership, vice presidents, directors, managers and analysts in risk, fraud, compliance, product and operations departments.

Letter from the CEO

Now that 2020 is behind us, we're exceptionally pleased to publish IDology's Eighth Annual Fraud Report. With input from over 300 fraud executives across industries, several supplemental consumer studies, and IDology system transactional data, our goal is to provide companies with the information they need to focus their efforts during the coming year and beyond.

Without doubt, digitization provided many people, communities, and companies with a lifeline last year and will continue to do so this year. In the lead up to the pandemic, it is worth noting how the buildup of digital transformation created the infrastructure for near real-time, wholesale change. Effective digital identity verification (IDV) played a critical role in facilitating the opening of new accounts and delivery of services to help people and organizations across the world survive and thrive in a trying environment. That's why, for the first time, digital identity verification became the most daunting challenge to fraud deterrence across industries in 2021.

As you'll read, identity verification presents an opportunity for businesses to set themselves apart from their competitors. Locating and approving more legitimate customers without friction boosts revenue while offering a smooth, seamless onboarding user experience. It also allows businesses to develop competitive differentiators.

Nonetheless, businesses cannot expect yesterday's online processes and technology to satisfy today's consumers. If customers must use an online channel, they want the interaction to be secure, smooth and friction-free, and they are willing to end a relationship if a company fails to deliver.

A modern, comprehensive and multi-layered verification approach that balances the need for safety and security with the customer's expectation of a smooth process plays a critical role in delivering the experience customers demand. In fact, we're already seeing changes in consumer expectations that hold business accountable to a far higher standard. Companies that struggle to deliver an exceptional online customer experience can expect increases in abandonment rates. And since many businesses expect a surge in fraud in 2021, ineffective technology will open the door to fraud and reputational risk.

In a similar vein, while customers welcome digitization, a growing number expect companies to do much more to protect their personal data. Thankfully, when companies invest in security that does not interfere with interaction, customers award them with their business. As companies continue to reinvent their business models, it's time to take stock and invest in identity verification to secure every digital channel.

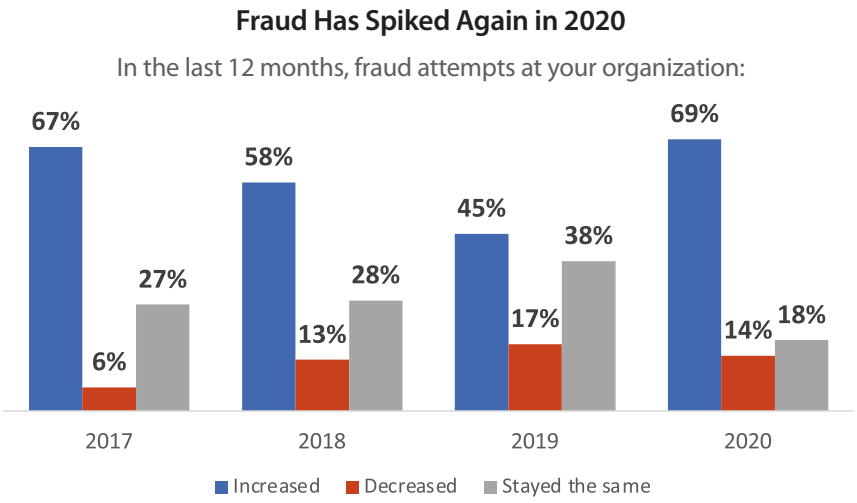
While life remains trying, we're optimistic that identity verification will play a critical role in minimizing fraud and helping millions join and become accustomed to the benefits of the digital economy. Why are we so hopeful? In 2020, we saw innovation result in the development of pandemic vaccines in record-breaking fashion. Simultaneously, millions of Americans flocked online, with many embracing the need for robust cyber-self-security.

Chris Luttrell
CEO

In the face of previously unimaginable changes in how society functions, businesses didn't lose sight of the challenges they face, with many increasing their fraud-related budgets and seeking out new innovations and technologies to fight fraud. We also saw greater participation in consortium networks that share intelligence and the continued march toward the internationalizing of integrated identity verification.

So, while 2020 is a year most of us would rather forget, there's a lot to be thankful for as we prepare for a new, and hopefully, less traumatic year ahead.

Surging Fraud During the Pandemic: Online and Mobile Bear the Brunt



Source: Eighth Annual Fraud Report, IDology, 2021

Fraud attempts spiked significantly in 2020. Sixty-nine percent of companies reported an increase in year over year fraud attempts, which is an increase of 53% compared to the prior year. Only 14% reported a decrease in fraud attempts, while 18% reported that it stayed the same.

Fraudsters came out in force during the pandemic to exploit opportunities from CARES to phishing, pandemic-related fraud, PPP, mass WFH deployments, decentralized fraud teams, nation-state attacks, civic discourse, fear and confusion. The pandemic was a historical fraud event, and the data shows criminals showed up.

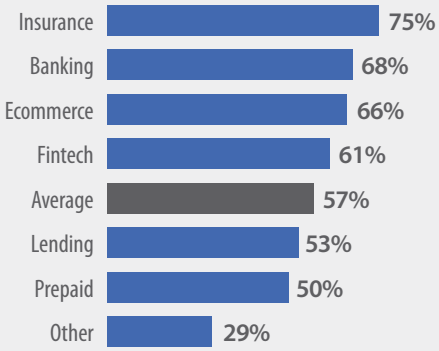
56M Americans have had a new account (e.g. bank account, credit card) opened in the past 12 months without their authorizaton

Source: Third Annual Consumer Digital Identity Study, IDology, 2020

77M million American adults have been the victim of identity fraud

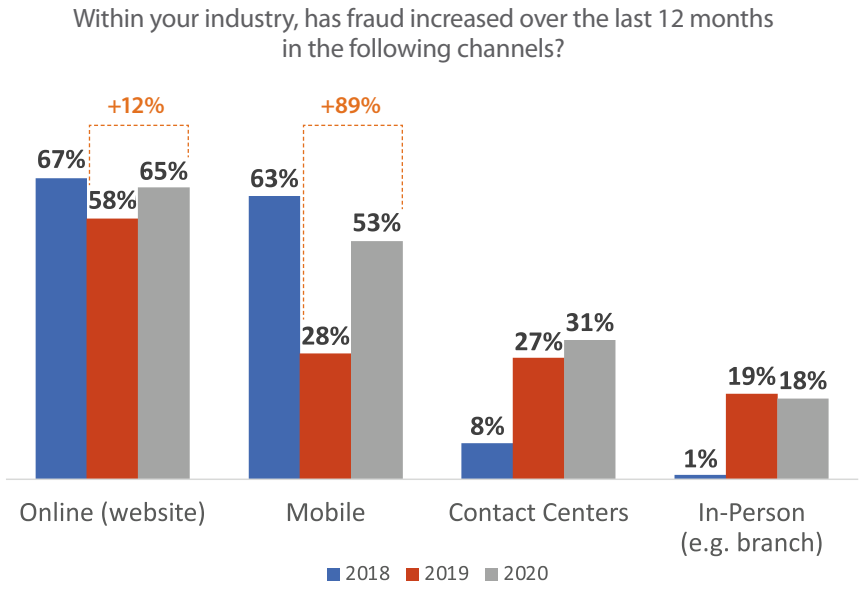
Source: Third Annual Consumer Digital Identity Study, IDology, 2020

Percent of Companies Per Industry Reporting Increases in Fraud Attempts Compared to Prior Year



Source: Eighth Annual Fraud Report, IDology, 2021

Increases in Fraud Primarily Felt Within Website and Mobile Channels



Source: Eighth Annual Fraud Report, IDology, 2021

Online and mobile experienced the largest increases, with 65% of companies reporting increases in fraud attempts via their website. Fifty-three percent reported increases in attacks via mobile. That represents marked increases over the previous year. In 2019, 58% of those surveyed reported increases in attacks via their website. However, the largest increase took place in the mobile channel, with those reporting year over year increases in attacks rising from 28% in 2019 to 53% in 2020. Attacks via contact centers and in person or branch operations remaining almost unchanged from 2019.

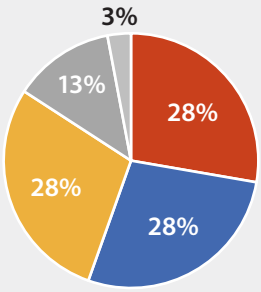
With consumers confined to their homes and forced to venture online, it stands to reason that companies saw dramatic increases in online and mobile transactions. Nonetheless, just as regular individuals themselves used online and mobile at greater scale to conduct business and interactions, criminals used those same channels to commit fraud.

The more a business embraces digitization, the broader the risk surface and ultimately, the more they'll attract cyber-based criminals and organized crime from across the world. Fast overhaul of business models and dramatic technology transformation inevitably has learning curves and mistakes that create and expose vulnerabilities. It's also important to note that technology "newbies" and the less than technically proficient were forced to go online as offline outlets for services such as groceries became literally life threatening.

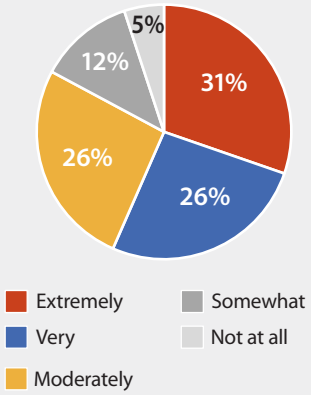
This introduced a new type of customer, many with thin credit files. Consequently, locating and onboarding became more important than ever. At the risk of losing those consumers to convoluted or confusing processes, companies needed to make it even easier to create an online account and conduct transactions.

Americans' Concern About Fraud Remains High

How concerned are you that your personal information could be exposed due to a data breach?

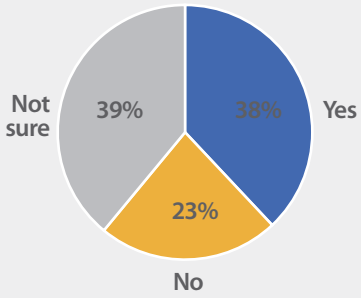


How concerned are you that your personal information could be used by a criminal to open a new financial account?



Source: Third Annual Consumer Digital Identity Study, IDology, 2020

Do you believe your personal information (such as name, SSN, and/or bank account number) is currently available for sale to criminals on the internet?

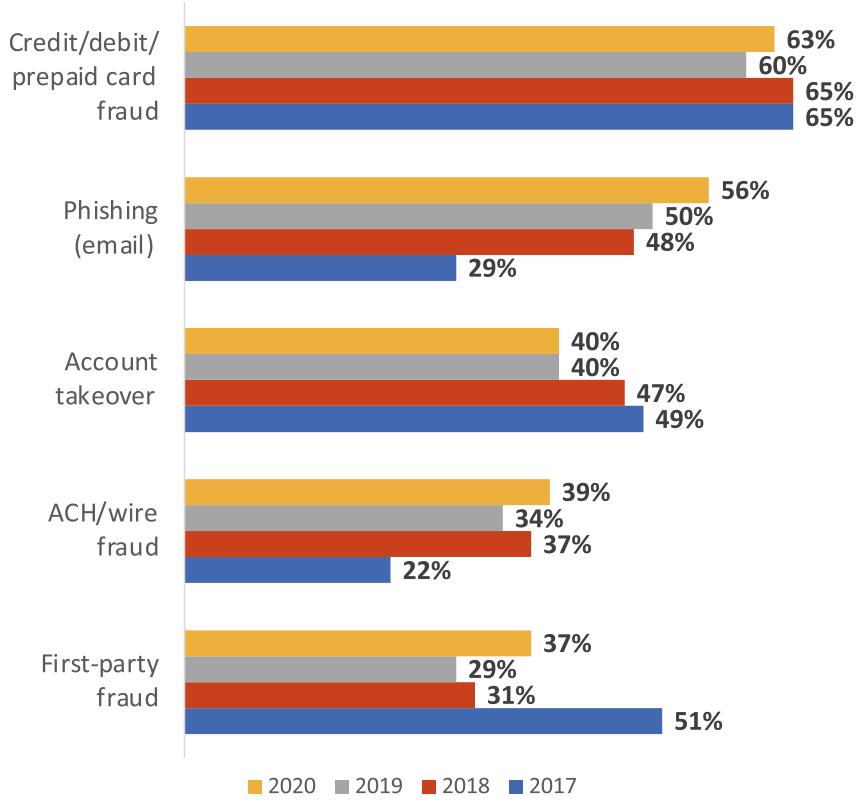


Source: Third Annual Consumer Digital Identity Study, IDology, 2020

Vectors and Schemes Where Fraud is Thriving

Most Popular Fraud Vectors

What types of fraud vectors or schemes do you think are most prevalent in your industry? (select all that apply)



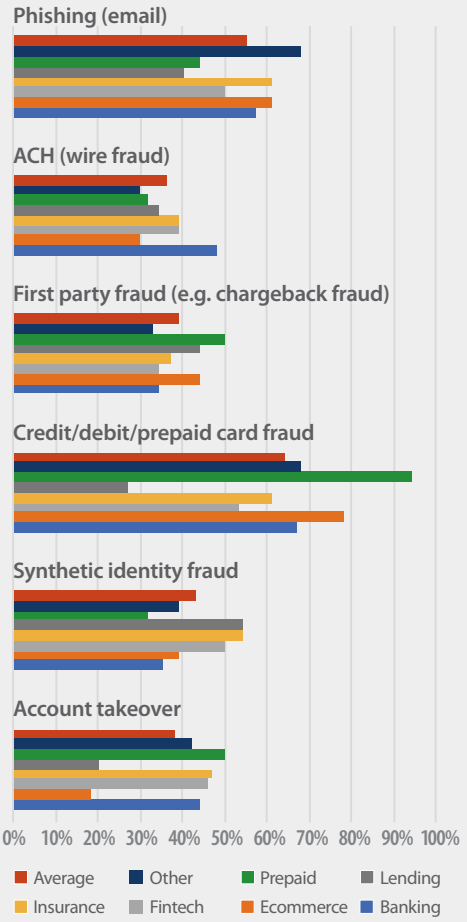
Source: Eighth Annual Fraud Report, IDology, 2021

Although fraud attempts and the operating environment have changed substantially, the established choice of fraud vector and technique types remain relatively stable, though with notable increases in prevalence. We did see a modest increase in the leading category of card funded fraud. Phishing, the most significant cause of and commonality among the most large-scale breaches, continued its surging growth as more consumers were targeted in 2020. In fact, in our previous research report, The COVID-19 Effect on Identity, Onboarding and Fraud, we determined that 84 million Americans received a phishing attempt during the pandemic, with a majority receiving three or more attempts.

ACH/wire fraud spiked by 15%, presumably due to rising P2P usage due to social distancing. First-party fraud saw a significant increase of 28%. This may be attributable to familiar fraud and chargeback fraud as many Americans were unemployed, underemployed, or suffering in shape or form financially in 2020, thereby increasing their pressure and rationalization of committing fraud.

Fraud Prevalence by Industry

What type/s of fraud vectors and schemes do you think are most prevalent in your industry? (select all that apply)



Source: Eighth Annual Fraud Report, IDology, 2021

Americans are fighting back!

Between March 2020 and July 2020

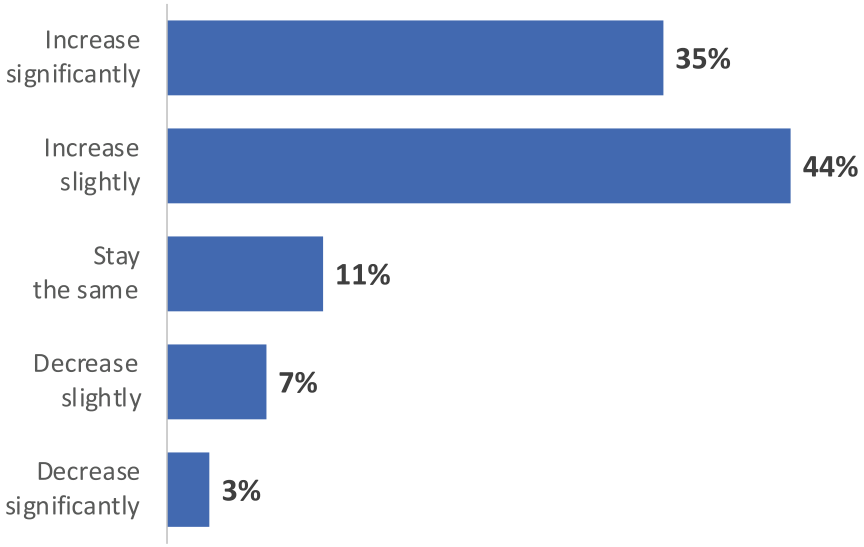
35M

online Americans have taken action to improve online identity credentials

Source: The COVID Effect on Fraud, Trust and Onboarding, IDology, 2020

Most Businesses Expect Fraud to Grow Next Year, More Than One-Third Significantly

How do you expect the level of fraud to change over the next year?



Source: Eighth Annual Fraud Report, IDology, 2021

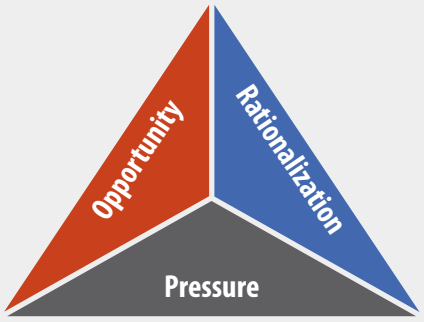
So, what does the move to digital, fresh collection of more Personally Identifiable Information (PII) from 2020, and potential economic conditions mean for fraud rates in the next 12 months? Most businesses anticipate some degree of increase, with 35% predicting a significant increase, while 44% envision a minor increase. Only 11% see it remaining the same, while an optimistic 10% see the potential for decreases in fraud. This is notable given these business fraud executives reported a four-year high in year over year fraud attempts, as mentioned previously.

Interestingly, these forecasts align with findings from a 2009 study conducted by the Association of Certified Fraud Examiners (ACFE). In that study, a year after the great recession, the ACFE asked 500 Certified Fraud Examiners to share their expectations of fraud in the following year. The answers are eerily close to the responses captured in our survey. Thirty-seven percent of CFEs expected fraud to increase significantly in 2010, while 51% predicted that it would increase somewhat.

Understanding Fraud's Why

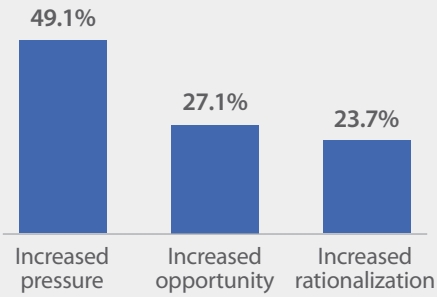
Fraud Triangle: Why People Commit Fraud

The Fraud Triangle



Source: Dr. Donald Cressey

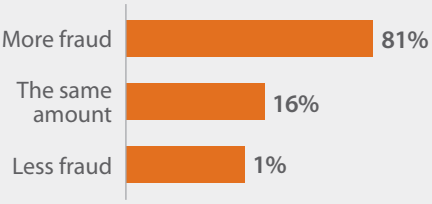
Biggest Factors Contributing to Increases in Fraud During Last Recession According to Certified Fraud Examiners



Source: Occupational Fraud: A Study of the Impact of an Economic Recession, ACFE, 2009

Fraud During Downtimes Compared to Stable Times

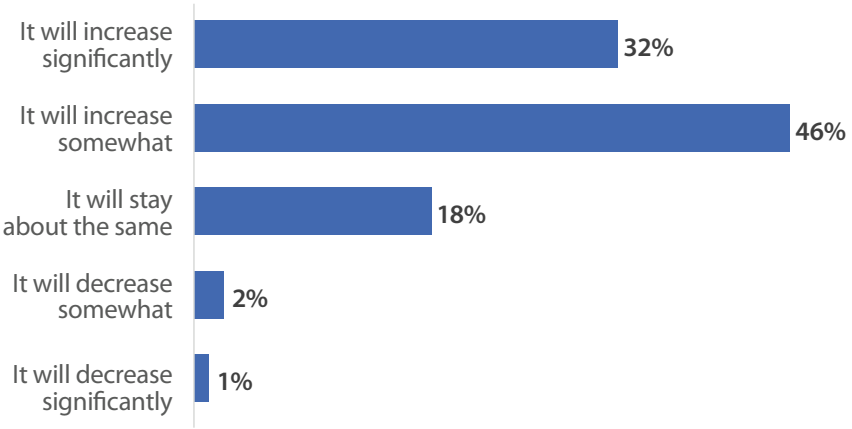
N = 507 certified fraud examiners



Source: Occupational Fraud: A Study of the Impact of an Economic Recession, ACFE, 2009

Majority Forecast Budgets to Increase Next Year

How do you expect spending and investment on fraud deterrence to change over the next year?



Source: Eighth Annual Fraud Report, IDology, 2021

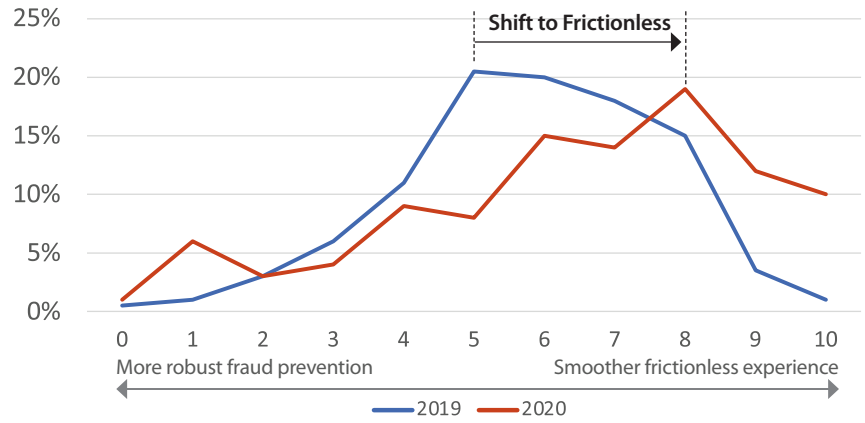
Since businesses expect fraud to increase, they also anticipate spending and investment to rise, interestingly, at nearly the exact same amount as expected fraud. Seventy-eight percent expect increases, with 32% believing it will increase significantly.

With an escalation in fraud on the horizon, when asked to identify the fraud prevention strategies under consideration, survey participants shared a growing interest in fraud mitigation solutions for mobile account verification (53%), Geo and IP intelligence (45%), mobile ID scanning (44%), email verification (43%), and AI (40%)

Fraud, Friction, and the Customer Experience

Businesses Increasingly Weighting the Balance of Fraud and Friction Towards Optimizing the Customer Experience

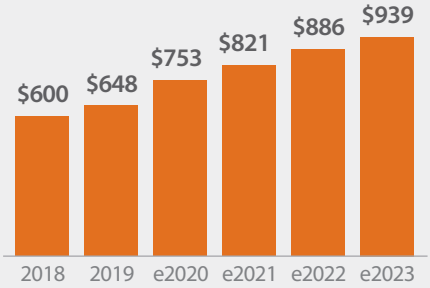
In balancing fraud prevention with customer friction, where would you weight your organization's position, with robust fraud prevention being a 1 and a frictionless customer experience being a 10?



Source: Eighth Annual Fraud Report, IDology, 2021

Estimated and Projected U.S. FI's DDA Application Fraud Losses

DDA Application Fraud Losses (in US$ millions)



Source: Aite Group

Nearly **2/3** of Americans **think companies don't do enough** to safeguard their personal identity information

Source: Third Annual Consumer Digital Identity Study, IDology, 2020

77% of Americans **are less likely to do business** where a new account was fraudulently opened in their name

Source: Third Annual Consumer Digital Identity Study, IDology, 2020

72% of Americans say the most important thing when opening a new online account is that **the process is secure.**

Source: Third Annual Consumer Digital Identity Study, IDology, 2020

There's always been a need to balance fraud with customer friction. Businesses drive revenue by greenlighting customers, which includes removing barriers and minimizing effort during the onboarding process to avoid unnecessary "friction". Yet, they must do so while deterring fraud.

Every firm and a majority of consumers want the new account opening experience to feel safe. This is where the challenge arises. The more steps to verify a new account and make the experience safer, the more friction customers experience, which leads to account abandonment. In fact, the fear of customers walking away from overly challenging processes is well founded. According to IDology's Consumer Fraud Report, in 2020 48% of online Americans reported abandoning signing up for a new account because it was too time consuming or did not seem trustworthy, up from 37% the year before.

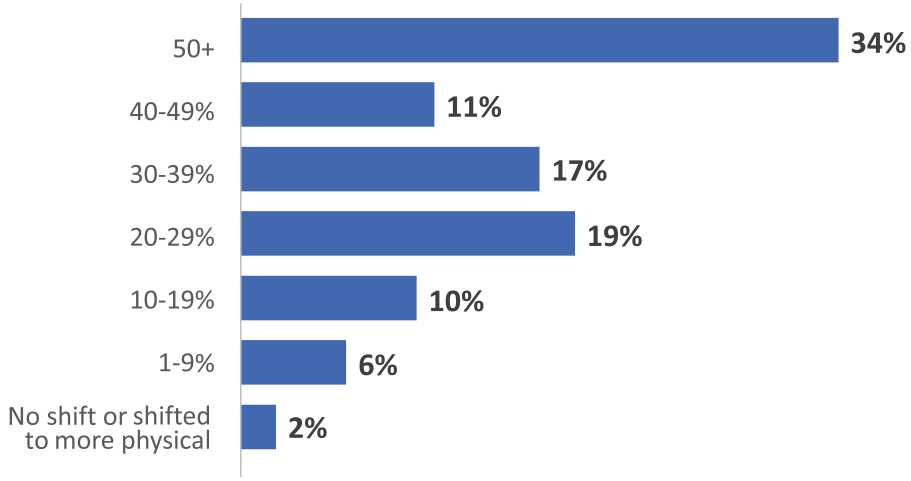
Hence the need for a delicate balancing act. Consumers overwhelmingly say that security (68%) is the most important part of the new account opening process but then nearly half (48%) say that they "strongly dislike" additional steps in the identity verification process to improve security.

In today's environment, it appears that companies are leaning towards removing friction, even at the possible expense of fraud losses compared to last year. The weighted average of respondents' position on the fraud-frictionless continuum in 2019 was 5.8. In 2020 the weighed average was 6.5, a 12% shift towards frictionless customer experience. While attempting to make their services more accessible, especially to tech newbies, or for business viability and competitive reasons, there's still a struggle taking place. When asked to rate their effectiveness in striking the balance, about half of businesses feel their companies are average or less at both deterring fraud and delivering frictionless customer experiences.

Historical Digitization Change Accelerator Event. Customers and Businesses Benefit, but So Do Fraudsters.

The Pandemic Has Caused Massive Shifts to Digital Channels

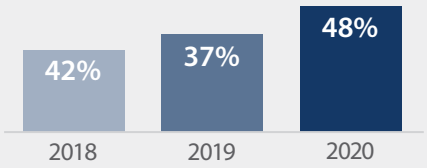
How much of your business has shifted to digital channels since the start of the COVID-19 pandemic (March 2020)?



Source: Eighth Annual Fraud Report, IDology, 2021

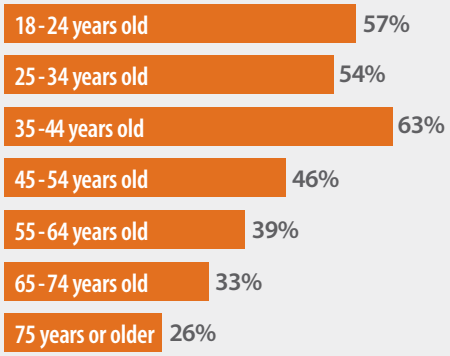
More consumers are abandoning the new account set up process because it's either too difficult, takes too long or is not trustworthy

Percentage of online American adults who have abandoned signing up for a new online account in the last 12 months



Source: Third Annual Consumer Digital Identity Study, IDology, 2020

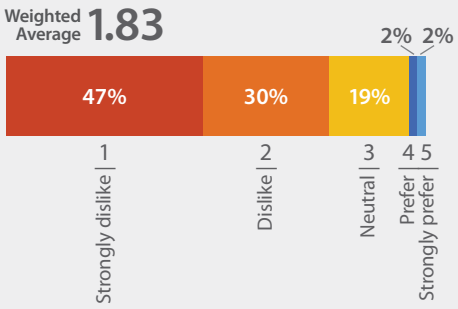
Online U.S. adults who have abandoned signing up for a new online account because the process was too difficult, too time consuming, or did not seem trustworthy, by age



Source: Third Annual Consumer Digital Identity Study, IDology, 2020

Consumers Dislike IDV Friction

Indicate your preference for requiring additional steps during identity verification (1=Strongly dislike and 5=Strongly prefer)



Source: Third Annual Consumer Digital Identity Study, IDology, 2020

The pandemic led to a historical acceleration of digital adoption. According to IDology's report, The COVID-19 Effect on Identity, Onboarding and Fraud, 93 million American adults have activated services that were once done in person prior to the pandemic. Of those who switched to digital from physical, 75% said they have made the switch for good, for most or all the services.

When asked how much of the business now operates in digital channels since the appearance of COVID-19, a staggering 34% of companies surveyed reported that 50% or more of their business was digital. In fact, only 2% reported no shift to digital or a shift to physical.

The remaining 63% reported varying rates of digital adoption, ranging from 6% reporting the movement of 1% to 9% to the digital realm, 10% reporting that 10% to 19% moved to digital. A further 19% reported the transition of 20% to 29%, while 17% reported 30% to 29% as now digital. Finally, 11% reported the movement of 40% to 49% to digital.

Note: Companies asked to participate in the survey must maintain online operations. Companies that operate primarily offline and smaller "mom and pop" businesses were not included in this survey. This resulted in more companies reporting the existence of digital channels than is the case for all companies in the United States.

A digital first strategy, which is critical in today's environment, creates more efficiencies but also more digital vulnerabilities. In 2020, there was immense growth in the amount of compromised PII, usernames and passwords to exploit. That trend will continue in 2021. And while the volume of new account openings results in financial growth, it also results in fraud. This includes the deployment of breached data that has been collected, organized and packaged, and criminals will operationalize in 2021 and prime for "bust-outs" this year that were incubated last year. And we cannot overlook the growing threat of fraud associated with synthetic identities that become more potent the longer they age.

The changes in the operating environment have already triggered significant changes to digital identity and fraud signal data that companies like ours use to evaluate and decision. Since March, we have observed surges in the volume of alerts around age attributes, mobile change events, and other indicators which are either indicative of fraud, or simply jarring shifts in behavioral and demographic trends. For example, there are more seniors opening online accounts to have groceries delivered. That also means there are more seniors and their identities being targeted by fraudsters.

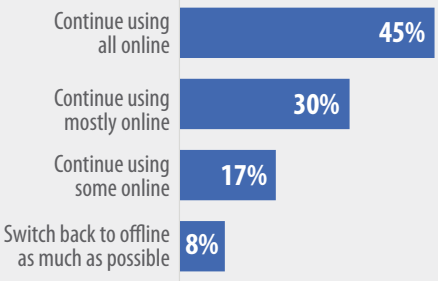
Let's not forget the fraud triangle, which states that opportunity, pressure, and rationalization must exist for internal fraud to happen. If we apply that model to the COVID economy and third-party fraud, it's easy to envision why 2021 might result in record-breaking losses.

Historic levels of digital conversion and permanence

Between March 2020 and July 2020

37M

American adults have signed up for online services that were once done in person



Source: The COVID Effect on Fraud, Trust and Onboarding, IDology, 2020

Between March 2020 and July 2020

142M

Americans have started using contactless payments...

...and

76M

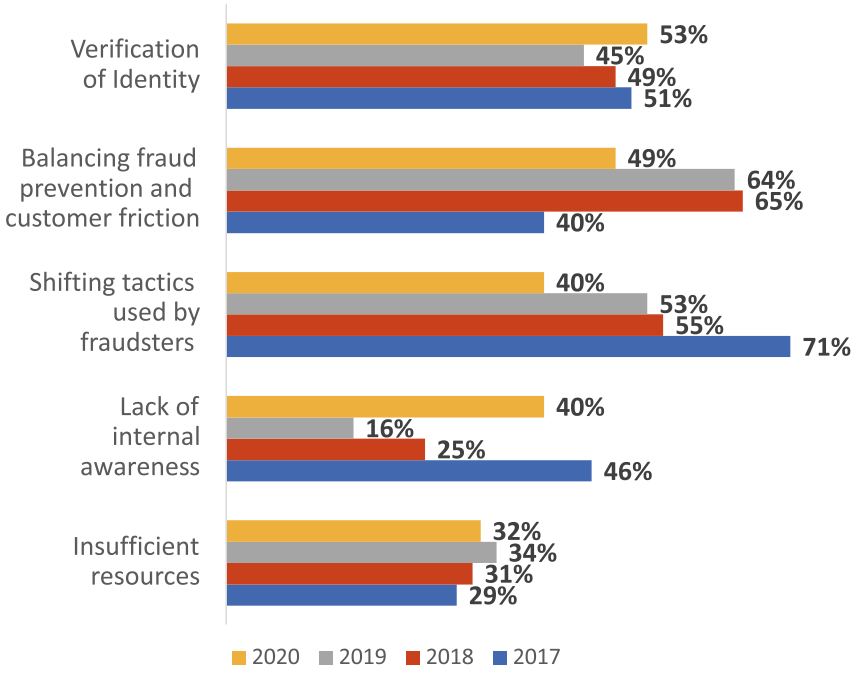
Americans have signed up for P2P services

Source: The COVID Effect on Fraud, Trust and Onboarding, IDology, 2020

Passing the Tipping Point: Identity Verification is Now the Top Cross-Industry Fraud Challenge

For the First Time Verification of Identities is the Biggest Challenge to Fraud Deterrence

What do you think are the biggest challenges to fraud deterrence within your industry? (select all that apply) - Selected Choice



Source: Eighth Annual Fraud Report, IDology, 2021

One of the most significant findings from the 2020 survey is the emergence of identity verification (IDV) as the biggest challenge to combating fraud. Fifty-three percent of those surveyed viewed verification of identities as their biggest challenge. That's an increase of 8% from 2019.

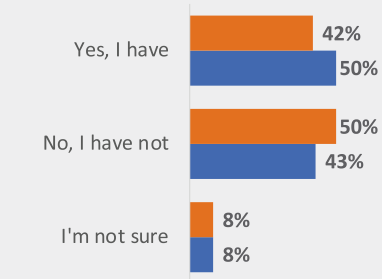
Interestingly, balancing fraud prevention and customer friction is slightly less of a concern than verification, with 49% identifying this as a challenge, down from 64% in the prior year. This does not mean that companies have resolved this challenge. Instead, it means that it is on their radar and something they consider as they evolve their approach to fraud detection and prevention. Lack of internal awareness saw a significant increase from just 16% in 2019, to 40% in 2020.

Shifting tactics is an interesting data point and has declined as one of the biggest challenges. This suggests that while fraud attacks are increasing and fraudsters adapt, organize and innovate, the tactics they use are relatively unchanged. The tried-and-true approaches, such as phishing, mobile compromise, new account fraud, account takeover, card-based

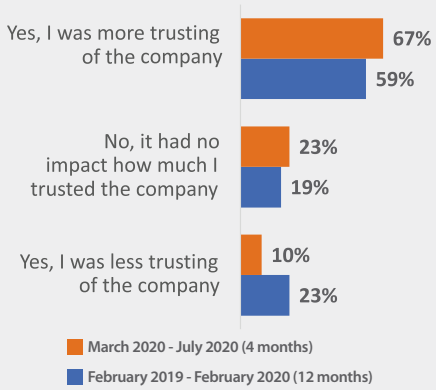
Evolving identity Verification Methods

62% who were required to provide further proof of identity did so by mobile ID document scan between March and early July, compared to **57%** in the **12 months leading up to COVID.**

Have you been required to provide further proof of your identity while signing up for a new online account or using an existing online account?



Did the requirement to provide further proof of your identity impact your ability to trust the company?



Source: The COVID Effect on Fraud, Trust and Onboarding, IDology, 2020

fraud, synthetic identities, and usage of mules continue to deliver results, so the fraud innovation is focused on upgrading and enhancing the potency of these methods. So, while fraudsters continue to refine their techniques, businesses do not see wholesale shifts to new methods. Instead, the volume of attacks continues to grow, with tweaks and revisions to overcome countermeasures – the proverbial cat and mouse, whack-a-mole dynamic remains in full effect.

With so many challenges to consider, what is the end customer's perspective on identity verification? Given its historical back office existence, which became part of the user experience relatively recently through the use of more prominent methods such as two-factor authentication, does identity verification matter to consumers? Our Third Annual Consumer Digital ID study determined that if a consumer knew that a financial services provider was using particularly more advanced identity verification methods, that fact would impact their decision and preference for a company that adopted that approach. In fact, 77% said that the use of a robust solution would influence their decision-making process, though what survey participants say they do in comparison to their actual behaviors can vary.

With this data point in mind, when we asked whether identity verification can be a strategic differentiator, 86% of businesses said yes, 4% said No, with 10% saying I don't know. Identity verification is also changing rapidly, with 65% believing it has become more complicated and complex over the last three years.

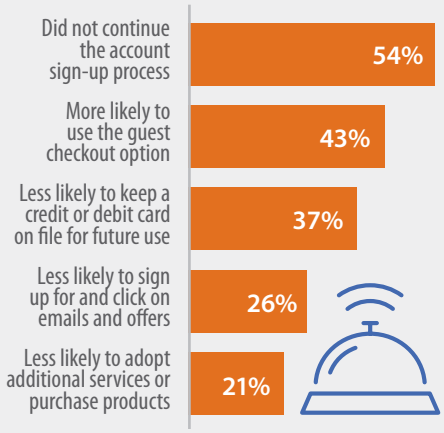
Our data also reinforces the value of identity verification in the consumer's mind and the consequences of weak verification downstream. Among online Americans, 77% say an unauthorized account being opened in their name would impact their likelihood to patronize or do business with that company. Furthermore, when Americans don't trust the digital identity verification process, they are more likely to use guest checkout (54%) and less likely to keep a payment card on file (43%), thereby creating a drag on profits while compromising the end-user's experience.

Mobile and Synthetic Fraud Concern at All Time High

Over the last 3 years, the two fraud vectors that have firms most concerned are mobile-related fraud and synthetic identity fraud. In this year's report, the trend continues and is more acute than ever. In fact, changes brought about by the pandemic amplify their potency. Americans have turned to their mobile devices even more so during the pandemic to open new accounts.

Synthetic identity fraud continues to trouble businesses, especially given the challenges associated with decentralized WFH fraud teams, and the need to interpret and apply once in lifetime changes in consumer behavior and the swings and noise they create. Not to mention the problems created by the never-ending stream of data breaches, and the use of personally identifiable information gathered from phishing attempts and other scams that continue to thrive in the COVID era.

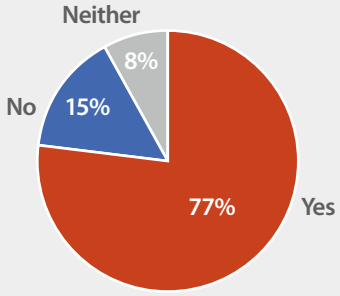
When Americans don't trust the digital identity verification process they are more likely to use guest checkout and less likely to keep a payment card on file



Source: Third Annual Consumer Digital Identity Study, IDology, 2020

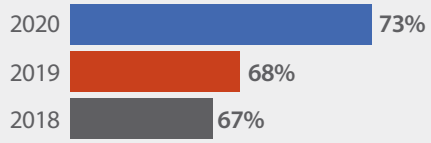
The Hidden Cost When Identity Verification Fails

Would an unauthorized account being opened impact your likelihood to patronize or do business with that company?



Source: Third Annual Consumer Digital Identity Study, IDology, 2020

Americans increasingly feel very strongly that it's a company's responsibility to protect their opersonal information...



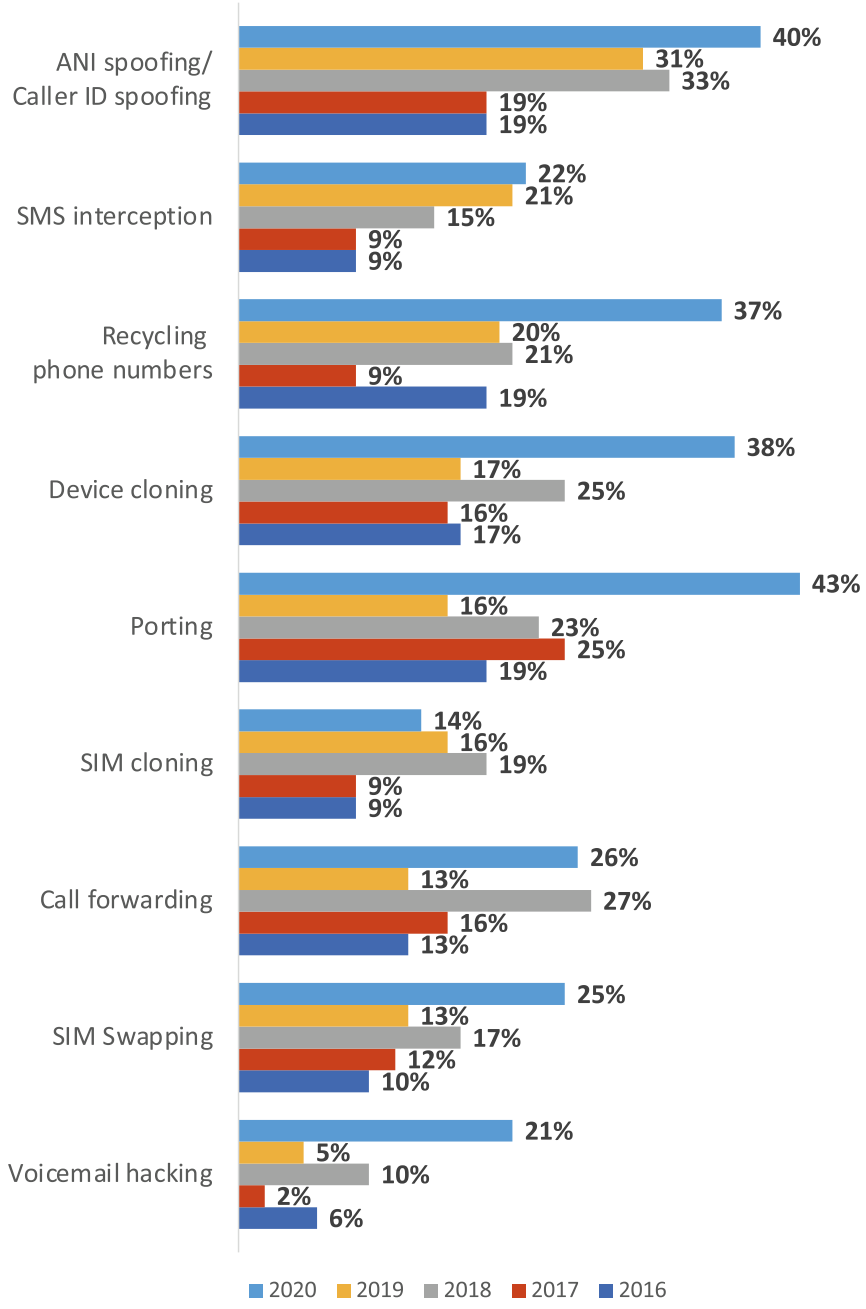
...and want companies to do more to protect it

Source: Third Annual Consumer Digital Identity Study, IDology, 2020

Mobile Fraud Surges Across Type

Mobile Fraud Techniques Spiking Across the Board

What types of mobile-based fraud techniques do you think are most prevalent within your industry? (select all that apply)



Source: Eighth Annual Fraud Report, IDology, 2021

As stated earlier, this year's study showed that mobile fraud attempts surged by 89% compared to the prior year. Mobile fraud encompasses a myriad of fraud techniques. Evaluating the prevalence of techniques used by fraudsters helps identify where potential weaknesses exist.

A surge in mobile phone usage

Between March and July of 20200

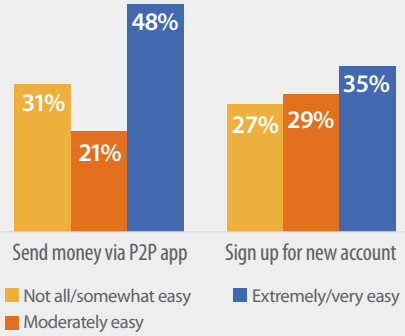
49%

of online Americans have used their smartphone more often to apply for new accounts

Source: Third Annual Consumer Digital Identity Study, IDology, 2020

Is Mobile Commerce Easy Enough?

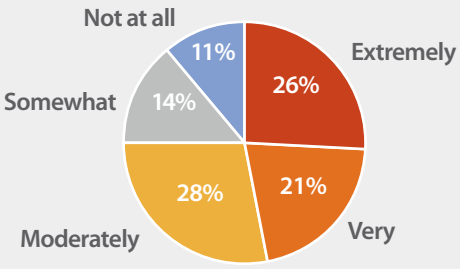
How easy is to do the following on your mobile device?



Source: Third Annual Consumer Digital Identity Study, IDology, 2020

Mobile Malware Troubles Americans

How concerned are you about the risk of malware on your smartphone?



Source: Third Annual Consumer Digital Identity Study, IDology, 2020

This year's survey found that mobile fraud activity occurred via many proven paths. The biggest surges occurred in porting, followed by device cloning and recycling of phone numbers, while ANI spoofing remains high. IDology mobile data also found surges in these categories.

A note of caution: there may be some noise in the data, as consumers may go through more mobile change events due to service shutoffs or switching to other plans during the pandemic economy of 2020.

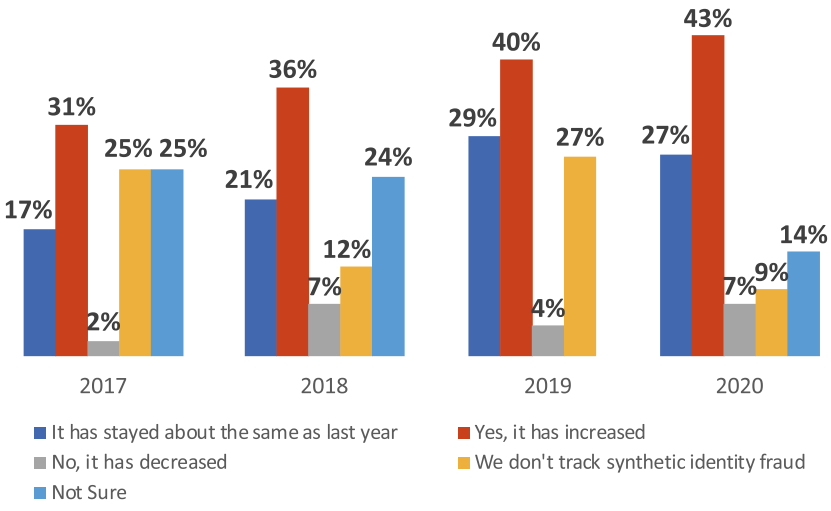
According to IDology's research, seventy-three percent of connected Americans that signed up for a new account online since the pandemic did so via mobile. Concerns regarding mobile fraud make sense, given the number of new online accounts opened since March 2020, which we estimate at 98 million. Of those accounts newly opened, our COVID Effect study found that consumers used mobile phones to open 73% of the newly created accounts. Computers opened 63%, while tablets opened 23%.

With mobile-based fraud identified as the most impactful, respondents reported significant increases in mobile fraud techniques. ANI spoofing / caller ID spoofing, recycling phone numbers, device cloning, and porting recorded significant increases. For example, porting soared from 16% in 2019 to 43% in 2020. Device cloning increased from 17% to 38%, and recycling numbers jumped from 20% in 2019 to 37% in 2020.

Synthetic Identity Fraud

Synthetic Identity Fraud Continues to Climb

Have you noticed an increase in synthetic identity fraud at your organization over the last 12 months?

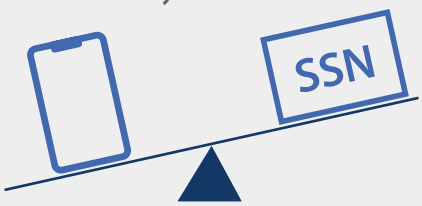


Source: Eighth Annual Fraud Report, IDology, 2021

We've talked about the growing threat of synthetic fraud, which involves the use of disparate identity attributes to manufacture identities, build histories, and exploit credit bureau data as difficult to identify and defend against for many years. Since 2017, we've noted increases in synthetic fraud. Our 2020 survey is no different, with 43% reporting increases in synthetic fraud, up from 40% in 2019, 36% in 2018, and 31% in 2017.

35M

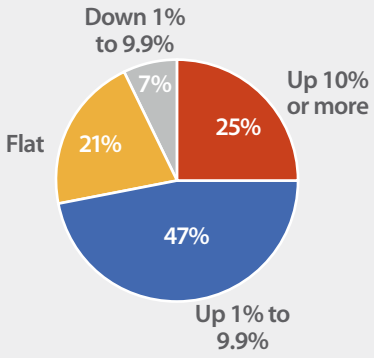
American adults would be more concerned if their mobile phone and phone number were compromised compared to their Social Security Number.



Source: Third Annual Consumer Digital Identity Study, IDology, 2020

Rate of Increase in Synthetic Identity Fraud Since the Start of the Pandemic

Trends in Synthetic Identity Fraud (n=28)



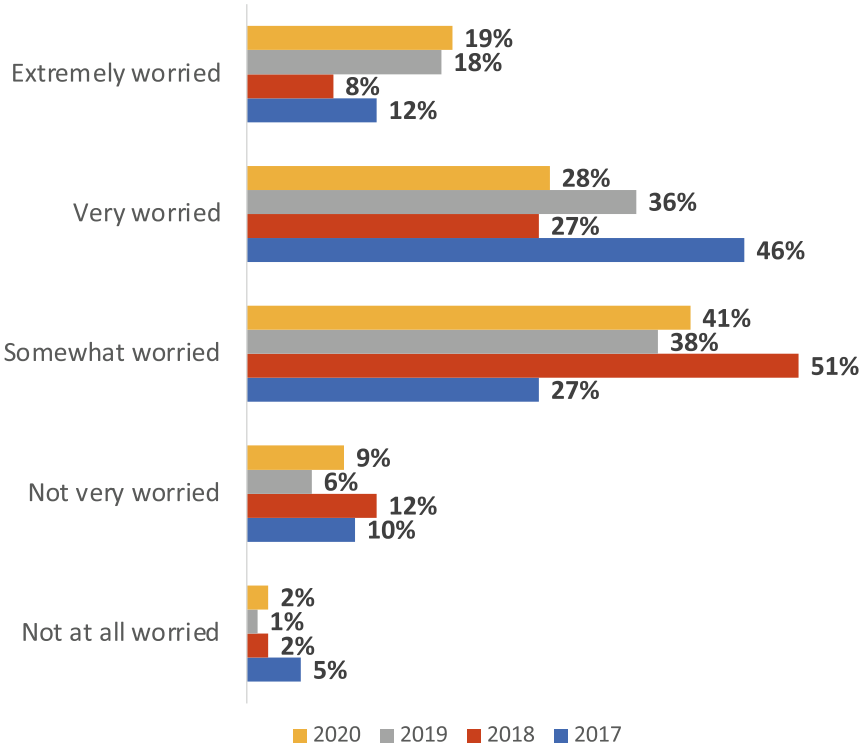
Source: Aite Group's survey of 47 financial services fraud executives, September 2020

Financial institutions experience **$50-$250MM in financial losses each year** due to SIF, with estimated YoY growth of 10-15% from 2011 through 2016 and approximately $1B in credit card losses across all financial institutions in 2016

Source: U.S. Government Accountability Office Forum, Panelists input

Concern About Synthetic Identities Continues to Grow

How concerned are you about synthetic identity fraud?



Source: Eighth Annual Fraud Report, IDology, 2021

When asked about the depth of their concerns regarding synthetic fraud, almost half of those surveyed reported that they were extremely or very concerned. Forty-one percent were somewhat concerned, with the remainder were not worried.

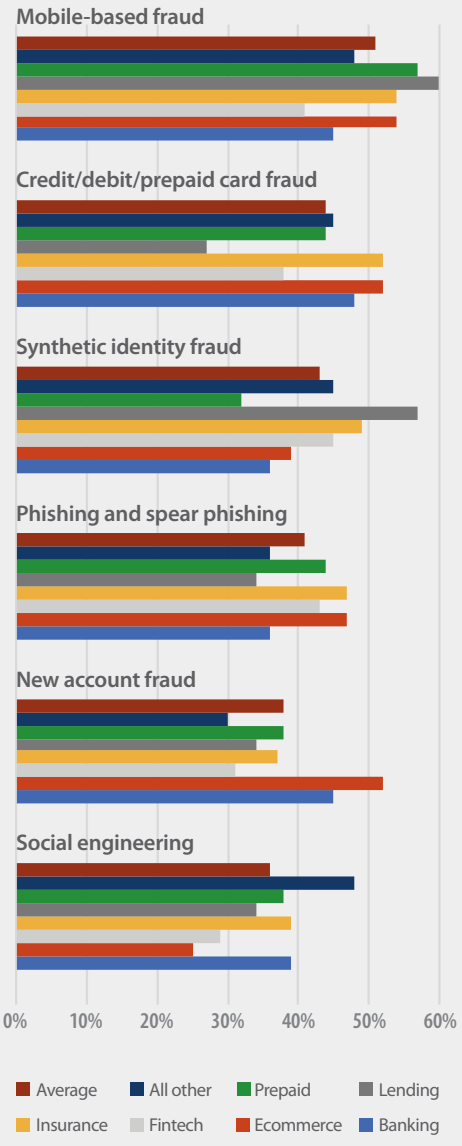
While history is not the only factor to consider with respect to how the environment might change in the next couple of years, this survey and our experience tells us that synthetic fraud deserves the national and federal attention it continues to receive and will likely be an even bigger concern this time next year.

How Leading Firms are Approaching Identity Verification and the Ongoing Struggle to Combat Fraud and Minimize Customer Friction

We dedicated a great deal of this report to understanding the depth and severity of the fraud problem facing businesses and consumers. We also took the time to focus on solutions.

Most Impactful Forms of Fraud by Industry in next 2-3 years

What do you foresee as being the most impactful type/s of fraud in the next two to three years? (select all that apply)

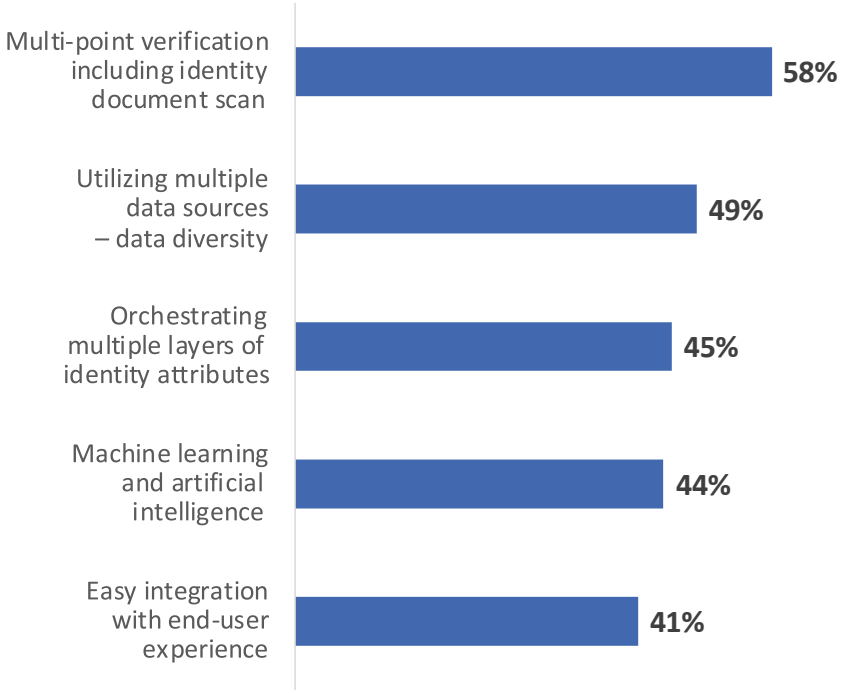


Source: Eighth Annual Fraud Report, IDology, 2021

We asked survey participants to shed some light on the top best practices for identity verification to locate, approve, and onboard legitimate customers with low friction while also deterring fraud and maintaining compliance.

Omni Identity Verification with Data Diversity and Multiple Layers Top Identity Verification Best Practices

Based on your experience and in your opinion, what are top best practices for identity verification to locate, approve, and onboard legitimate customers with low friction while deterring fraud and maintaining compliance? (select all that apply)



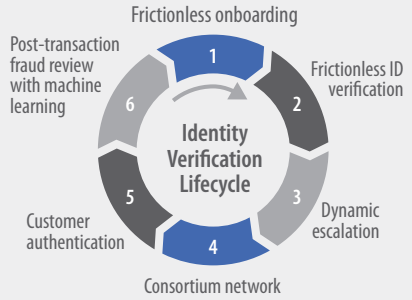
Source: Eighth Annual Fraud Report, IDology, 2021

Fifty-seven percent identified multi-point verification including incorporating methods such as identity document scan as important. Forty-eight percent selected data diversity as a best practice, while orchestration in the form of multiple layers of identity attributes was selected by 45%. Given the focus placed on machine learning and artificial intelligence, it's not surprising that 44% selected this as a best practice.

Deploying multiple levels of identity verification allows businesses to identify legitimate customers more accurately versus those intent on committing crime. It can also present additional methods of stepped-up verification dynamically, at the right time to the right customers.

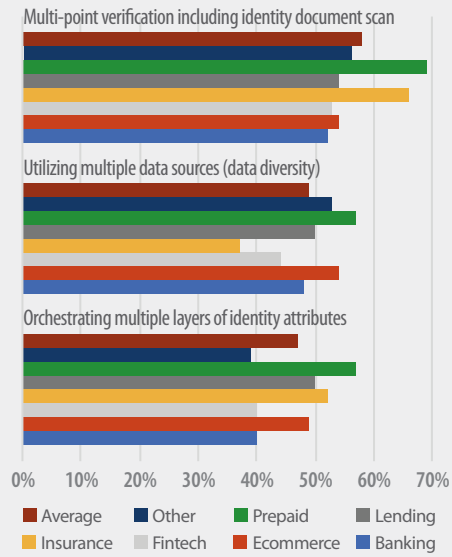
As fraudsters have added more sophistication to their schemes, adding additional layers or blankets of attributes offers scale and covers gaps. To function effectively, these layers need to speak to one another. Businesses need solutions that "orchestrate" multiple dynamic data sets and present seamless invisible experiences that are easy to explain and defend.

A Comprehensive Lifestyle



Source: Eighth Annual Fraud Report, IDology, 2021

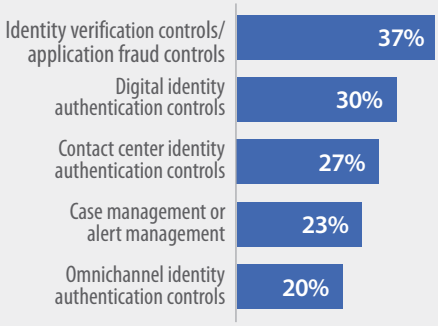
Top Three Best Practices for Identity Verification by Industry



Source: Eighth Annual Fraud Report, IDology, 2021

Areas of Investment Receiving the Most Funding

Which two areas are getting the most funding in terms of investment/transformation? (Select up to two; n=30)



Source: Aite Group

Layers should include consortium intelligence from other companies across other industries. Data diversity is also critical. An effective solution cannot use the same data pool for risk decisions as for identity verification for example, especially given the compromised nature of standalone pools based on one or few sources.

Artificial intelligence (AI) and machine learning (ML) technologies deliver a scalable approach that supports effective decisioning, assuming the solution receives access to relevant data to train.

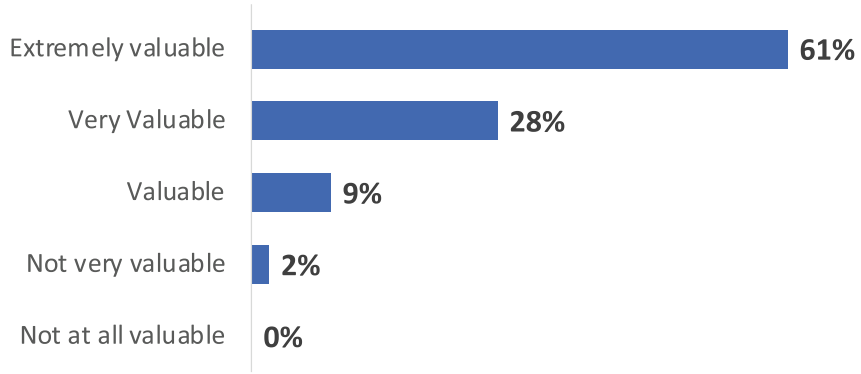
That said, AI and ML solutions trained using pre-pandemic behaviors may struggle to make sense of behaviors and data gathering during the COVID era. According to the survey, one in five respondents state they believe ML is much less effective to somewhat less effective in deterring fraud and reducing false positives. That's why an AI solution augmented with humans delivers a superior approach to detecting fraud patterns and the spotting of novel fraud techniques.

Finally, forty-one percent felt easy integration with the end-user experience merited consideration. According to the survey, 65% say identity verification has grown more complex and complicated over the last three years. Admittedly, IDV is complicated. Yet consumers want an easy, softer approach. At the same time, businesses want technology they can implement seamlessly, that supports a highly customizable and responsive approach, without the need to engage IT to make refinements and updates. From our perspective, IDV shouldn't get in the way, it should pave the way.

Streamline Managing Identities Cross Border

Among Companies with Multi-National Operations Singular Identity Verification Solutions are Highly Valued

How valuable would it be to verify customer identities, detect fraud, and meet compliance for multiple countries on one platform?
Among companies with



Base: Among multi-national businesses

Source: Eighth Annual Fraud Report, IDology, 2021

Internationally extending full digital ID coverage could unlock economic value equivalent to **3 to 13 percent of GDP** in 2030 depending on global region.

Source: Digital identification: A key to inclusive growth, McKinsey Global Institute (MGI), 2019

One billion people around the globe face challenges in proving who they are and struggle to access basic services such as financial services

Source: World Bank

"Providing a single platform that enables access to identity verification across multiple geographies enables companies to use it more easily and efficiently, and can save expense if a new implementation project can be avoided."

Shirley Inscoe, senior analyst for Aite Group.

Business is increasingly international and so is fraud, which knows no borders. Firms that have cross-border presences, or plan to venture into new international markets, need to access viable identity verification sources, deploy identity verification solutions that follow local regulations as well as comply with national compliance and privacy requirements. Given this we wanted to know the degree to which verifying identities, detecting fraud, and meeting compliance for multiple countries in one platform was of value to companies. A resounding 61% felt it would be extremely valuable, with an additional 28% viewing it as valuable.

Identity verification varies greatly by region and country creating complexity. For example, in Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) allows the collection and usage of personal information of commercial activities for economic transactions.

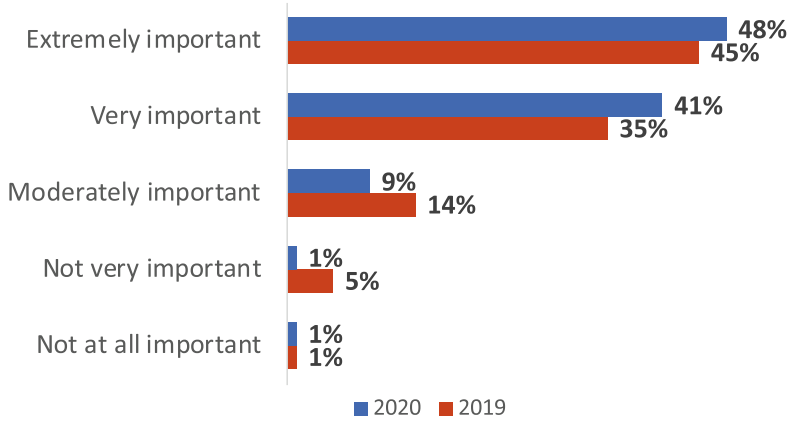
In France, the Data Protection Act (DPA) incorporates specific provisions while keeping in line with General Data Protection Regulation. Brazil's Lei Geral de Proteção de Dados, its version of the General Data Protection Law created the National Authority for the Protection of Data, comes with its own set of onerous requirements.

In Mexico, companies need to comply with regulations including the General Law for the Protection of Personal Data in the Possession of Obliged Subjects and the Privacy Notice Rules and Binding Self-Regulation Parameters.

With so many laws on the books and under development, businesses with international operations appear to highly value solutions that provide built-in regulatory compliance for every foreign market in which they maintain a presence.

Accurate Address Deliverability in Successfully Verifying Identities Growing in Importance

How important is accurate address validation to the identity verification process?



Source: Eighth Annual Fraud Report, IDology, 2021

Americans Prefer Businesses that Utilize Robust Identity Verification

77% say **better identity verification** influences their decision to use a company's services

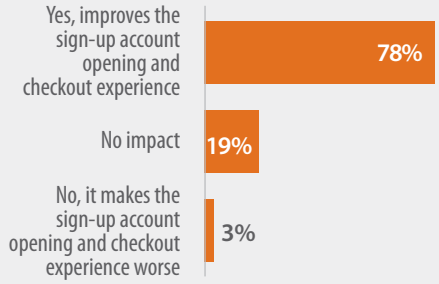
Source: Third Annual Consumer Digital Identity Study, IDology, 2020

Between March 2020 and July 2020

114M

American adults have signed up for an online service or purchased an item online that has an auto-complete address function on the checkout order form

Does auto-complete address verification improve the account opening or online checkout experience?



Source: The COVID-19 Effect on Fraud, Trust and Onboarding, IDology, 2020

Accurate address validation including postal deliverability as an identity verification attribute is also a growing hot button for companies, with 48% viewing such functionality as extremely important. Forty-one percent viewed it as very important. The remainder of 11% viewed it as less important.

Aside from the rise in home deliveries for essentials such as groceries in 2020, inaccurate address deliverability data collected from disparate public information sources during the new customer onboarding process adversely impacts an organization's ability to thoroughly verify the identity of a new customer. It also complicates the detection of potential fraud attempts and the ability to deliver products and necessary communications to customers via the mail.

Significant postage, processing and chargeback costs can result when address undeliverability data lacks accuracy and integrity. Also, when a customer's orders and critical communications can't be delivered, it degrades the customer service experience resulting in a decline in satisfaction and engagement, not to mention compliance risk.

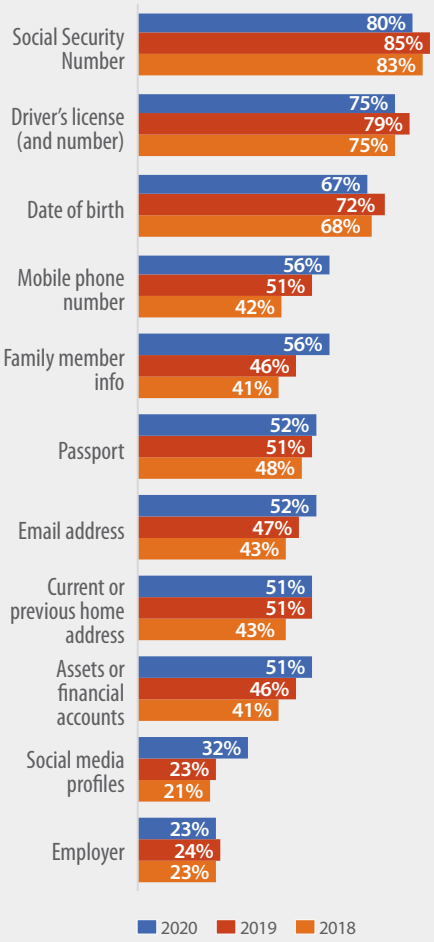
Just as importantly, fraud risk increases with imperfect customer mailing address information. Not knowing whether a submitted address or found address is deliverable reduces the ability to precisely evaluate the veracity of a submitted identity. It also diminishes a business's ability to use the data as a critical identity attribute and fraud signal.

More robust address deliverability data can help spot fraud such as synthetic whereby fraudsters piece together incongruent identity attributes including incomplete/partial addresses. Furthermore, first-party fraudsters leverage slight yet meaningful address mistakes for deniability.

Ultimately, address deliverability data is a powerful attribute which facilitates the effective location and identity of legitimate customers especially when cross referenced with high-risk address intelligence based on historical or consortium intelligence. Accurate, verified addresses can result in a 10% -15% uplift in identity verification matching, according to Loqate, a GBG solution.

Which of the following do you consider to be an important part of your personal identity?

(Check all that apply)

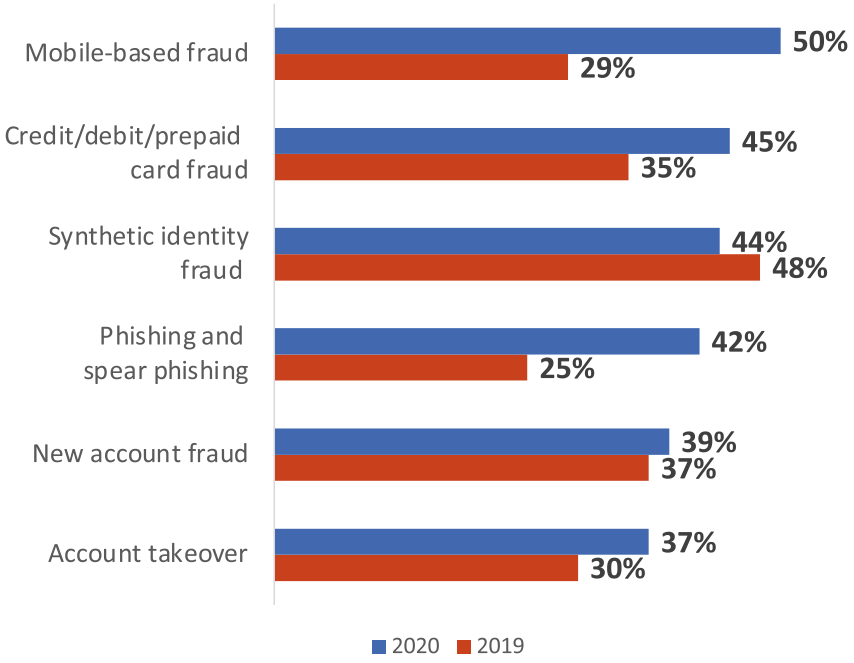


Source: Third Annual Consumer Digital Identity Study, IDology, 2020

Looking Over the Horizon

Mobile, Cards, Synthetic and Phishing Most Potent Fraud Types in Next 2-3 Years

What do you foresee as being the most impactful type/s of fraud in the next two to three years? (select all that apply)



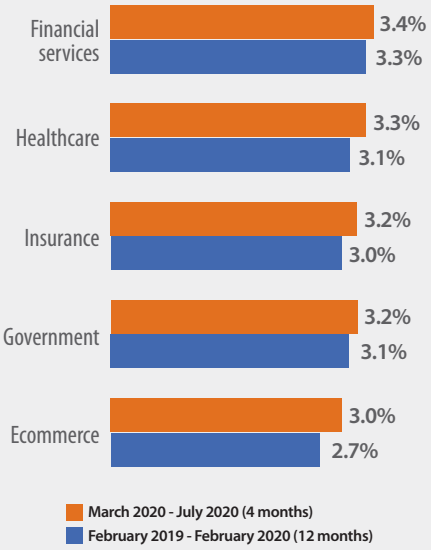
Source: Eighth Annual Fraud Report, IDology, 2021

The fraud crystal ball is as cloudy as ever with references to "uncharted territory" and "unprecedented times" becoming cliches. That said, the data gathered from over 300 fraud executives across industries confirmed some of the cliches and provided a window into how things might shape up in 2021.

We should expect more fraud, while digital adoption gains will maintain, and likely gather speed. Relative to the most potent forms of fraud, we predict the schemes and vectors as in years prior, but with added intensity and most likely more "bust outs" from incubating fraud hatched in 2020. Mobile, card, and synthetic led the way in 2020. Except for synthetic, all grew compared to last year in terms of expected impact.

Before vs During COVID; Americans' Confidence in Organizations to Protect their Personal Data

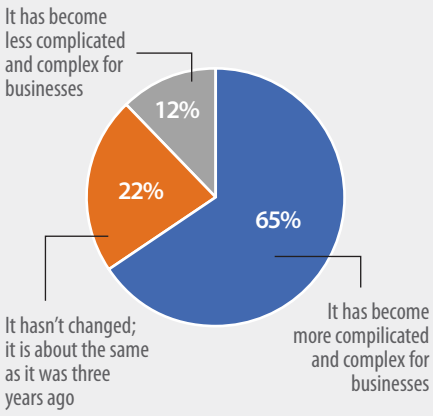
Average for each group



Source: The COVID-19 Effect on Fraud, Trust and Onboarding, IDology, 2020

Most Believe Identity Verification Has Grown in Complexity Over Last Three Years

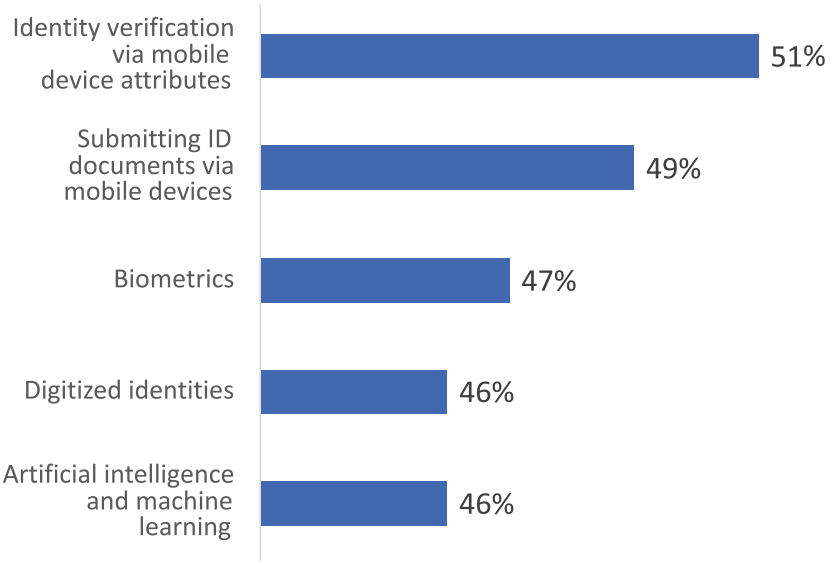
How has identity verification changed in the last 3 years?



Source: Eighth Annual Fraud Report, IDology, 2021

Mobile Attributes and ID Scan, Biometrics and Machine Learning Biggest Trends in Next 3-5 Years

What is going to be the biggest trend(s) in identity verification over the next three to five years? (check all that apply)



Source: Eighth Annual Fraud Report, IDology, 2021

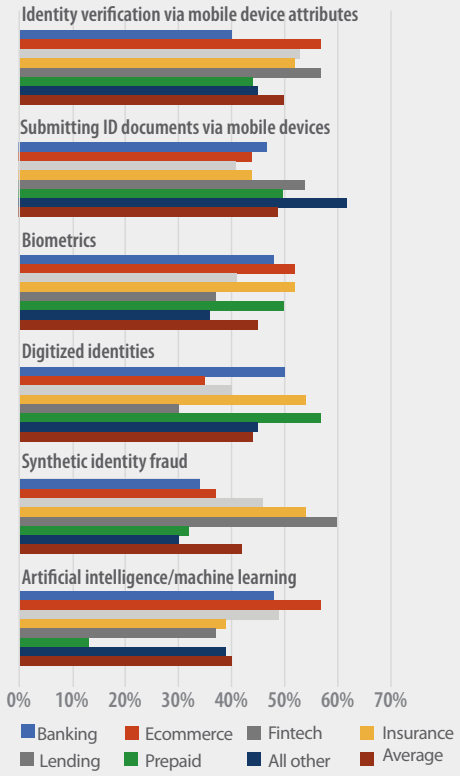
When asked to anticipate the biggest trends in 3-5 years, fraud executives confirmed the power of mobile as a transformative force. Identity verification via mobile device attributes received top billing with 51% of the responses. Submitting ID documents via mobile devices was a trend identified by 49%. Biometrics, digitized identities, and AI and machine learning also featured prominently.

In both developed and underdeveloped countries the mobile construct identifies us and opens the door to new omni services and experiences. Identity verification for the mobile customer offers the ability to establish and nurture trust between consumers and businesses.

And while regulations did not make it on the top of the list we can expect governments at the state and possibly federal levels to legislate. For example, the California Privacy Rights Act, aka California Consumer Privacy Act 2.0, which gives Californians even broader rights may be the first of many state laws with a long list of implications for the digital economy.

Biggest Trends by Industry

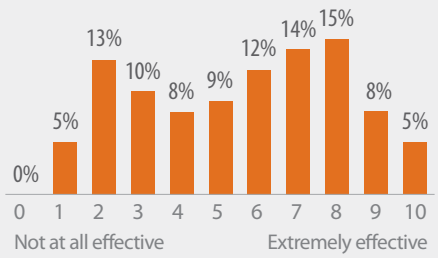
What is going to be the biggest trend/s in identity verification over the next three to five years? (select all that apply)



Source: Eighth Annual Fraud Report, IDology, 2021

About Half of Businesses Feel Their Companies Are Average to Less Effective In Both Deterring Fraud and Delivering Frictionless Customer Experiences

In your opinion, how effective is your firm in deterring fraud and providing friction-free user experiences with (1= not at all effective and 10=extremely effective)



Source: Eighth Annual Fraud Report, IDology, 2021

Conclusion

Like so many facets of life, fraud and identity verification experienced upheaval and change – some of which will be permanent. In 2021, we expect to see a continuation of many of the trends that appeared in 2020. There will be an intensification of digital adoption and engagement, as well as the approaches to fraud that worked. Phishing schemes, social engineering, elder fraud, mobile, and unemployment fraud will remain challenging. Synthetic fraud and first-party fraud will grow in 2021 as well.

While we expect the fraud threat to intensify, so too will customer expectations of a streamlined customer (onboarding) journey. The fusion of physical identity attributes with digital attributes will accelerate, maybe helping to close the gap between mutual exclusivity of friction and fraud.

While the collapse in demand for international travel kept people out of airports, cross border digital commerce brought the world closer. Unfortunately, the rush to digitize provided organized crime and nation states with the environment to commit fraud and steal data on a massive scale.

The push to locate and approve new customers without friction, deter fraud, and streamline the customer journey, especially for those newly digitized, requires businesses to execute numerous complex and involved processes.

For example, privacy and compliance regulations, which differ by region and country, will require transparency in data collection. The decisions made in the pursuit of compliance and even reputational risk will need to be more explainable and defendable as the compliance landscape intensifies and AI bias in areas such as lending comes into focus and scrutiny. Businesses will continue to pursue cross- border commerce which intensify the need for cross-border identity verification with the ability to process identities in compliance with foreign regulatory requirements and expectations.

As fraudsters collaborate and share intelligence, notably on the dark web in sophisticated forums and marketplaces, networks of organizations across industries and around the world will continue to gravitate towards the sharing of fraud intelligence. This will help to mitigate the impact of well-funded partnerships of criminals and nations who intend to inflict financial harm or pursue political agendas.

We expect to see more companies rely on the orchestration of layers of identity attributes and verification methods dynamically to remove friction and deter fraud. Data intelligence and data diversity will remain critical inputs to an effective defense.

Customization of IDV to meet the needs of the individual customer will accelerate. This includes the need to tweak and tune IDV in real time. It also requires businesses to possess the tools to anticipate discrete attacks, adapt to systemic changes in human behavior, and respond to the emergence of new customer segments, profiles, and needs.

How will the pandemic change identity verification and fraud deterrence?

"A lot of criminal groups know that systems are overwhelmed and understaffed and under-supported in these times, and they are taking every precaution necessary to try and take advantage of that."

"More identify verification happening across multiple channels, with multiple instances occurring for transactions so that we can try to truly verify identity."

"More deaths mean more chances of identity theft schemes and higher unemployment means more 1st party fraud plausibility."

"I would expect an increase in fraudulent behavior – desperate individuals often take drastic measures to access funds."

AI will need to more seamlessly integrate with fraud analysts to train machine models at efficient scale with the human eye and intuition, catching novel attack schemes that machines can miss.

Entire segments of population were forced to be digitally engaged, and the trust handshake of IDV at the front door to onboarding was IDV. It's why IDV is now the number one challenge in fraud deterrence

Here's the upside of the changes forced upon the world by the virus - humans adapt. In a matter of months, much of the US population moved from a familiar offline world to an unfamiliar and online environment. Enterprises embraced work from home (WFH) in a matter of days. And the scientific community developed vaccines in less than a year. In strange and unsettling times, Americans continue to adapt, which includes shoring up their digital defenses as they uproot much of their life to move online.

In fact, there's reason for optimism in this year's survey. Eighty-seven percent either completely agree or somewhat agree that their organization is equipped to make necessary changes to stay ahead of rapid digitization and COVID-19 fraud trends. Furthermore, 78% are increasing their fraud budget.

While businesses seem willing to rise to the challenges that lie ahead, a large percentage of consumers also seem committed to a safer, more secure future. In our recent report on the effects of COVID-19, the data showed that 119M Americans have taken steps to improve online security since the pandemic began.

In the aftermath of a trying year, there's reason to look forward to a more engaging and protected online environment for consumers and the businesses that serve them.

About IDology, a GBG Company

IDology offers real-time and on-demand identity verification and fraud prevention solutions for organizations operating in the digital environment. The IDology platform serves as a collaborative hub for monitoring and stopping fraudulent activity while also driving revenue, decreasing costs, and meeting compliance requirements.

For details on how IDology can help your business onboard and verify customers, visit **www.idology.com**.

IDology
a GBG company