

Black Swan? The COVID-19 Effect on Identity, Fraud and Customer Onboarding

IDology

If you're unfamiliar with the term "black swan," it's defined by Investopedia as an extremely rare event with severe consequences. While there is some debate as to whether our current pandemic is a black swan, the massive upheaval in global human behavior, business practices and data patterns, including the rise in criminal fraud caused by Covid-19, is undeniable.

Tasked with managing this disruption, enterprises across the world are searching to deploy systems that are safe and effective in reaching, identifying and trusting new and existing customers. In this effort, the most significant factor for success is a company's ability to access and understand its data. MIT Sloan research shows how utilizing numerous kinds of data can help prevent or limit the risk associated with a black swan event. Collecting more transparent, determinant and risk-related data intelligence, such as fraudulent verification data, is increasingly necessary to identify, model, mitigate and perhaps, establish a competitive advantage during such unpredictable events. Organizations that have access to important verification data and the ability to delve deeply into it are more likely to determine what is occurring in their domains and why.

However, data visibility is only half of the formula for identifying fraud while also onboarding customers with minimal friction. While more data granularity provides insights into the deeper causal factors at play, that data is wasted if it can't be used to achieve positive outcomes. The ability to adjust and fine-tune identity verification systems with deeper, more exact levels of precision and put data insights to work creates the ultimate value and drives revenue, creates effortless user experiences and deters more fraud. The more data-fed and customizable the identity verification and anti-fraud systems system, the better it can respond to current and future black swans. Increased data transparency and collection means faster recognition of behavioral changes, emerging threats and customer insights. When these systems are offered as SaaS they, at least theoretically, give businesses the agility needed to make real-time adjustments to risk profiles on the fly. The end result is better performance, empowerment, stakeholder trust and competitive advantage.

Black Swan events: Fastest times to reach bear market in the S&P 500 – The 2008 global financial crisis and COVID-19 pandemic

(Bear market: Price of stock index or security falls at least 20% or more from its 52-week high)



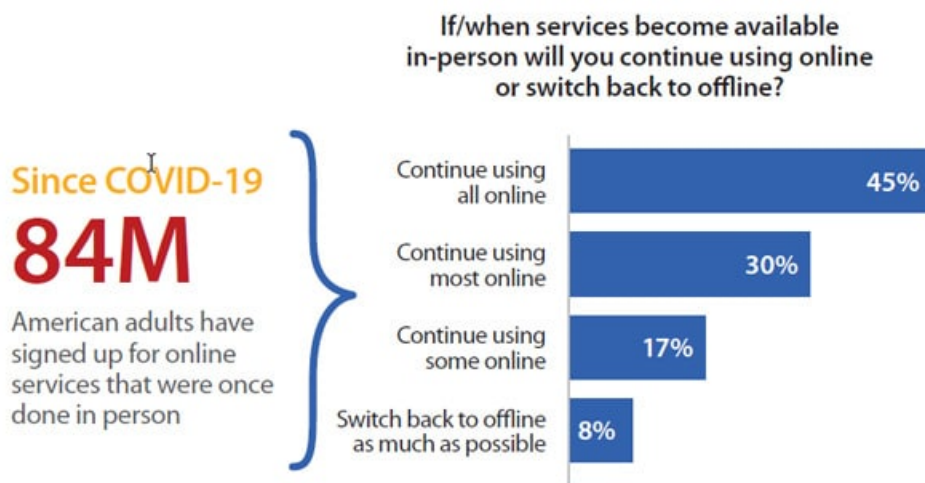
Credit: IDology

Understanding macro consumer behavior changes is a critical step in anticipating opportunities and mitigating impending risk, including fraud. Recent IDology research evaluated the pandemic's effect on digital identity verification, fraud and new account onboarding and confirmed just how consequential the COVID-19 crisis is. The data demonstrate the permanence of new consumer practices, such as the adoption of online services at the expense of offline interaction and more consistent, deeper engagement with smartphones (as if we thought that was even possible). It also indicates the potential for criminals to take advantage of black swan events.

In addition, historical IDology transaction data during Covid-19 has revealed unique consumer behavior and data trends, such as surging online account openings among the nation's elderly and swings in mobile attributes. The result is a retrenching of how people around the world prefer to interact with each other and companies and protect themselves from fraud, as well as what they expect from the customer journey and which businesses they trust today and in the future.

Research Highlights:

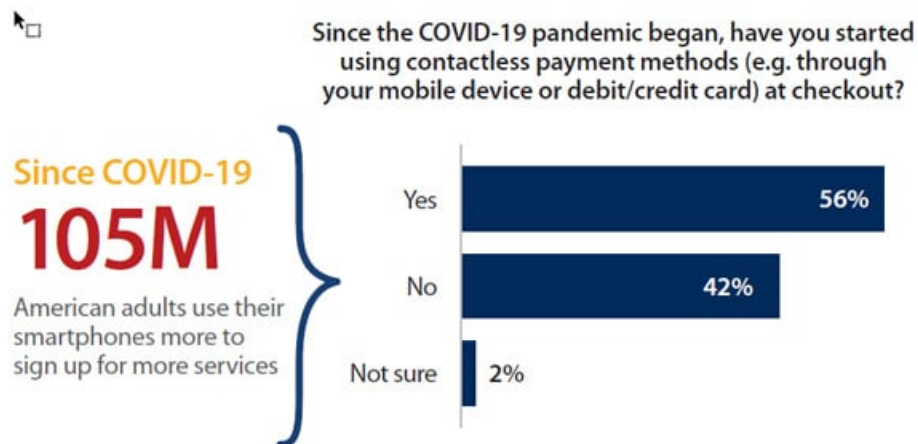
America is experiencing hyper-accelerated digital adoption, much of which will be permanent. Eighty-four million Americans signed up or applied for online services that were previously carried out in person. And, 75 percent expect to continue using all or most of these new online services after the pandemic subsides. With respect to the digital experience, America will never be the same.



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

Credit: IDology

Smartphone activity is surging beyond a number that already seemed high. One hundred and five million Americans are using their smartphones to sign up for new services. For example, 56 percent of adult Americans began using contactless payments during the pandemic, which is not surprising given the surface contact contagion of the virus. This level of adoption puts contactless payments in the mainstream of the technology adoption curve. The demise of cash is too early to declare, but the COVID-19 black swan may be the beginning of the end of mainstream paper and metals-based currency usage.



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

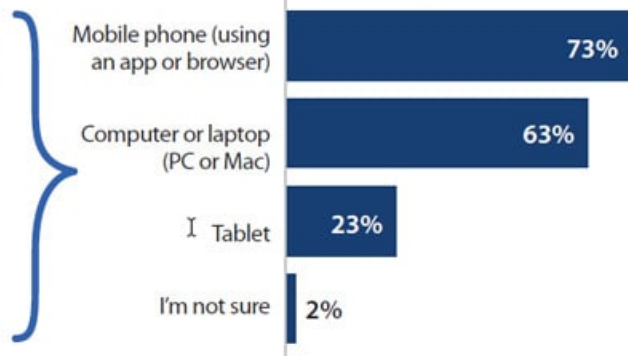
Credit: IDology

Driving the smartphone surge is the fact that Americans across the demographic spectrum are signing up for and activating services primarily from their mobile devices. A significant number of multi-channel online account enrollments from PCs and tablets remains but most are initiated from the palm of our hands. The number of Americans using mobile phones to open new accounts has increased 43 percent since the start of the pandemic.

Since COVID-19
98M

American adults have
signed up for a new
online account

Which of the following did you use when
signing up for your new online account(s)?
(Check all that apply.)

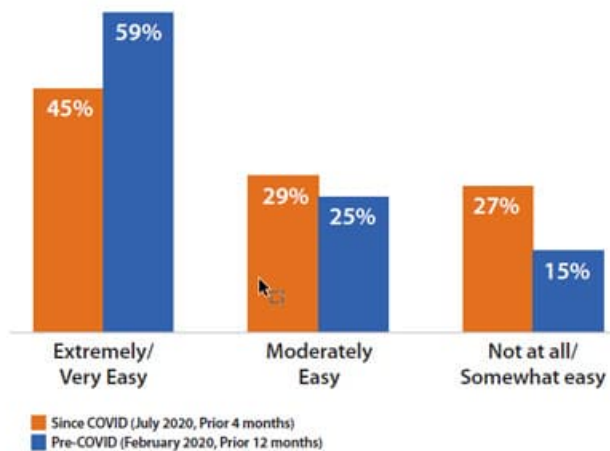


Source: The COVID-19 Effect on Fraud, Trust and Onboarding, IDology, 2020

Credit: IDology

IDology data showed a noticeable drop in the number of survey participants who viewed digital account opening and intuitiveness as extremely or very easy, from 59 percent before the pandemic to 45 percent during COVID-19. This is yet another data point indicating a rise in less technology proficient newbies turning to digital services. On the other hand, the number of Americans who reported that opening accounts online from their mobile devices was not at all or only somewhat easy increased by 80 percent. Another explanation to this trend could be that opening online accounts is actually more difficult given how unprepared entire industries and companies were for mass utilization of their digital account opening onboarding systems. Verticals such as healthcare and insurance did not build up robust, intuitive and streamlined identity verification and account onboarding offerings, thereby placing them at a disadvantage as consumers are conditioned to expect low friction, new account opening journeys.

When on your mobile phone, how easy is it to do the following?

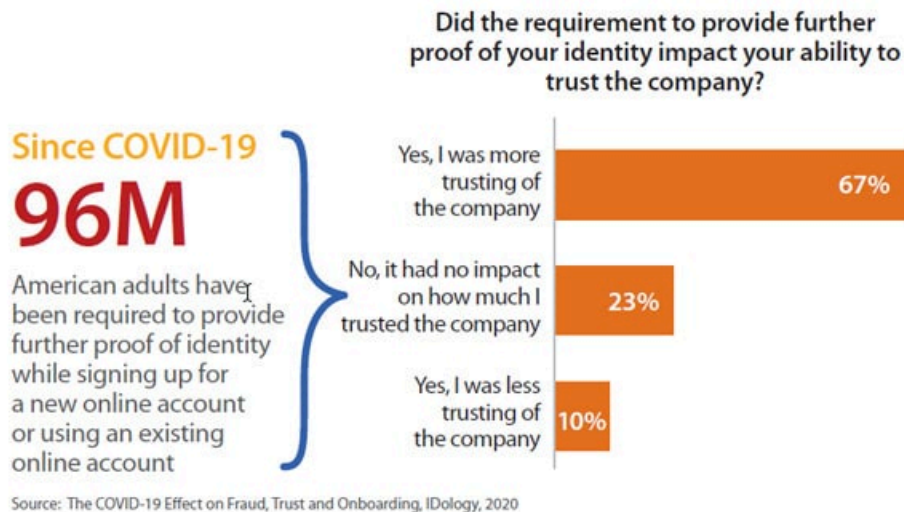


Source: The COVID-19 Effect on Fraud, Trust and Onboarding, IDology, 2020

Credit: IDology

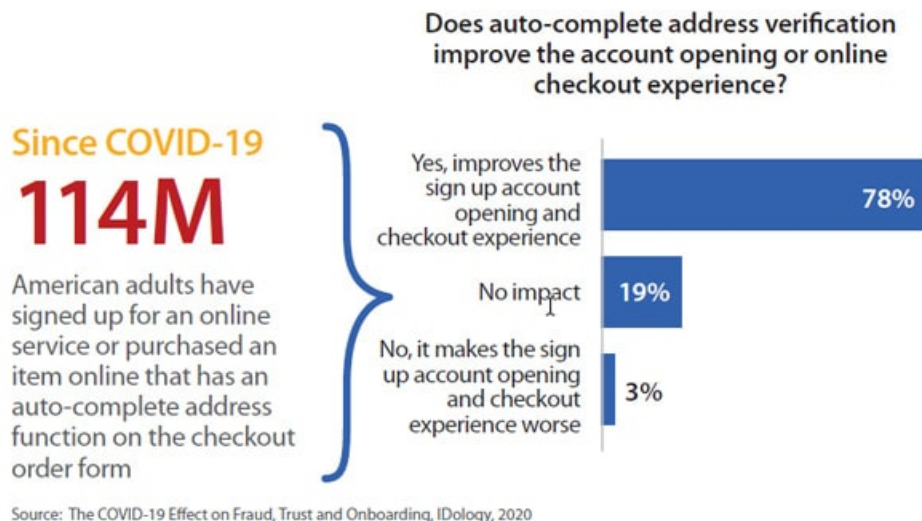
Enhanced identity verification experiences create trust. In the heightened environment of concern and fear, Americans seem to value businesses that take identity verification seriously. Once a back-end function, the identity verification experience has become a critical front-end success factor. In fact, 77 percent of Americans say they will choose a bank, insurance company or lender over another if they knew that organization had more robust verification credentialing. Of the 96 million

Americans that have been required to provide further proof of their identity when setting up a new account online, two-thirds indicate they were more trusting of the company as a result.



Credit: IDology

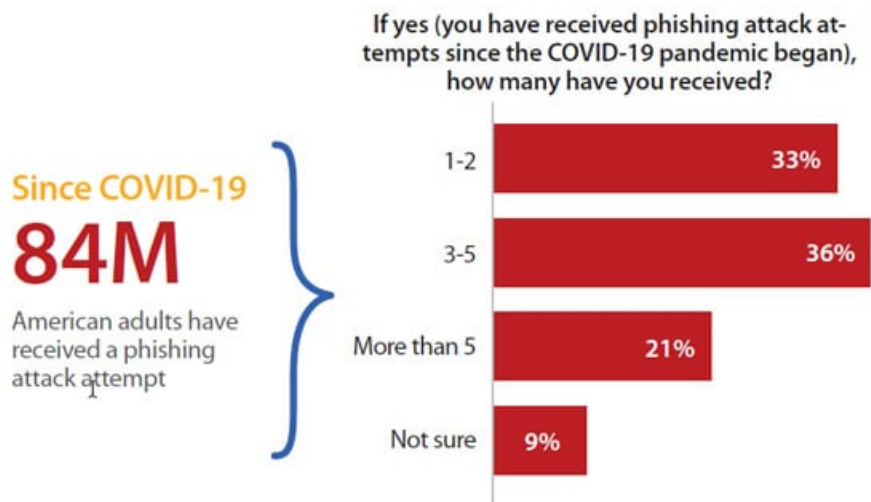
Increasingly, consumers are experiencing auto-complete address verification during account opening and online shopping, nearly 80 percent of which report that this functionality is helpful. Auto-fill makes entering personal address information easier and cuts down on effort, which is even more impactful when entering information on a mobile device. It also reduces the chance of fat-fingering incorrect information and ensures the delivery of goods and advancement through the onboarding process.



Credit: IDology

The number of Americans experiencing fraud is growing at a more rapid rate. Thirty-two million Americans (14 percent) were victims of new account fraud in the first four months of 2020, compared to (19 percent) in the 12 months leading up to COVID-19. Phishing has been especially insidious during the pandemic. Eighty-four million Americans reported experiencing a phishing attack attempt in the months following the pandemic's start, with an average of four attempts per person between March and June. This has shaped concerns about becoming a victim of fraud,

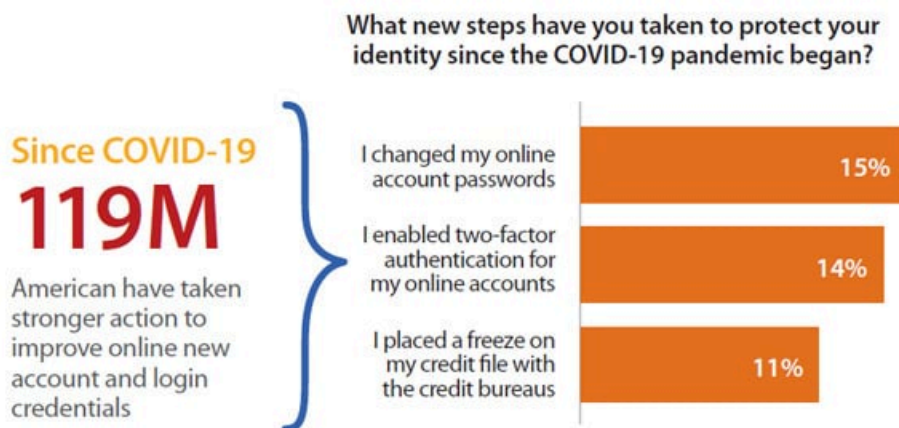
leading 71 percent of Americans to express extreme to moderate concern that their personal information could be used by a criminal to open a new financial account. Additionally, 68 percent have extreme to moderate concerns about mobile malware and fraud.



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

Credit: IDology

Americans are fighting back against fraudsters and taking stronger action to prevent compromising their personally identifiable information. Since the beginning of the pandemic, 119 million Americans have reinforced defenses by changing their account passwords, enabling two-factor authentication and placing freezes on their credit files, among other things. This is especially good news as dependence on the digital channel for basic services, such as shopping for groceries, increases and tech newbies vulnerable to sophisticated fraud schemes increasingly transact online.

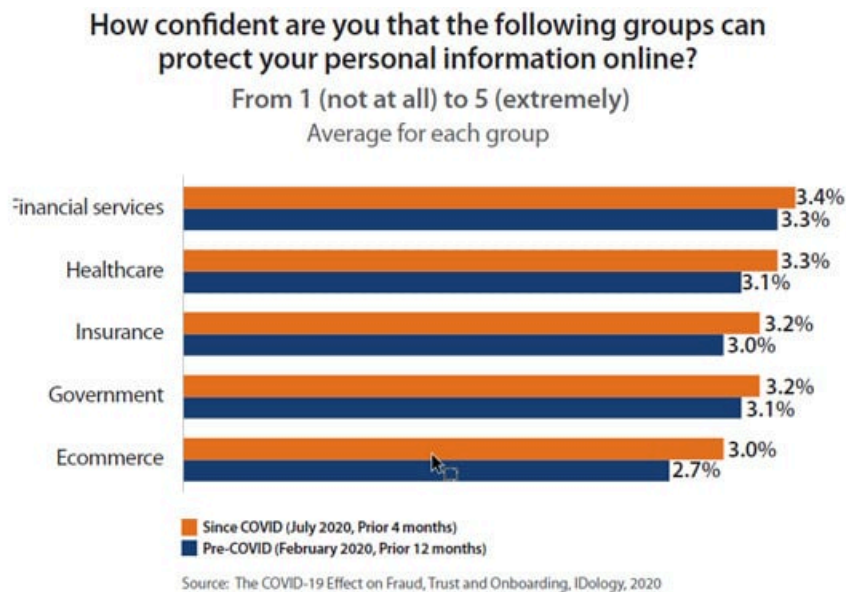


Source: The COVID-19 Effect on Fraud, Trust and Onboarding, IDology, 2020

Credit: IDology

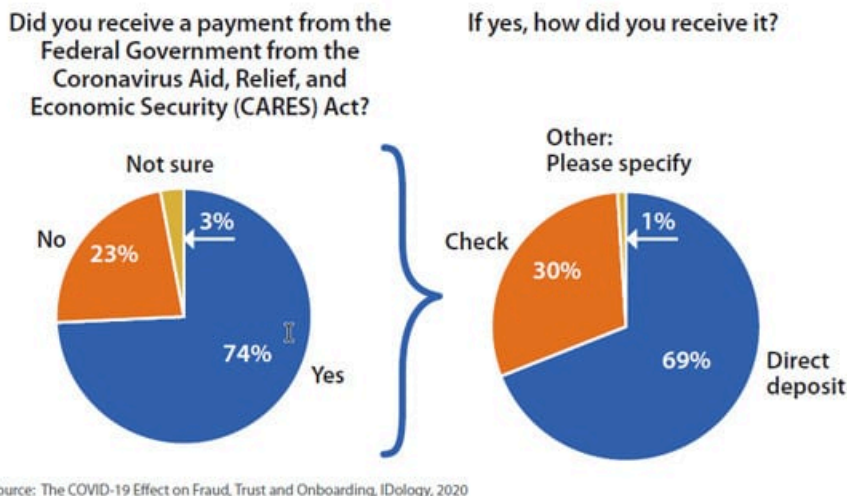
The research also revealed that Americans appear to have more trust in groups that can protect their personal information online. Compared to pre-pandemic, consumer faith in banks, healthcare providers, insurers and e-commerce companies has risen incrementally during the pandemic. Trust in the government's ability to protect personal information also rose, albeit slightly. One should note this is not indicative of the trust consumers place in organizations overall but of the ability of

an organization to protect their personal information. Given recent headlines about fraud associated with the Coronavirus Aid, Relief, and Economic Security (CARES) Act and more recent waves of state unemployment identity fraud, it will be interesting to see if this changes.



Credit: IDology

The majority of CARES Act payments are deposited via direct deposit. Among the 228 million American adults transacting online, 74 percent or 168.9 million received a payment from the CARES Act that was signed into law on March 27, 2020. Among those Americans 116.5 million adults received their disbursement by direct deposit and 50.6 million American adults received it by check, while the remaining 1.6 million received it by other methods.



Credit: IDology

Conclusion

Tectonic shifts in how humans interact and the modes they choose have disrupted identity verification and fraud detection data models. What once were red flags are now green lights.

Americans across demographic spectrums are digitizing to survive and this mass disruption enables criminal fraud to thrive.

As always, trust is at the core of commerce. The necessity to determine trust and the process of securely and smoothly verifying identities in a customer not present environment has taken on increased importance. Black swan or not, our data shows that the pandemic has triggered significant and, in many cases, permanent changes in human behavior, the importance of online identities, the usage of digital engagement and delivery, and fraudster go-to-market strategies.

Like swans, firms navigating through stormy waters need data signals and visibility to manage the currents and stay oriented. Streams of change require the agility to adjust and course-correct on the fly. And since each is unique, organizations need to outfit themselves based on their specific location, identity and fraud deterrence requirements, not someone else's. The fraud landscape is changing faster than ever before, resulting in a growing number of elements that need to be tweaked, tuned and verified to validate a consumer's identity. As a result, enterprises must view and understand novel shifts in their customer data, rework assumptions and meanings, and adjust systems to higher levels of sophistication.

As we exit into a post-COVID world and attempt to prepare for the next black swan, the importance of data transparency and customization that delivers the friction-free digital identity verification needed to locate and pass the legitimate while failing the fraudulent will never be the same.

The COVID-19 Effect on Identity, Fraud and Onboarding

Before vs. During the Pandemic

(March 2020 compared to July 2020)

Historic levels of digital conversion and permanence

Since COVID-19

84M

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

After the pandemic do you expect to:



A surge in mobile phone usage

Since COVID-19



Since COVID-19

142M

Americans have started using contactless payments

76M online Americans have signed up for P2P services

A rapid rise in fraud

Since COVID-19

35M

online Americans say a new account has been opened up without their authorization



84M

Americans reported experiencing phishing attacks

Americans are fighting back!

Since COVID-19

35M

of online Americans have taken action to improve online identity credentials



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.



The rules are changing rapidly

EMPOWER your identity verification and anti-fraud response systems with more data, more agility, more precision and more customization.

Your business is different. Verify differently.

IDology offers the most **customizable** digital identity verification solution in the world – 34 million custom scenarios **you control in real-time.**



For more information on how IDology can help onboard and verify your customers, visit www.IDology.com

IDOLOGY
a GBG company

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

© 2020 IDology Inc., a GBG Company