EQUIFAX

Data lights the way for meaningful insights

DATA & ANALYTICS | VOLUME 8

Identity & Fraud On The Horizon

PR Daily's CONTENT MARKETING Awards

Honorable Mention

Be Yourself.

Everyone Else Is Already Taken.

Oscar Wilde

Deliver experience, secure privacy

Four ways customers can win in best-in-class identity & fraud

ADAM GUNTHER
SENIOR VICE PRESIDENT
GLOBAL IDENTITY & FRAUD

MARK LUBER
CHIEF PRODUCT OFFICER
US INFORMATION SOLUTIONS

The digital commerce explosion as a byproduct of the pandemic changes how businesses leverage and view their digital channel. Digital can no longer be viewed as a risky option for omni–channel experiences because it is increasingly the primary or only channel. And going beyond omni-channel — innovation in multi-channel transactions that blend digital purchase and in-person access — further stretches traditional thinking. Innovations in digital commerce have created opportunities to manage a firm's risk while engaging consumers like never before.

1 Winning Firms Optimize and Safeguard Digital Channels

Winning firms want to transact confidently with their customers by saying "yes" more often to their "good'' consumers. Working together, a delightful customer journey can also be one that enhances privacy while being secure. For instance, in a physical world, a driver's license is often used to confirm age of majority. When sharing a driver's license, a consumer is also sharing their full address, date of birth and height. Digitally, we have the opportunity to simply know, yes or no, that the consumer is over the age of majority. Imagine further, if a consumer has even greater access and control of their personal data so they may consent and safely share their credentials with others. This scenario has come to life with a credit union service provider, Boniffi Member Pass. With Member Pass, credit unions assign members a single digital credential that they can use as verification across all channels and across credit unions.

2 Winning Firms Glean and Make Use of Greater Insights

Although digital banking is moving mainstream, particularly with digital native consumers, all ages have now hopped on board and the need to validate identities digitally has become table stakes. While there are a plethora of data and technology vendors in the market, smart companies are not only validating identities, they are gleaning and making use of greater insights. These insights are then being mapped back to individual consumers so they can meet consumers' expectations to deliver a delightful and personalized engagement model. These delightful experiences drive repeat business, loyalty and maximize customer lifetime value.

The convergence of identity, fraud and customer engagement has come to life in the new mainstream digital channel. That said, this shift has not altered the consumer's security and privacy expectations. Conversely, lenders still need to meet regulatory requirements and adhere to risk tolerance policies. It is possible to meet all stakeholder needs while optimizing the digital journey experience. Advancements provide lenders with more opportunity to evaluate and react to consumer behavior incrementally and over time. Such approaches provide lenders the opportunity to approve smaller limit amounts initially and increase the amount — along with associated exposure and risk — as the relationship deepens over time.

3 Winning Firms View Identity as a Line of Business

To meet these demands, businesses must not view identity assurance and fraud prevention as the cost of doing business. There are opportunities to work collectively together to address these needs with common standards and cooperation so we can all transact confidently in a non-face to face environment. For inspiration, consider the sharing economy. Participating in the sharing economy — renting a house for a weekend — requires members of the network to share information with one another to create an enjoyable experience for all participants from the guest to the host.

4 Winning Firms Recognize Identity is a Team Sport

When businesses work together by leveraging networks of information, they can create a truly pervasive digital identity and deliver personalized and secure customer experiences. Customers can safely deliver a better digital experience, accept more good customers and say "yes" more often. Given the explosion of digital interactions, every company must balance privacy, security and customer experience.

Advancements in analytics, big data computing, identity systems and modern cryptography make it possible to broaden your reach into more areas of the consumer's digital journey. Customers can safely deliver a delightful digital experience, accept more good customers and say "yes" more often. ■

Download the full report

Lenders prioritize digital identity security over acquisition security

The benefits of adopting digital identity protection

DAVID ADAMS
PRODUCT MARKETING, COMMERCIAL

The increased use of digital services within the past year has come with an increased risk of security issues. Cybercrime is worsening as hackers plan attacks on a massive scale to steal usernames and passwords, with 36 billion records on social sites breached in 2020 alone. This unfortunate reality means that firms like auto dealers, banks, credit unions and peer-to-peer (P2P) lenders that use digital services must focus on bolstering user identity verification and authentication measures.

PYMNTS' research finds that 43 percent of firms have plans to invest in digital authentication solutions to protect their businesses and their customers from increased security threats. Interest is so strong, in fact, that 79 percent of them are willing to sacrifice customer growth to improve the security of their transactions. Even with so many firms wanting to improve in this area, many admit they still have issues reconciling the need for enhanced digital identification processes with the implementation of new customer-facing technologies.

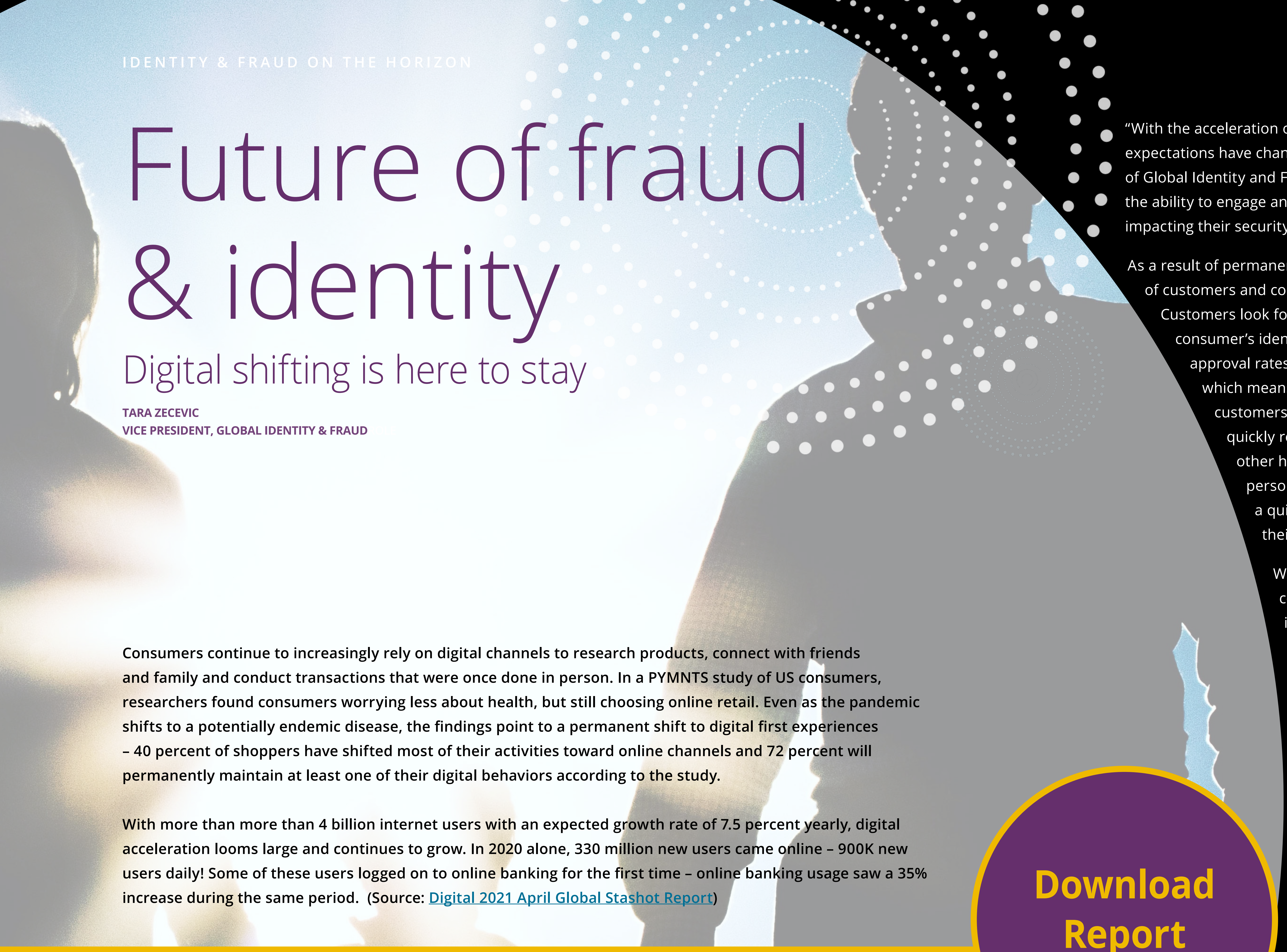
The Next Wave: Business Adoption Of Digital Identity Protection, a PYMNTS and Equifax collaboration, explores the key drivers, perceived benefits and obstacles to implementing digital identification and verification technologies. The report is based on a survey of 307 auto dealers, banks, credit unions and alternative or P2P lenders and explores what motivates them to seek solutions that can help them verify their consumers' identities throughout their digital journeys.

Businesses view consumers' lack of digital skills and technology as a major problem when implementing digital verification and authentication solutions. Fifty-one percent of all firms planning to invest in such solutions believe that consumers lack the necessary digital skills to navigate them, and 48 percent of businesses feel customers also lack the required technology to do so.

Firms also report internal difficulties with implementing identity verification and authentication, especially when it comes to operational challenges related to these processes. Fifty-four percent of P2P lenders that plan to invest in these solutions report this to be a problem, for example, while 42 percent of banks and credit unions report the same. Internal problems that can cause these difficulties include digital processes that take too long, lack of financial resources to implement digital authentication and digital authentication processes that have resulted in false identities.

Other organizational issues can also prevent the implementation of identity verification and authentication improvements. Fifty-five percent of all firms admit that poor coordination between their fraud and security strategies and their customer-facing operations prevents identity verification and authentication processes from becoming more efficient. More established businesses tend to have coordinated fraud and security measures with their customer-facing operations, however. Forty-five percent of firms that have been in business for more than 30 years say their fraud and security are tightly coordinated with customer-facing operations, compared to just 21 percent of businesses that are less than 10 years old that say the same. Banks and credit unions are the most likely to say their fraud and security operations are tightly coordinated with customer-facing operations (47 percent), followed by P2P lenders (40 percent) and auto dealers (31 percent).

These findings touch on just a few of the insights outlined in our research. To learn more about businesses' perceptions of and plans for digital identity protection, download the report. ■



Future of fraud & identity

Digital shifting is here to stay

TARA ZECEVIC
VICE PRESIDENT, GLOBAL IDENTITY & FRAUD

Consumers continue to increasingly rely on digital channels to research products, connect with friends and family and conduct transactions that were once done in person. In a PYMNTS study of US consumers, researchers found consumers worrying less about health, but still choosing online retail. Even as the pandemic shifts to a potentially endemic disease, the findings point to a permanent shift to digital first experiences – 40 percent of shoppers have shifted most of their activities toward online channels and 72 percent will permanently maintain at least one of their digital behaviors according to the study.

With more than more than 4 billion internet users with an expected growth rate of 7.5 percent yearly, digital acceleration looms large and continues to grow. In 2020 alone, 330 million new users came online – 900K new users daily! Some of these users logged on to online banking for the first time – online banking usage saw a 35% increase during the same period. (Source: Digital 2021 April Global Stashot Report)

"With the acceleration of digital, consumers' expectations have changed," says Adam Gunther, SVP of Global Identity and Fraud at Equifax. "They want the ability to engage and transact with ease without impacting their security and privacy."

As a result of permanent digital shifting, the needs of customers and consumers are converging. Customers look for assurances about the consumer's identity so they can maximize approval rates with low false positives — which means negatively impacting good customers — and have the agility to quickly react to changing needs. On the other hand, consumers are seeking a personalized, stress-free experience — a quick response time with certainty their identity is secure.

When businesses feel increased confidence about the consumer's identity, they can accelerate growth by approving more customers. "Winning firms can meet both their needs and consumer's needs and deliver a delightful customer experience," says Adam Gunther. "Consumers enjoy larger control over what information is shared and experience greater protection against first and third party identity theft."

Growth of the Internet of Things (IoT)

With technology advancements (e.g. computing power and Internet of Things) firms now have unprecedented access to vast amounts of data and signals that can be harnessed to drive the insights. These insights will enable firms to interact with confidence while managing their risk. In financial services, better insights help customers differentiate between normal and suspicious behavior. Each interaction consists of hundreds of signals such as time, location (for example the location of a smart car), behavior with the device, etc. "Taken holistically, signals can paint an accurate picture because humans are creatures of habit," says Sriram Tirunellayi, VP of Global Identity and Fraud Data Sciences at Equifax. "Knowing where consumers normally live, work and play can be used to make better business decisions."

Rise of digital identity frameworks with modern cryptography

Globally, new ecosystems are aiding consumers in their ability to provide identity assurance, credential assurance and their informed consent.

These systems center consumer security and privacy along with transparency and user experience at the heart. In these frameworks, trusted digital identities can be thought of as a set of trust outputs that can be accessed at various times by relying parties with consumer consent. An example of this is the Canadian Verified.MeTM service. Verified.Me helps consumers confirm their identity by sharing consented personal information held by their financial institutions with other parties (e.g. government, other financial institutions, telecommunication providers, retailers) to provide identity assurance and in turn receive access to goods or services.

Such ecosystems can enable an enjoyable digital first experience where identity assurance comes in a single click. Examples include:

- Confirming a consumer is legal age of majority to access adult content
- Verifying vaccination status
- Providing proof of education credentials
- Accessing voting rights
- Renewing your driver's license

The above use cases may only be annual events and hence, consumers often forget their usernames and passwords. These events are frustrating for consumers, yet can be exploited by fraudsters and can be operationally challenging for organizations to manage password resets. Given the permanent shift to digital first experiences, businesses should not expect to see customers in-person any time soon. Instead, adopt the latest advances in fraud and identity and know who is behind that single click. ■

Mitigating fraud across the omni-channel gap

Three foundational pillars for fraud mitigation

PRIYA SARATHY
IDENTITY & FRAUD, DATA & ANALYTICS

Watch
How One Synthetic ID Leads to a
$700K Loss

Businesses—from retail to financial services—are increasingly seeing fraud as a barrier to digital innovation and omni channel experiences. To mitigate omni-channel fraud risks effectively, businesses need to focus on three foundational pillars of fraud mitigation:

- Verify identity with multi-data sources
- Link multi-data dynamically (not statically)
- Develop intelligent AI enabled signals

1 Verify identity with multi-data sources

Businesses need the ability to access and organize diverse data sources from: service channels, digital and non-digital, industries, and applications. Multi-source data includes contributed data, interaction data, consent data, feedback data and social media data. Together the enriched and organized information pool can add dimensionality around an identity.

By associating a digital identity with specific and confirmable PII entities and triangulating the identity's changing relationships over time, data scientists can accurately verify the consumer's identity with person, time and location pins.

2 Link multi-data dynamically (not statically)

By linking multi-data with a dynamic key, we can create a holistic view around the identity in motion. Data scientists can use AI-driven graph algorithms to build a rich matrix of relationships. Keying and linking digital data from email address, phone number, and device ID along with static PII elements dramatically reduces customer friction. The omni-channel gap between the digital and in-person profiles. This is important for retailers because fraudsters can register purchases quickly against different industries using synthetic identities.

3 Develop intelligent AI enabled signals

AI enabled multi-data signals help catch fraud faster by locating very subtle and complex fraud such as first or third party fraud or credit washing activities. AI enabled insight engineering designs support deep searches across data to respond to query like: *How do you establish the patterns of credit washing behaviors using not just one financial institution but across a network of institutions?*

Digital information is dynamic by nature and can accumulate rapidly. To stay one step ahead, analytic intelligence must translate information faster and evolve with the complexity of a digital identity. Then, data scientists can investigate these patterns with AI and build a framework to capture fraud signals in the digital ecosystem.

Increasingly, consumers demand a seamless digital payment experience. Omni-channel experiences require accurate and real time information linking across online transactions and traditional store/ branch interactions. By verifying identity with multi-data sources, linking multi-data dynamically and developing intelligent AI-enabled signals, businesses generate intelligent signals and insights to fight fraud across multiple channels.

New fraud types roar onto the scene

Fight back with the latest insights

LAURIE ANDERSON
IDENTITY & FRAUD, PRODUCT MARKETING

Introducing: The Identity and fraud trends report from Equifax

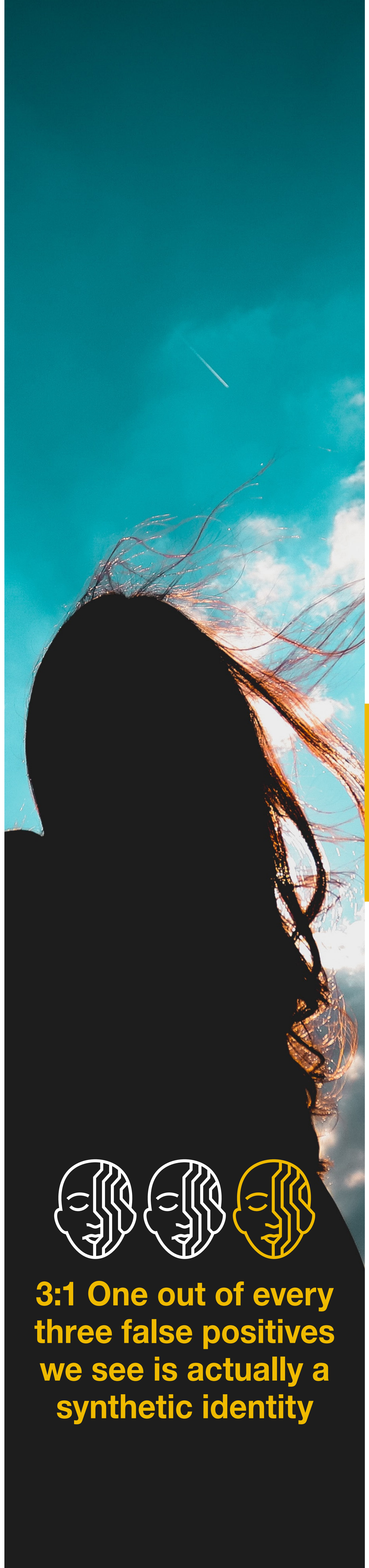
This new quarterly report will help organizations better protect against fraud threats by exposing the top trends we're seeing in the market. Knowing that you can't battle what you can't see, our goal is simple. We're providing timely, hyper-relevant insights to help businesses better understand new and existing fraud schemes. Packed with data, trends and "pro tips" from our expert team of fraud analysts, the report offers a big-picture fraud perspective and a rare opportunity for companies to benchmark fraud activity with their portfolios.

Each quarterly report will have a dedicated fraud focus, with this report focusing on synthetic identity fraud. Inside, you'll read about year-over-year synthetic ID trends and get first-hand "insider" information and insights on fraud mitigation best practices.
You'll get fresh ideas for intelligently differentiating and detecting suspicious activity. That way, you can put guard rails around it and steer legitimate, qualified customers toward a path of financial empowerment.

Fraud is escalating. It's time to act. Keep reading for actionable data and insights to help you better detect and fight fraud across your organization, at every step of the customer journey.

What is synthetic identity? A foundational fraud scheme

Unlike traditional identity theft, where a consumer's personally identifiable information (PII) is stolen and used to obtain financial products, synthetic identities are fictional. They can include a hodge-podge of real information — bits and pieces of real names, addresses and SSNs from different people — or a combination of real and fake information.



3:1 One out of every three false positives we see is actually a synthetic identity

Once the identity is created, criminals start building a credit history associated with the identity, often by first becoming an authorized user of someone else's good account. They then start applying for credit. This legitimizes the synthetic identity's credit and as a result the identities look like real people and creditworthy consumers, which is what makes synthetic identities hard to detect. While synthetic identity fraud is a global fraud issue, it's important to note that it's also the foundation of other fraud schemes like authorized user abuse and credit piggybacking. Put simply, the issues aren't separate; instead, they're intertwined.

- **Authorized user abuse:** The synthetic identity fraudster may pay a primary account holder to allow them to become an authorized user on their good account. This is collusion where both parties benefit. This relationship gives the authorized user direct access to the primary user's credit line and accompanying history.
- **Authorized user velocity risk** A notable risk of authorized use abuse is when organized crime rings continually add synthetic identities to credit cards as authorized users over time. We call this authorized user velocity risk.
- **Credit piggybacking:** Authorized user abuse is a form of credit piggybacking, in which fraudsters use information from legitimate card holders who are in good standing. This can manifest into credit boosting schemes tied to credit repair and other fraud types. While not all piggybacking is fraud, it can point to an increased potential for fraud as criminals look for ways to activate synthetic identities.

One portfolio. $25 million in fraud charge-offs.

A recent portfolio-specific Equifax study redlined $25 million in potential charge-offs in one year due to fraud charges associated with authorized user abuse. Within that same portfolio, more than 62,000 existing accounts were identified as potential synthetic identities, which could easily result in $8 million+ losses in a single year.

Equifax Case Study, Tackling fraud initiated through authorized user abuse

Consumers face more exposure online: Evidence of double-digit increases across fraud types

To explore the synthetic identity risk trend related to authorized user abuse, we monitor consumer activities based on inquiry transactions. Our data and insights around synthetic identity reveal a shift fueled by the accelerated move toward "faceless," online channels during 2020. As a result, we're seeing double-digit increases across specific fraud types.

To track the impact of synthetic identity fraud risk for credit and lending industries, we monitor two trends:

the synthetic identity alert rate (which represents the potential synthetic identity risk on the booked portfolio) shown on booked accounts.
the booked accounts performance (e.g. delinquency) based on the trades reported to the Equifax consumer credit file.

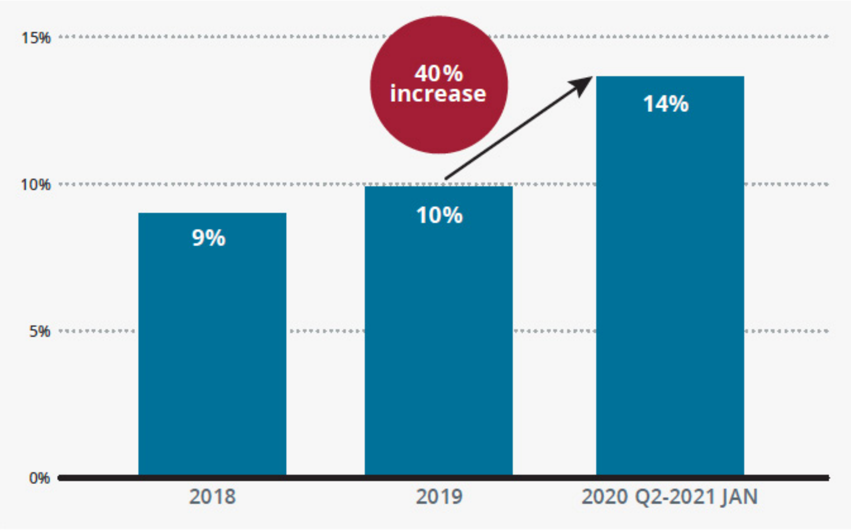


Figure 1: Credit piggybacking among suspicious synthetic identities

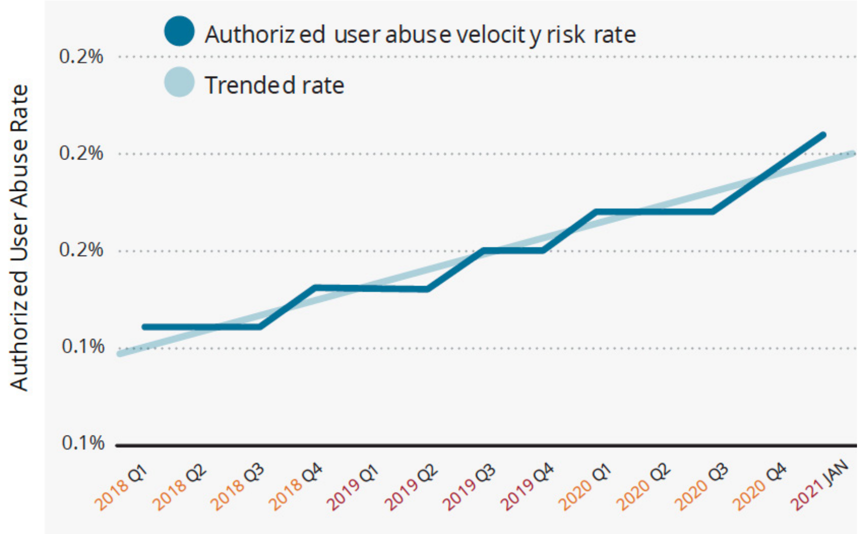


Figure 2: Authorized user abuse velocity risk: Quarterly analysis

After the Covid19 outbreak in April 2020, we saw that fraudsters were more likely to use credit piggybacking. Figure 1 shows credit piggybacking usage among suspicious synthetic identities increased by 40 percent through January 2021. In Figures 2 and 3, we see authorized user velocity risk has slowly but steadily increased from January 2018 through January 2021 by 26 percent.

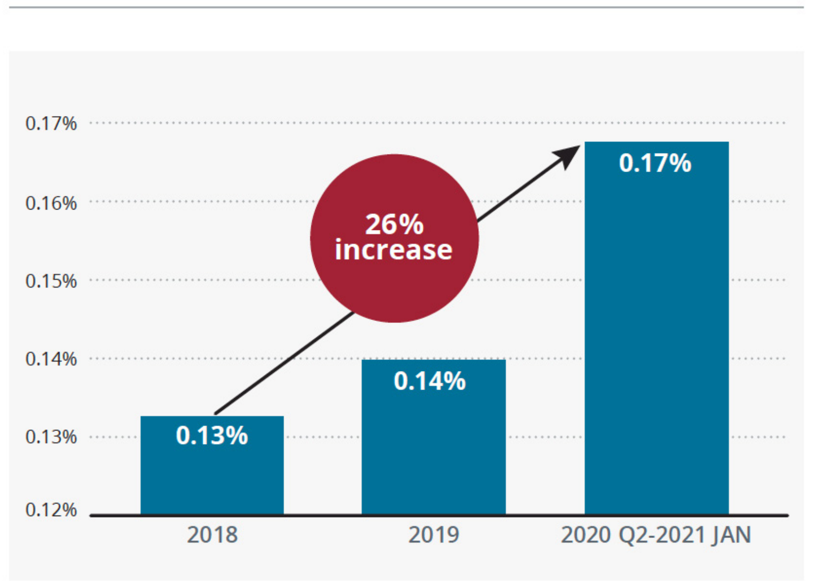


Figure 3: Authorized user abuse velocity risk: Year over year analysis

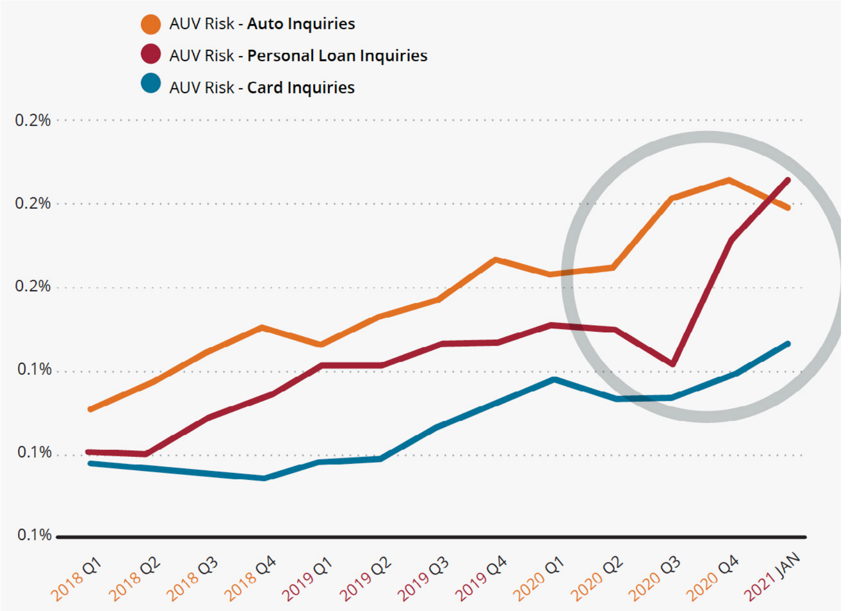


Figure 4: Authorized user abuse, velocity risk: Lending portfolio analysis

Interestingly, in Figure 4, we see authorized user velocity (AUV) risk is an increasing trend seen across all different lending portfolios: card, auto loans and personal loans.

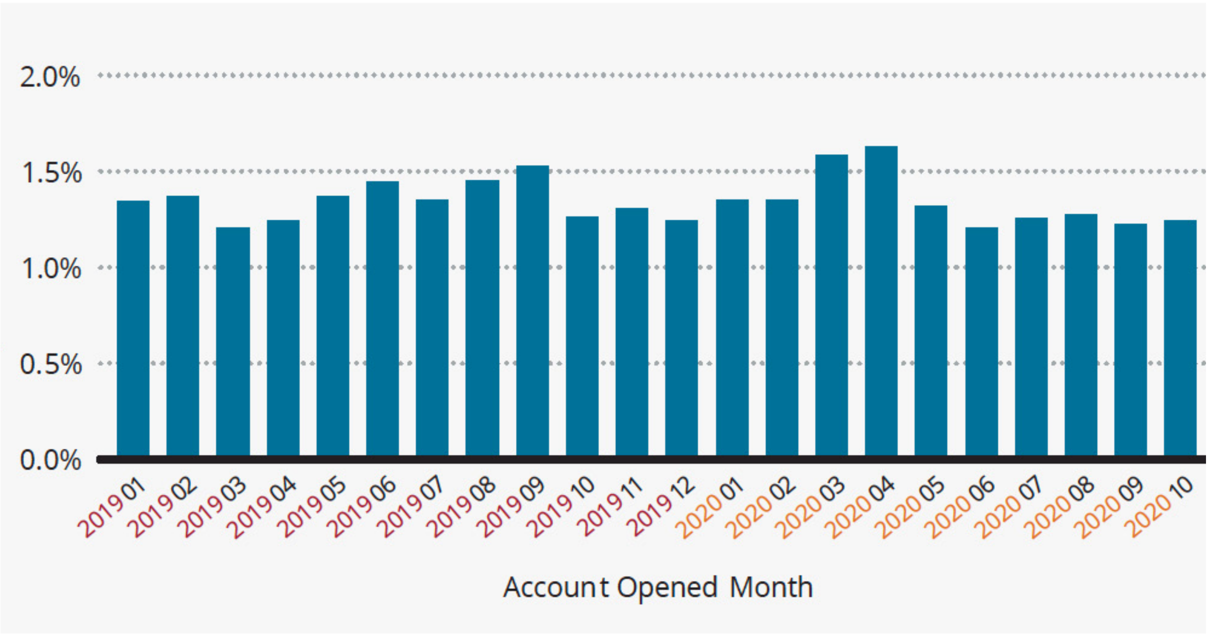


Figure 5: Synthetic identity fraud risk on the booked accounts

As we see in Figure 5, synthetic identity alert rates were high in 2020 March and April, but after 2020 April the alert rate returned to the normal level around 1.3 percent.

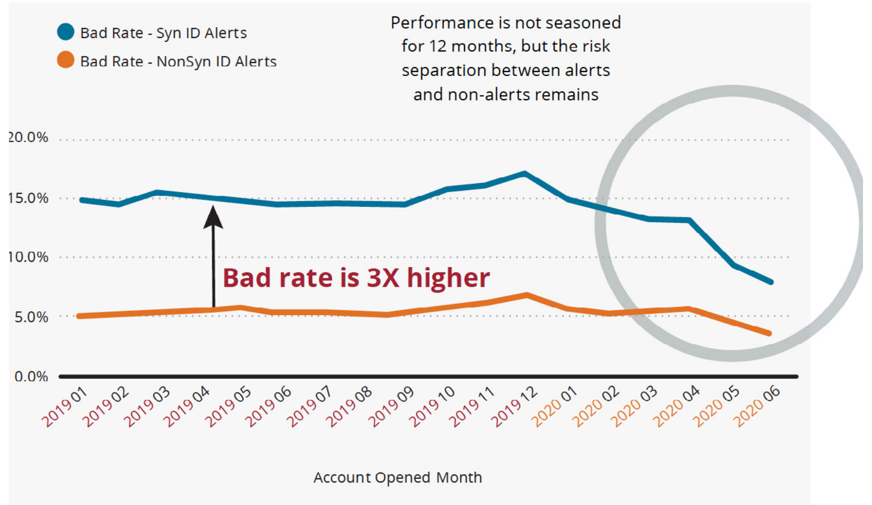


Figure 6: Bad rate (60 DPD+ in 12 MoB) — Performance observed 2020 Dec

In Figure 6, we see stark differences in bad rates. "Bad" accounts are 60 days past due (DPD) or worse in 12 months on the book. The bad rate among the synthetic identity alerts remained stable over time, yet it is three times higher than the non-synthetic identity alerts.

Behind the numbers

As criminals focused their efforts on the "opportunity of the moment," namely government benefit and stimulus payments, synthetic fraud activity slowed during 2020. However, given the year-over-year increases in credit piggybacking and authorized user velocity risk from 2018 to 2021, it's clear that a lack of comprehensive synthetic identity fraud control remains an industry issue. In a post-pandemic era, reducing synthetic identity risk on the books is a top priority for fraud executives.

What's more, the surge in use of online services last year increased the potential for fraud, prompting businesses such as auto dealers, banks, credit unions and online lenders that use digital services to focus on strengthening user identity verification and authentication. Recognizing their increased vulnerability to identity verification risks, businesses are taking action.

In a recent survey conducted by Equifax and PYMNTS.COM, almost half of the participants plan to invest in digital ID solutions to address these concerns. ■

SOURCE: Large Firms Are Focused On Digital Identity

Four keys to fighting identity fraud

1 DATA

Supplement internal anti-fraud tools with multi-dimensional data resources from credit reporting agencies and data aggregators specializing in fraud. This information uncovers "proof of life" behavior characteristics of legitimate applicants.

2 BEST PRACTICES

Use fast, reliable identity verification techniques that check applications against multiple sets of public and proprietary data to confirm things like:

Is the address real?

Is there an employment record or a registered vehicle? Are there utility accounts?

3 TECHNOLOGY

Use machine learning algorithms to help discover identity discrepancies and unique behavior patterns, such as authorized user abuse, that may transcend multiple accounts at multiple creditors. This can help increase detection rates while lowering false positives — in essence, providing a better experience for the consumer.

4 ANALYTICS

Use data analytics to detect linkages and suspicious patterns indicative of phony or manipulated identities. For example, by comparing a SSN to a consumer's PII, algorithms can determine how well a supplied SSN matches its identity. A positive SSN confirmation along with several negative alerts can signal the creation of a synthetic identity or other SSN-related fraud account opening.

Download latest trends report

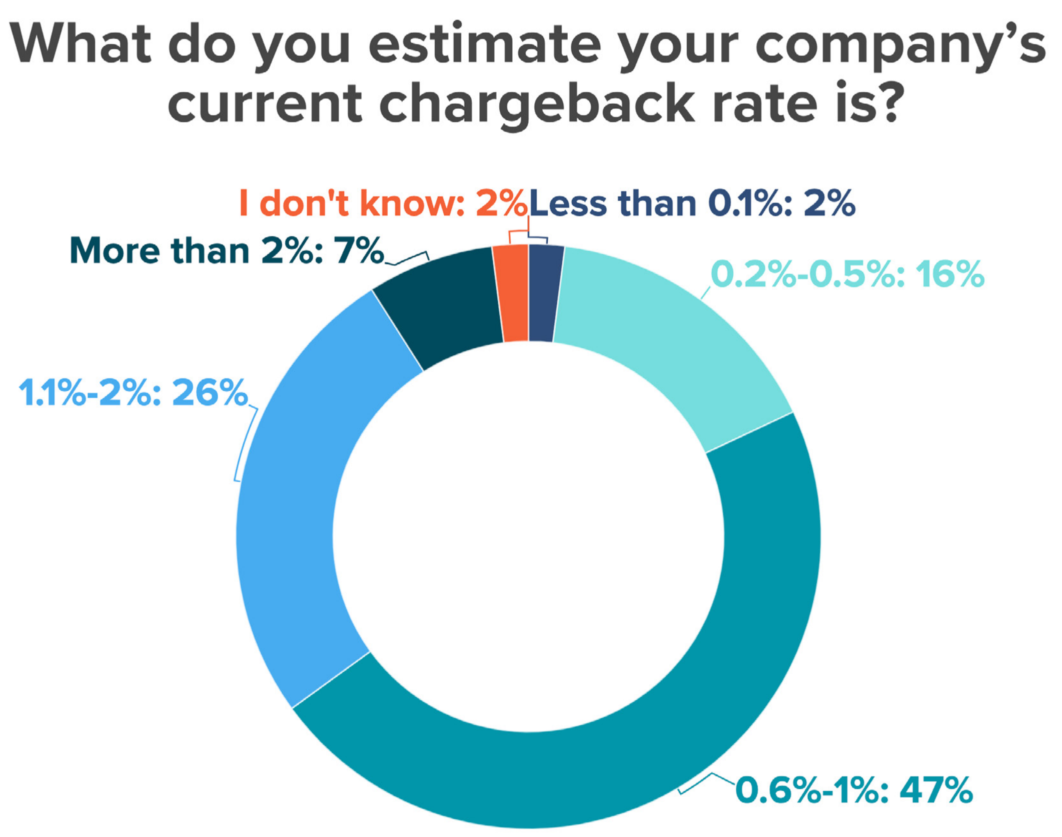
Digital payment experiencing big changes

Data shows digital payment opportunities and chargeback risks in 2021

The global adoption of digital transactions exposed more businesses than ever to the ups and downs of e-commerce. Accepting more payment methods means businesses can better compete and cater to consumers' needs.

70% of businesses have been in a fraud monitoring program in the last 12 months.

Today, an average of 33% of companies in a 2021 Kount survey accept card-not-present (CNP) payments via contactless payment apps, online transactions, and telephone. Additionally, 19% accept cryptocurrency, and 86% offer subscription-based or recurring billing. But new payment methods and pickup options dramatically increase a business's risk of accepting fraudulent orders and dealing with the resulting chargebacks.



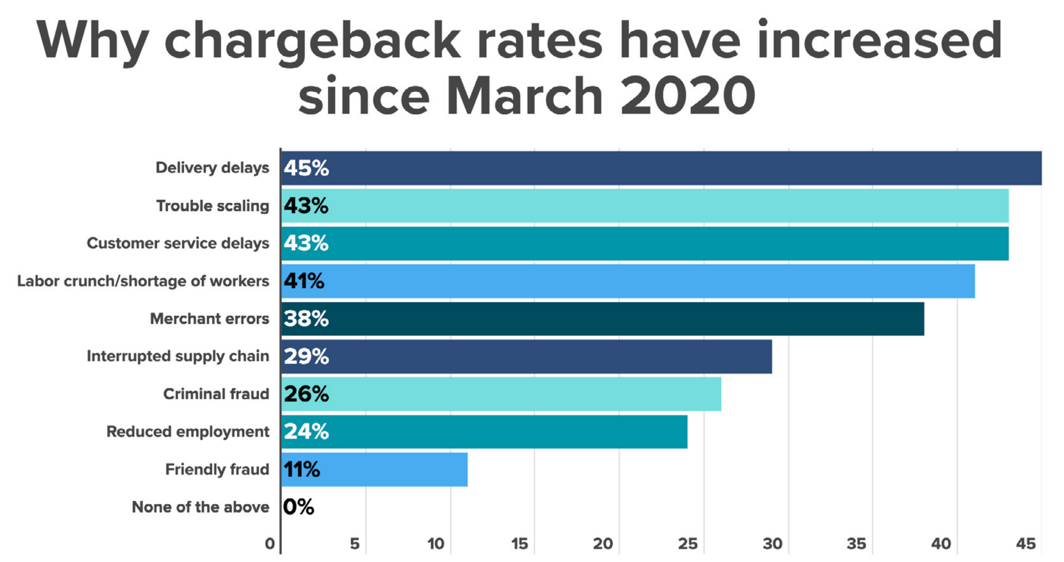
What do you estimate your company's current chargeback rate is?

Kount's survey, "Digital Payments in 2021: Opportunities and Chargeback Risks," takes a deeper dive into 2021 chargeback trends and risks across customer experiences, before and after businesses approve orders.* In it, a sample of 508 U.S. adults that work for companies that process at least 500 online transactions monthly reveal:

- Why their chargeback rates have increased
- Their top chargeback sources and challenges
- How they manage disputes and representments

58% think their company's chargeback rate has increased.

In 2018, Kount and Chargeback 911's "State of Chargebacks" report found that 18% of people surveyed estimated their chargeback rate was between 0.6% and 1%. 13% of respondents estimated their chargeback rate was between 1% and 2%.



Why chargeback rates have increased since March 2020

Kount's "Digital Payments in 2021" survey suggests some companies have experienced big changes. When the survey asked respondents how their company's chargeback rate has changed since March 2020, over half said it increased. Among all respondents, 47% estimate their company's current chargeback rate is between 0.6%-1%. And 33% estimate their company's current chargeback rate exceeds 1%.

Shipping delays are responsible for increased chargeback rates.

The 58% of respondents who think their company's chargeback rates have increased since March 2020 speculate a number of reasons why. 45% of respondents say delivery delays are the top reason for their company's increased chargeback rate. 43% of respondents say trouble scaling and customer service delays, respectively, are top reasons.

However, when the survey opened the question up to all respondents, answers varied. Consistent with those who speculated that delivery delays are responsible for increased chargeback rates, 20% of all respondents also say delivery delays are their company's most frequent chargeback source. 18% say friendly fraud is their company's most frequent source of chargebacks. And 17% say package theft and porch pirates are their company's most frequent source of chargebacks.

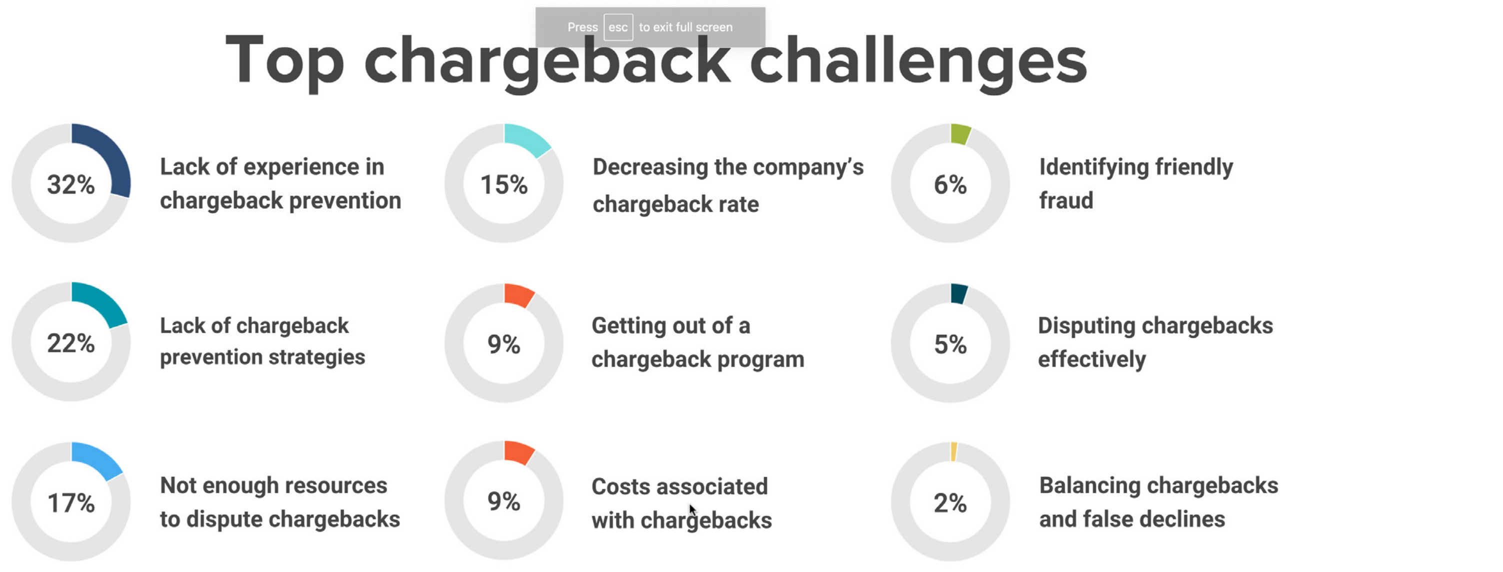
On average, respondents' top chargeback sources, from most to least frequent, are:

1. Friendly/accidental fraud
2. Package theft/porch pirates
3. Shipping or delivery errors
4. Stolen cards/fraudulent purchases
5. Policy or refund abuse
6. Customers forgetting purchases
7. Unclear merchant or billing descriptors

32% say a lack of experience with chargeback prevention is a top chargeback challenge.

The 2018 "State of Chargebacks" report found that business's top chargeback challenges included disputing chargebacks, identifying friendly fraud, and reducing chargeback rates. But the digital payments survey wanted to know if that changed for companies in 2021.

32% of respondents say a lack of experience with chargeback prevention is their company's top



Top chargeback challenges

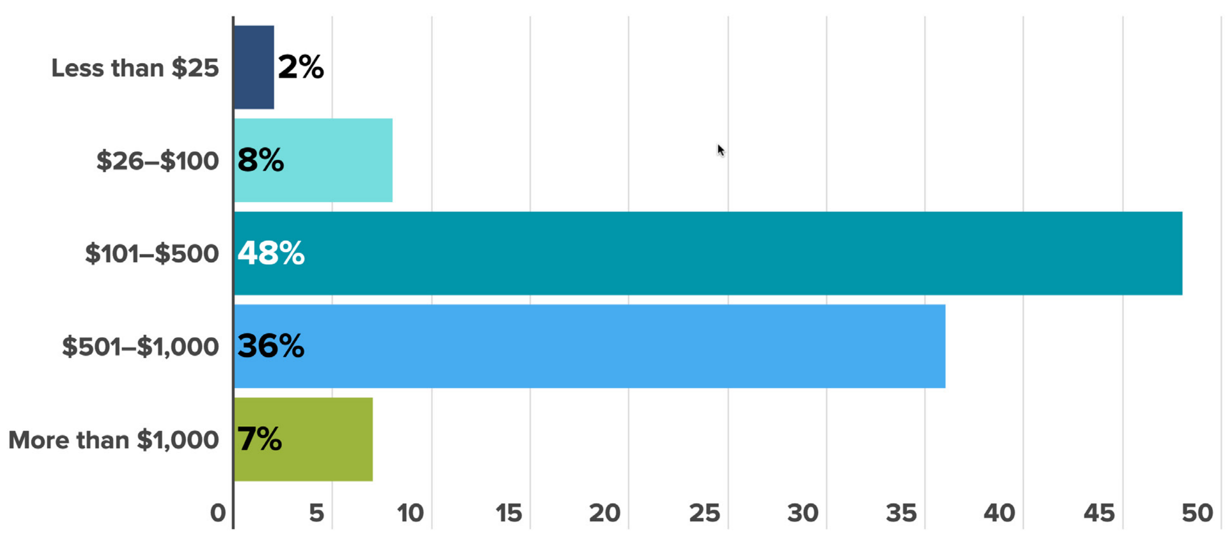
chargeback challenge. 22% of respondents say a lack of chargeback prevention strategies is their company's top chargeback challenge. And 17% of respondents say not enough resources (i.e., time, information, personnel) to dispute chargebacks is their company's top chargeback challenge.

On average, respondents' top chargeback challenges, from most to least challenging, are:

- Lack of experience in chargeback prevention
- Lack of chargeback prevention strategies
- Not enough resources to dispute chargebacks
- Decreasing the company's chargeback rate
- Getting out of a chargeback program
- Costs associated with chargebacks
- Identifying friendly fraud
- Disputing chargebacks effectively
- Balancing chargebacks and false declines

These responses are interesting, given that 84% of respondents say there are at least three people working on their company's fraud prevention teams. And 82% of respondents say at least three people review orders for fraud as their primary job function. This suggests that companies might need to spend more resources on educating fraud teams on dispute and chargeback management to better mitigate their challenges.

Average online transaction values



70% of companies have been in a fraud monitoring program in the last 12 months

Given the surge in demand for online purchasing options, businesses stand to experience greater losses due to chargebacks. 83% of respondents in the digital payments survey say their company's average online transaction value is between $100 and $1,000.

Considering the direct and hidden costs of chargebacks can amount to at least double a transaction's value, these companies risk substantial losses per chargeback. Add that to the fact that 63% of respondents say their companies process between 500 and 1,000 online transactions per month, and losses can quickly top the tens of thousands.

Unfortunately, these higher online transaction values expose companies to greater chargeback risks and consequences, especially fraud monitoring programs. 70% of respondents say their companies have been in a fraud or dispute monitoring program within the last 12 months. And that's not surprising, given respondents' current estimated chargeback rates. If they're not in a program already, the 47% of respondents who say their company's chargeback rate is between 0.6% and 1% are dangerously close.

Businesses that want to reduce chargebacks can do so by engaging in the representment process. But 60% of respondents dispute only some chargebacks — 5% don't dispute chargebacks at all. Reasons businesses don't dispute chargebacks include not having enough time, information, or personnel.

Fraud solutions open opportunities for digital payments, reduce chargebacks, improve customer experiences.

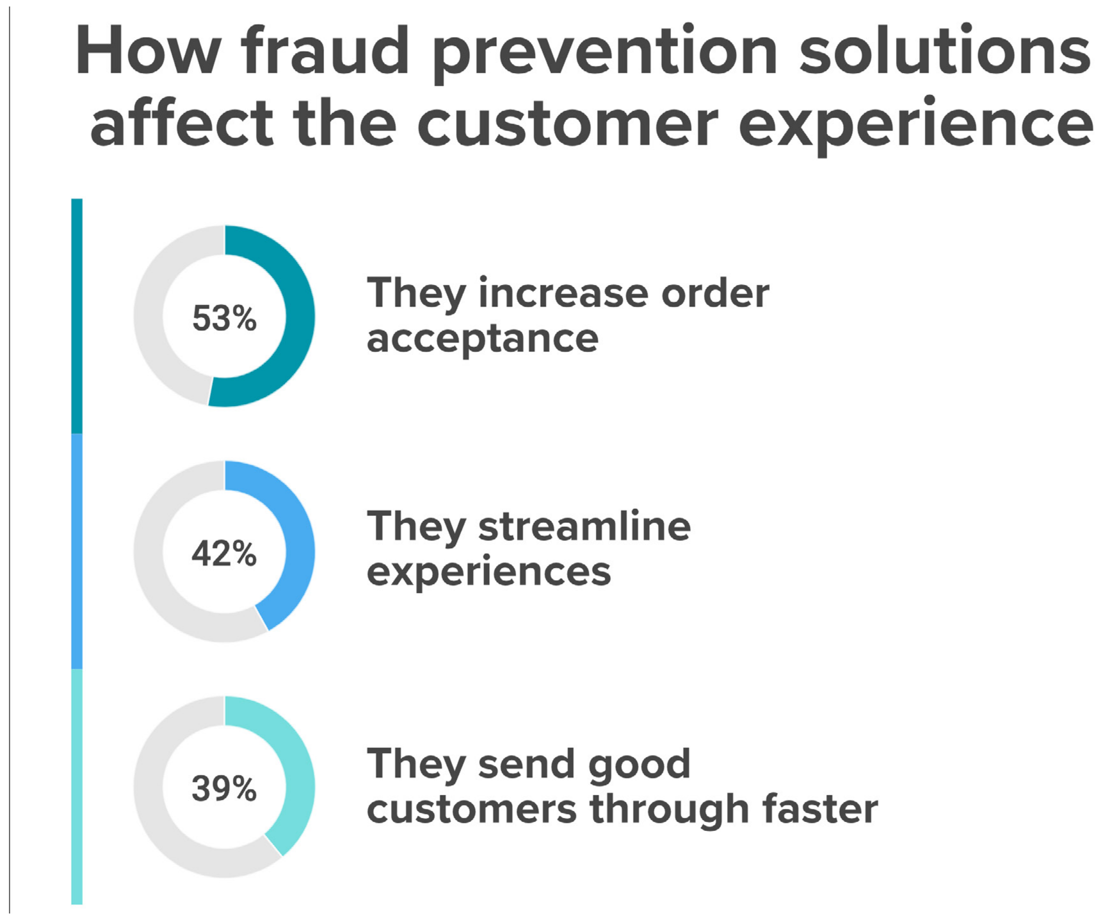
The best way to reduce chargebacks is to reduce fraud pre-authorization and deflect customer disputes with post-authorization tools. When businesses use these solutions in tandem, they stand the best chance of reducing chargebacks.

But, according to Kount's survey, 22% of respondents say their companies don't use a fraud solution. And 15% don't use post-authorization chargeback tools. Considering the widespread adoption of digital payment methods, these companies expose themselves and their customers to fraud. And they miss opportunities to resolve customer disputes before they become chargebacks.

Fraud prevention solutions don't just mitigate fraud and chargeback challenges.

They can also make it easier for businesses to adopt new digital payment methods with confidence. And they can automate decisions to accept more good orders and decline high-risk transactions.

Automation could eliminate manual reviews for businesses that have fraud teams but lack experience in chargeback prevention. Spending less time on manual fraud processes can free up workers to address challenges like scaling, merchant errors, and customer service delays.



Plus, the right solutions can prevent fraud without affecting customer experiences. Not only will they not slow down identity verification or authorization decisions, but they won't create false positives and false declines.

In fact, among respondents who use a fraud prevention solution, over half (53%) agree that it improves the customer experience by increasing order acceptance. 42% agree that it can streamline customer experiences, and 39% say it can send good customers through the purchasing process faster. ■

Consumer Trust is Key in Digital Banking

AS THE BANKING INDUSTRY accelerates digital innovations for better efficiencies, online fraud continues to chip away at consumer trust. Modern conveniences in digital banking, digital payments and online account activities are on the rise, but there remain opportunities for financial organizations to strengthen trust and connectivity as the global marketplace moves toward being more consumer-centric.

It starts with banks leveraging the right consumer data at the right time to make the right decisions.

"A lot of the challenges are a direct result of banks' inability to take consumer data that they have or should have and leverage it to make a friction-free environment for customers," said Brad Wiskirchen, senior vice president and general manager of Kount, an Equifax company. "So, the result is a lack of trust by the end consumer not being able to get transactions authorized. That increased friction results in, for example, the bank's cards being pushed to the back of the wallet and other cards moving up front."

Speed of data

What's critical in this era of greater consumer control and convenience, is banks and other institutions having speed of data to meet increased, complex demands.

"Sometimes financial institutions can have information, but don't have it accessible in real time," said Mark Luber, chief product officer at Equifax. "Lack of current, actionable data can look like an institution is out of touch, unaware of important life changes for their customers, or where that consumer is at any moment in time. Speed of data matters because, of course, for the person everything happens in real time, and we have to get the data to match those experiences to optimize consumer trust."

Establishing digital trust

With the evolution of the Internet of Things (IoT), a singular security breach can negatively impact client trust. "A recent consumer survey showed that cyber attacks and fraud are the No. 2 reason why customers would leave their bank, so it is a major concern," said Luber.

"Increasing digital security with leading technologies, and being transparent with customers help build relationships," he said. It's not only the threat of financial loss that keeps executives up at night when it comes to cyber attacks; it's also risks to brand reputation and consumer loyalty.

When consumers share personal information with banks through online channels, the expectation is that data will be secure, and used primarily for making daily routines and transactions more personal, easier and faster. Deviance from security protocols, such as not verifying login credentials on an unknown system, could be considered a violation of digital trust.

Find the right balance

Kount recently sponsored a study by Javelin Research, showing that 42% of businesses think digital fraud slows innovation and expansion. As banks, in particular, invest in features and functionality, many times those innovations can run ahead of their ability to manage fraud, which can result in financial loss, said Wiskirchen. On the other hand, an overly cautious approach with too much concentration on risk avoidance can lead to innovation stagnation that can drive customer attrition.

"You've got to find the right balance," said Wiskirchen. "Retailers have historically done a better job of finding that balance, and financial institutions can learn from retailers and e-commerce participants. The right balance is bringing together the e-commerce teams, the revenue-generation teams and the fraud-control teams right out of the chute."

Leverage key data solutions

What's the best way to build digital trust? There's not an easy answer, but when done the right way, banks can strengthen relationships with consumers while still protecting the business and clients from potential risks. Converging new technologies and digital transformation with streamlined, personal customer engagement must remain top of mind.

Like any relationship, building trust has to be a two-way street - banks must be able to trust that consumer data provided is factual and up-to-date. For their part, financial centers must leverage the right data solutions, such as Kount's Identity Trust Global Network™, to make sound decisions with better confidence. Customized data solutions can help banks create access to credit for their customers, enable financial equity and inclusion, and build consumer trust. ■

Source: Consumer Trust is Key in Digital Banking

Learn more about Kount's Identity Trust Global Network

Our experts are leading

Conversations

around identity and fraud

Meet us at

Gartner Identity & Access Management Summit
March 14, 2022