

2021 Global Identity and Fraud Report

Protecting and enabling customer engagements
in the new digital era



The surge in digital demand over the past year reinforced the deep connection between recognition, fraud prevention and the online customer experience. As businesses transformed their operations to accommodate the rapidly growing volume of digital transactions, consumer expectations for easy, secure interactions increased at an even faster pace. And that meant less tolerance for the interruptions caused by security and risk controls.

Our 2021 Global Identity and Fraud Report highlights these shifts and more, drawing on three waves of data collected throughout the pandemic. The business and consumer surveys took place in waves from June 2020 to January 2021 across 10 countries spanning North America, Latin America, Europe, and Asia-Pacific. The breadth of data reveals notable changes in consumer and business behaviour and priorities as each navigated the crisis.

One of the many heartening discoveries included the fact that eight in ten businesses said that they now have a customer recognition strategy in place, up 26% since the start of the pandemic. Many companies also developed digital strategies as they strove to improve their online experience and provide security and fraud prevention measures when customers needed it most.

When it comes to fraud prevention, companies are continuing to invest in securing online experiences. This is an encouraging trend, especially given that we anticipate fraud attacks will increase significantly in the near-term. Dive into this year's report for insights and detail into:

1

Business priorities for 2021 and the current disconnect between the support companies say they provide and what consumers report

2

Why the digital experience remains siloed from security and fraud prevention

3

Changes in consumer preferences regarding security methods and the right approach going forward

4

The normalisation of pandemic-era digital activities and how they've changed consumer expectations

Our report also provides five key pieces of guidance, outlining how companies can implement a continuous authentication strategy that significantly improves the customer experience while also reducing their fraud risk.

“Sixty percent of consumers globally have higher expectations for their online experience, while 55% are saying security is their top priority. You have a challenge because you want this environment to be as easy and convenient as possible, but consumers also want this vetting to be done.”

- Eric Haller, EVP and General Manager
Global Identity & Fraud, and DataLabs



Businesses invested in digital strategies, but customers need and want even more support



Consumers flooded online channels over the past year, including many who were “digital newbies.” For example, the percentage of consumers over age 40 who reported using online banking increased from 33% pre-Covid to 38% in January 2021. The same demographic also witnessed a 10-percentage point increase in online food and grocery ordering over the same period.

Businesses moved mountains to meet the growing need. Consider that nine out of ten businesses said they have a digital customer journey strategy, and nearly half (47%) implemented it during the pandemic. Financial service companies launched online customer support to address repayment concerns. Businesses everywhere began utilising online and contactless forms of payment. And customer recognition strategies became essential, with 82% of companies saying they now have one in place.

Yet, despite the effort there's still a disconnect between digital initiatives across the business and the resulting customer experience. This is a continuation of a trend we reported in 2019, when 95% of businesses said they solved the recognition problem, but 55% of customers said they still didn't feel recognised.

In our most recent survey, 50% of companies said they increased customer support; yet only about one in four consumers said that they've received quicker responses from customer service and that they were able to connect with customer service if they got stuck online. These figures held around the globe, and were in fact lower in the U.K.

Businesses responded to the heightened volume as best they could at the time. But now with the pandemic crisis abating, they appear to be homing in on the issue. In 2021, businesses cited one of their top priorities as improving support for digital operations and digital customer service. This was especially true across the four countries surveyed in the Asia-Pacific region. Brazil, and the U.S., where nearly 40% of businesses reported increasing support for digital as their number one concern. In the U.S., 39% of companies noted that adding support meant specifically hiring more people in call centres. Those figures may reflect a shift to pre-pandemic norms of in-person staff or a strategic move to augment digital processes with people.

The latter merits additional scrutiny. Certainly, some tasks require humans—the times at which customers truly need a compassionate voice and some extra help. Many other tasks, however, are an ideal fit for AI and machine learning solutions. The rise of truly intelligent bots can help improve and scale customer support in ways humans can't. Companies need to be exceptionally strategic about how they combine humans with technology to ensure they're not just kicking operational bottlenecks and costs down the road. What's more, poorly implemented AI can exacerbate customer service problems and ultimately hinder revenue growth.

Businesses look ahead

Top priorities for businesses globally this year

	Global	Australia	Brazil	France	Germany	India	Japan	Singapore	Spain	U.K.	U.S.
Net: Investing in advanced analytics and artificial intelligence	52%	53%	60%	52%	41%	60%	58%	54%	46%	44%	54%
Net: Investing in fraud detection software and methods	47%	52%	66%	50%	52%	53%	36%	44%	37%	43%	40%
Increasing internal staff/support for digital operations	33%	30%	37%	31%	23%	49%	36%	36%	29%	30%	36%
Investing in digital decisioning software	30%	26%	34%	26%	22%	30%	29%	37%	26%	23%	39%
Increasing call centre support staff	27%	22%	26%	23%	20%	42%	17%	26%	26%	30%	39%
Increasing in-branch personnel	23%	21%	19%	20%	21%	24%	20%	26%	23%	23%	31%
Resolving legacy technology issues	23%	22%	23%	21%	19%	30%	26%	23%	27%	22%	21%

Business survey. In thinking about your organisation's priorities for 2021, where do you intend to direct any financial resources in the area of improving digital customer service? Check all that apply.

Key takeaway: Everything centres around various ways to improve the customer experience

As we reviewed the business priorities in the coming year, we found some common themes. Broadly, businesses are looking for ways to automate more of their decisions. You can see this in the focus on AI and decisioning software. But they also want to sustain the staff to provide that high-touch when customers need it, whether that's across digital operations, in-branch or at call centres. Finally, fraud prevention remains a concern and a priority as companies look to increase investment in software and other detection methods.

Behind regional differences



Throughout our study, there were marked differences in the behaviour and expectations of consumers and businesses across different countries. For instance, throughout the four markets surveyed in Asia Pacific, businesses reported that they are putting less attention on most digital initiatives, with declines over the year that outpaced other regions. This may reflect a recalibration of risk and priorities as companies gather increasing amounts of new data about their customers.

Meanwhile, as Brazilian companies cited investment in fraud detection software as one of their top priorities, it fell to the bottom for businesses in the U.K. U.K. businesses are prioritising investment in fraud detection methods, which suggests they're aiming to optimise the investments they've already made in software.

In the U.S., most companies said they planned to hire more people to support digital operations—a departure from other regions. On the consumer side, 44% of U.S. consumers said they were worried about their online privacy compared to 23% of Europeans.

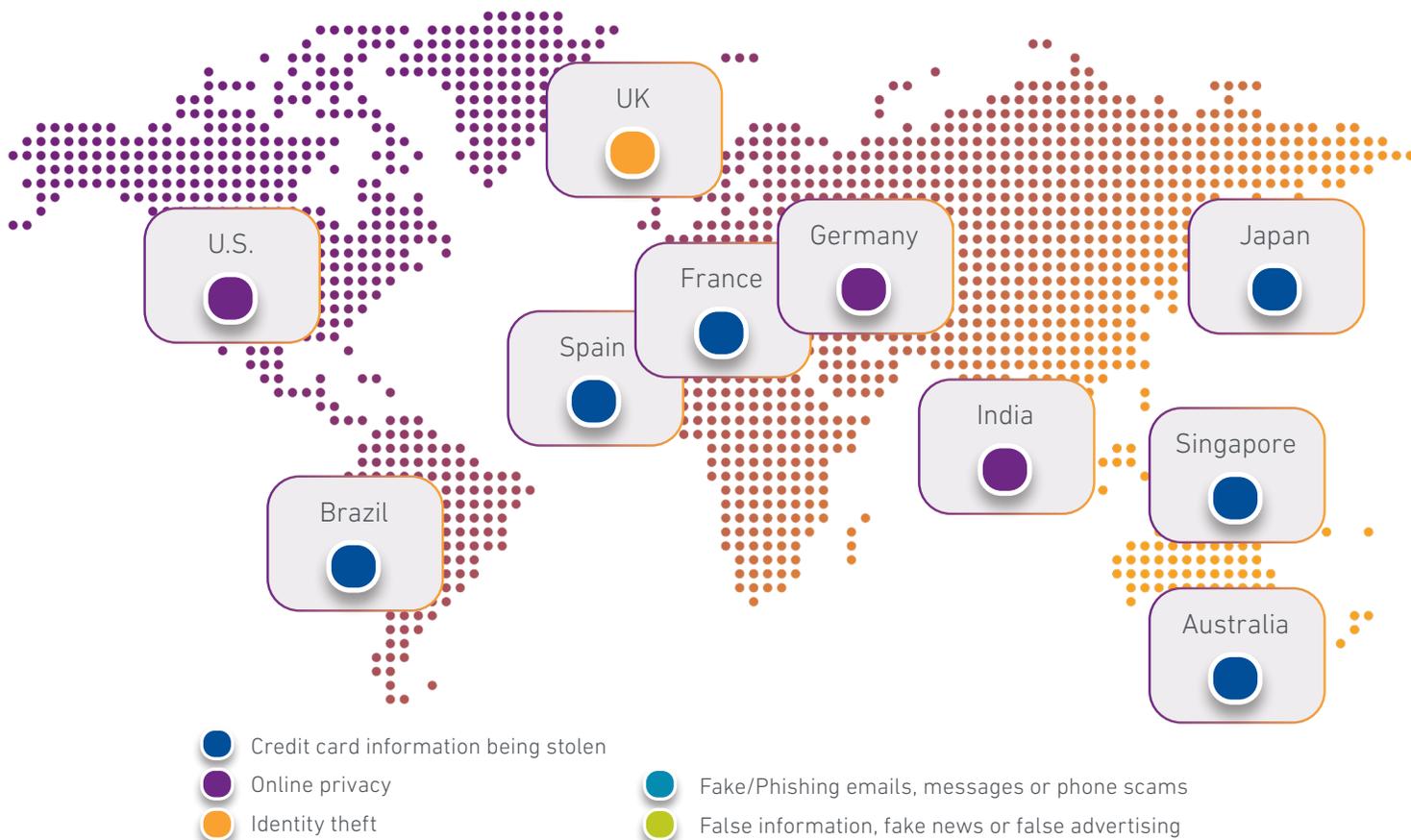
There are a few key drivers of these differences. The varied business priorities across countries likely reflect prior investment in fraud prevention as well as the maturity of existing initiatives. And the consumer privacy concerns correlate with local regulations—consumers in countries with more robust privacy laws are less worried than those in areas that don't have them.

It's important to understand the nuances of each market. However, broadly speaking, we're also seeing more similarities and patterns as countries learn and adopt best practices and policies from each other and the digital experience evolves.

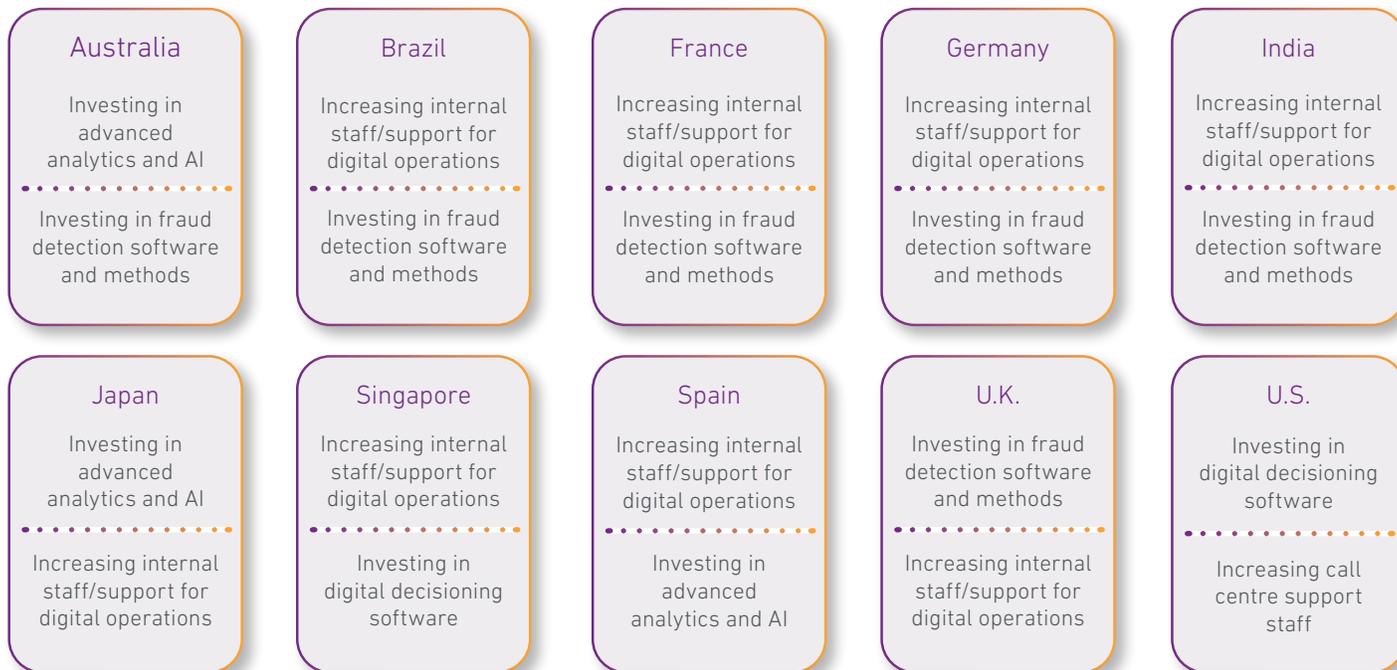
“Businesses are spending the same on fraud management now as they did pre-pandemic. With the increase in threats, the key will be to balance revenue generation and fraud prevention rather than prioritising one over the other. Striking that balance will ensure both a top-notch customer digital experience and accurate customer recognition as part of their fraud prevention programme.”

- Steve Griffiths, Managing Director of Decision Analytics, Operations & Transformation
Experian Asia-Pacific

Consumer concerns vary by country...



...and so do business priorities



Security and fraud prevention remain a focus

Even as businesses prioritise the customer experience and support, they are still sustaining pre-pandemic levels of investment in mobile security and fraud management. Throughout the course of our research, the intention of businesses to increase fraud management budgets fluctuated. From a high in June 2020 back to pre-pandemic levels in January 2021, there was a 6-percentage point decline in business intention to increase fraud management. The four markets surveyed in the Asia-Pacific region reported the most significant change, with a 16 percent point drop in companies saying they'd increase their fraud management budgets. These results suggest that businesses may still not realise that the same data and tools they can use to improve security and fraud detection also enhance the customer experience.

Now is the time to continue investing in fraud management. During the pandemic, many fraudsters found new opportunities in exploiting government-based pandemic assistance programs. For example, according to conservative estimates, at least \$36 billion of the \$360 billion in U.S. CARES Act unemployment benefits was lost, primarily due to fraudulent claims.¹ In the U.K., as much as \$35 billion in Covid-related loans may have been fraudulent.² As those programs wind down, we expect criminals will turn their focus to traditional digital fraud schemes, taking advantage of the increase in digital traffic to exploit data stolen over the past three years.

We're already seeing an increase in account takeover attacks, which entail fraudsters using compromised usernames and passwords to commandeer consumer accounts.

If companies want to continue to meet customer expectations, they need to maintain their focus on fraud prevention even as they prioritise the digital experience. We caution companies against viewing fraud prevention and the customer experience as separate efforts. While that may reflect your organisational structure, it's not necessarily how customers experience your business. For example, marketing is focused on attracting new customers. Security is concerned with mitigating risk, and fraud prevention teams are responsible for reducing fraudulent transactions. Their goals may not align. Yet, customers and fraudsters don't operate in silos. They switch devices and channels often, and fraudsters frankly exploit disconnects between the two.

Your digital customer experience may be top-notch. But if you're not accurately recognising customers as part of a fraud prevention program—or worse, if you're errantly enabling fraudsters by believing they're legitimate customers—then your efforts are ineffective. And while the primary damage is financial loss, the collateral damage is customer trust.

¹ <https://www.cnn.com/2021/01/05/scammers-have-taken-36-billion-in-fraudulent-unemployment-payments-.html>

² <https://www.pymnts.com/news/security-and-risk/2020/report-an-estimated-26-billion-in-uk-covid-loans-might-be-fraudulent/>

Companies continue to increase investment in fraud prevention

Despite increasing investments to make the shift to digital, businesses are continuing to increase their budgets in fraud prevention



“Fraud has become more complex and it’s critical to anticipate future fraud risks. In our increasingly digital world, now is the time for companies to adopt targeted verification strategies using data, technology, and advanced analytics to keep up with the rapid pace of fraudsters”

- Kathleen Peters, Chief Innovation Officer
Experian Decision Analytics, North America

Consumers are increasingly ready for invisible means of security

One of our most significant findings was the increasing comfort and preference that consumers have for physical and behaviour-based—or invisible—methods of security. Consumers ranked the following methods based on their perceived security:

- 1) 74% of consumers said physical biometrics: Mostly applicable to mobile devices and include facial recognition and fingerprints
- 2) 72% of consumers said PIN codes sent to mobile devices: Requires the use of two devices, each connected to the users' account.
- 3) 66% of consumers said behavioural analytics: Leverages passively observed signals across browsers and mobile devices, requiring no effort from the consumer.

Notably, passwords didn't earn a spot in the top three most secure methods for authenticated customer identity, even though nearly every digital account and device includes some sort of password protection.

This indicates a new shift in consumer thinking that moves away from the realm of the password. The methods consumers deemed least secure: personal information, account usernames and social media accounts.

Even as their preferences evolve, consumers still prioritise security and privacy. In fact, global concern among consumers regarding many types of fraudulent activity remains at levels higher than before the pandemic. For instance, 34% of consumers said they were worried about online privacy in January 2021 compared to 29% before Covid-19. Thirty three percent said they're concerned about identity theft, up from 28% pre-pandemic. In Europe, consumers also cited concerns about government requirements for tracking related to contact tracing and pandemic management.

However, the data shows that consumers are more willing to have businesses manage their security and privacy without their overt involvement. Historically businesses have used authentication methods that relied on customer action, such as memorising passwords, answering questions, and receiving one-time passcodes (OTPs). Consumers used to think that those methods constituted robust security, though in reality, they're extremely brittle. Passwords can be stolen or forgotten and OTPs can be intercepted.



In these cases, bad actors can easily present themselves as another person, providing businesses with a false sense of their security's effectiveness.

Given the shift in consumer preferences, businesses have the opportunity for a new approach to security, layering visible and invisible methods. By leveraging data and observations garnered throughout the customer journey, companies can facilitate accurate recognition and authentication at each discrete decision. The same insights that companies use to improve the customer experience power that continuous authentication—and reduce friction across the customer's journey.

Companies that meet consumer expectations in this new era of secure digital experiences stand to benefit. For example, consumers consistently said they'd abandon a transaction if they had to wait more than 30 seconds. This highlights the importance of keeping fraud checks fast and seamless. Improving security can also improve loyalty and trust. Consumers reported that they had enhanced opinions of companies that implemented physical and behavioural biometrics, and those that send PIN codes to devices. The percentage of consumers saying so increased from June 2020 to January 2021.

“There's an opportunity for companies to more freely adopt invisible security solutions without having to play the 'theatre of security' game, which can reduce friction and increase customer satisfaction.”

- David Britton, Vice President of Industry Solutions
Experian Global Identity & Fraud



Consumers want businesses to do more when it comes to privacy and security

Use more security steps while online

55%

60% in APAC

Provide more information on how data is used and stored

51%

Have more visible security measures in place online

49%

Implement strong, invisible security measures

47%

59% in the U.S.
60% in the U.K.

Provide more information about why they're requesting personal information

45%

“Businesses more than ever need to balance fraud prevention and a smooth customer experience. Fortunately, many of the necessary checks can be carried out invisibly and in real-time while onboarding the customer. For example, running consistency checks on their device or behavioural biometric assessment of the customer.”

- James Brodhurst, Head of Experian Identity & Fraud Practice
Europe, Middle East and Africa

The credit card misconception

In our research, 44% of consumers said they were most concerned about protecting credit cards and bank account details. Only 23% were concerned about protecting personal data such as their date of birth, address, and social security numbers.

Personal data poses inherently more risk, enabling fraudsters to steal identities and take over existing accounts.

Credit cards, meanwhile, offer some of the most robust protections regarding fraudulent use.

The misconception around credit card vulnerability presents an opportunity for financial service organisations to educate consumers about the benefits of credit card transactions.

Such information may prove especially timely as consumers are increasingly interested in non-credit based forms of online payments such as peer-to-peer payments, which provide much less protection.



Consumers moved rapidly online—and they're here to stay

The explosion of digital demand introduced new consumers to online services and accelerated digital transformation across companies and industries. Now for many the question is: What happens next? The needs of consumers throughout the crisis are giving way to a new, more permanent way of living and working digitally. It's one that businesses need to support.

Our analysis revealed an increased use of digital services at the start of the pandemic, a spike in September 2020, and then a leveling out (though at higher than pre-pandemic demand). For example, ordering food and groceries online has declined slightly since September, but the activity remains 20% higher than before the crisis. The purchase of clothing, electronics, and beauty and wellness products is also on an upward trend.

Regardless of the activity, consumer expectations for their digital experience remain high.

For example, throughout our study, the percentage of consumers who said they're remaining loyal toward online brands and service providers dipped from 66% to 63%. In the four markets surveyed in Asia Pacific, the figures went from a high of 70% to 60%.

The shifting loyalty suggests that we're at a unique moment in which companies may capture consumer attention, and just as quickly lose it. Related, the percentage of consumers who said they're tolerant of online service delays and digital inconveniences also dipped by 5 percentage points over the three waves.

The research surfaces an imperative to provide convenient and seamless recognition and authentication throughout the digital experience. That means consumers can access their accounts across devices, be consistently recognised at each point and not have to authenticate themselves multiple times during their experience.

For companies, the time to act on this is now—the pandemic revealed that organisations that invested in digital experience and fraud prevention fared better than those who restricted their investments. We may not be able to predict the next crisis. But the companies that prioritise functionality across all aspects of the digital channels will be ready to respond to the next wave of consumer demand and will continue to meet rising expectations.

“With the acceleration of the adoption of digital channels in consumers' lives, companies have no alternative but to invest in new methods of fraud detection and increasingly sophisticated technologies throughout the customer journey so that the security of the operation does not affect their seamless experience.”

- Jaison Reis, Head of Identity & Fraud Product Management
Serasa Experian

The rise of mobile wallets

The increase in mobile wallet usage is part of our “new normal.” At the height of the pandemic, 64% of global consumers said they used mobile wallets. That dipped to 60%, but remains well above the 53% that reported using mobile wallets before Covid-19. Usage is especially high in Brazil, with 70% of consumers reporting that they used mobile wallets, a 19-percentage point increase since June 2020. While it’s likely that mobile wallet use in Brazil is concentrated to metropolitan areas, it highlights its growth due to the mass

adoption of smart phones by the Brazilian population. Mobile wallets offer distinct benefits that are particularly relevant now:

- They provide a contactless way to pay, reducing the need to touch or Point-of-Sale device or hand a card to a cashier.
- Payment data is encrypted into the device and merchants only receive tokenised data.
- The device usually needs to be unlocked by a physical biometric, furthering improving the safety of the payment method.

Consumer preference for universal mobile wallets as a payment method:

	Global	Australia	Brazil	France	Germany	India	Japan	Singapore	Spain	U.K.	U.S.
Prior to Covid-19 (before June 2020)	53%	48%	51%	47%	59%	70%	34%	68%	54%	53%	49%
Since Covid-19 (as of January 2021)	60%	44%	70%	46%	72%	84%	37%	78%	61%	54%	53%

Consumer preference for universal mobile wallets as a payment method by age:

January 2021	Global	Australia	Brazil	France	Germany	India	Japan	Singapore	Spain	U.K.	U.S.
Under 40 years old	66%	55%	65%	48%	70%	87%	43%	85%	60%	59%	58%
Over 40 years old	56%	37%	54%	45%	73%	80%	35%	73%	62%	51%	50%

In the minds of pandemic-era digital customers

Consumers surveyed in January 2021 showed less loyalty to current online service providers, less tolerance of online service delays, and less trust of online businesses compared to the previous June. They also felt more concerned about fraud.

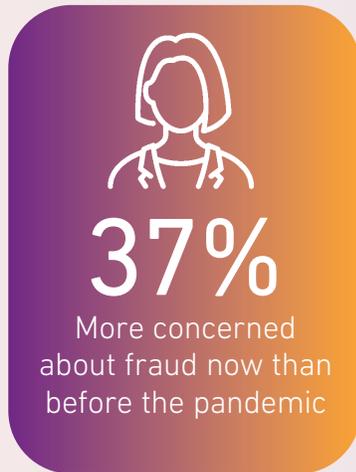
	June 2020	September 2020	January 2021	Six-month change
I'm more tolerant with online service delays/ inconvenience I encounter	48%	48%	43%	-5%
I'm staying with the same online businesses now	66%	67%	63%	-3%
The businesses I prefer to deal with have not adapted so I've taken my business elsewhere	25%	26%	22%	-3%
I'm more trusting of online businesses with they demonstrate signs of security	44%	46%	43%	-1%
I increased the number/types of businesses I visit online	41%	42%	40%	-1%
I feel safer sharing my personal information	25%	28%	25%	0%
I feel safer that businesses have put in more complex security procedures	46%	51%	47%	1%
I feel safer using biometric security features	40%	45%	41%	1%
I believe businesses have put more security in place	41%	48%	42%	1%
I'm now more of a target of online fraud	39%	43%	42%	3%
I like to know what my data is being requested for more now	50%	57%	53%	3%

Consumer survey. When thinking about ways that you engage and interact currently with businesses online (e.g. sign-up or check your accounts, buy or apply for things online), to what extent do you agree or disagree with the following.

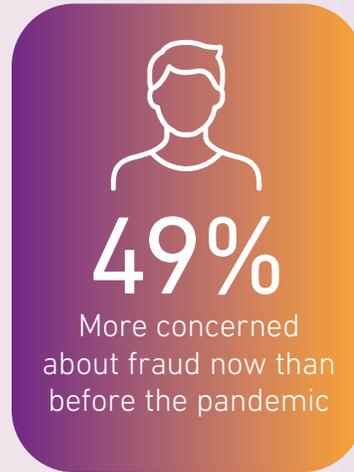
Fraud concerns and age

Younger consumers remain more concerned about fraud, which may explain why they're also more likely to use biometric security features.

Older than 40



Younger than 40



“Its critical businesses are confident in who they are dealing with and protect their customers by identifying suspicious activity not only at the point of log-in but throughout all points of the digital journey.”

- Eduardo Castro, Head of Experian Identity & Fraud United Kingdom

Consumer authentication and fraud prevention are foundational to the digital experience

As the digital experience becomes an increasingly important component of consumer lives, continuous authentication needs to underpin everything. In a not so distant future, companies will recognise consumers across every interaction in a way that replicates human interaction in the physical world. For example, humans use senses to develop highly complex profiles that connect sounds, smells, speaking styles, appearances, and behaviours with specific individuals.

Our digital world is in the early stages of modeling these interactions, transforming recognition and authentication from a chore that relies on consumers doing “something” to something that happens automatically. Here are five tips for creating a digital strategy with continuous authentication as the foundation:

1) Eliminate silos to create secure, seamless, end-to-end customer experiences.

Organisational silos are contributing to a fractured system that delivers disjointed customer experiences. Customers don't think of fraud prevention or recognition as separate from their account onboarding or payment transaction. Companies need to think holistically about their digital experience, using insights at every interaction to build customer profiles that lead to greater interaction and reduced friction.

2) Layer security methods to meet consumer expectations.

Utilise a combination of security methods—visible and invisible—to meet evolving consumer expectations regarding recognition and security. A layered approach also includes data from consumer observations and activities.

The right formula will differ by companies and transaction value; however, it should include an advanced mix of recognition, authentication capabilities and sophisticated analytics to achieve the best results.

3) Blend AI and ML tools with your high-performing processes.

To adopt layered security and build end-to-end experiences, businesses need to leverage more advanced technologies. AI and ML tools help make sense of the data, automate processes, and scale the digital experience. But they're not a wholesale replacement for people. Instead, take a strategic approach to AI and ML solutions, blending them with your well-performing processes to add value and improve the customer experience.

4) Double-down on identity recognition to improve decision making and customer trust

Last year, we reported that accurate recognition was critical for improved customer engagement and mutual trust. The pandemic put this concept to the test, showing that consumers are more trusting of businesses that show signs of fraud prevention and security. Effective customer recognition is the start of that trust and the lynch pin in fighting fraud.

5) Look to other countries for innovative solutions and new paths to success.

Too often we find that countries tend to think of themselves as standalone markets when it comes fraud and consumer expectations of digital experiences and support. While there are nuanced differences, companies in different countries can also learn from each. Look across borders for approaches that are succeeding and consider how you can incorporate those successes into your own digital customer experience.

Winners of a new era



In the face of a global crisis, businesses more than rose to the occasion, transforming how they digitally engage with customers. The silver lining of a challenging year has been a deeper understanding of consumers' digital needs and expectations, pending opportunities, and potential risks.

Going forward, businesses need to find ways to continually improve the customer experience, while protecting consumer identities and information. The winners of this next era will be those that incorporate continuous authentication and advanced recognition into a digital strategy that considers the complete customer journey.

For additional identity and fraud prevention research and trends, visit the [Experian's Global Insights blog](#)

Survey respondents and methodology

Survey fielded:

June 20-July 7, 2020
September 16-30, 2020
January 2-24, 2021

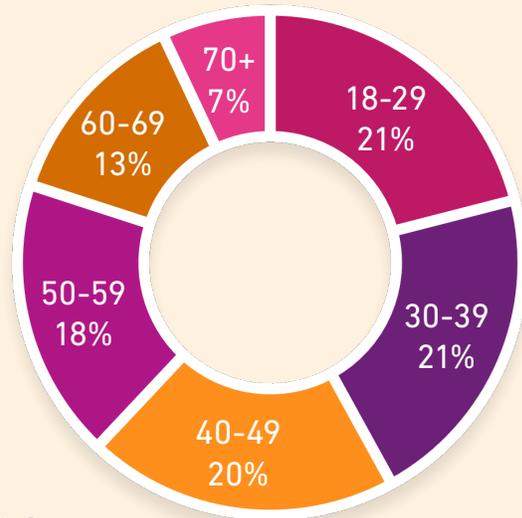
Respondent base:

Includes samples from Australia, Brazil, Germany, France, India, Japan, Singapore, Spain, United Kingdom and the United States

Includes representation from the following business functions: credit risk, fraud risk, customer experience, information technology, innovation, product and marketing

9,000

Consumers age 18-70 years old and older with at least one online account.



2,700

Business executives from North America, Latin America, Europe, Middle East and Africa, and Asia Pacific.

Enterprise 40%

Mid-market 44%

SMB 16%



Retail banking and cards



E-commerce



FinTech



Telco and utilities



Insurance

Effective fraud prevention does more than stop fraud

Without a doubt, your fraud prevention efforts are aimed at stopping fraud and reducing losses. But, an effective program also makes it easier for your good customers to do business with you. So how do you achieve both? It starts with moving away from a one-size-fits-all approach. Instead, you should apply the right level of protection needed for each and every transaction.

Most consumers aren't aware of what's happening behind the scenes to keep them safe as they do everyday things... like shop online or check bank balances from a mobile device. We're proud of the fact that we helped our clients screen more than 15 billion fraud events this past year. That's over 3,300 events per second.

With more than 300 fraud specialists around the world, Experian continually invests in its technologies and platforms to help our clients build a layered approach to fraud. Access to this expertise along with a range of best-in-class industry solutions, flexible workflow and integrated orchestration are critical requirements in the modern age of solving identity and fraud challenges. It means developing strategies that may introduce friction only when it's not possible to re-recognise consumers from their digital footprint. We call that hassle-free, and that's how it should be. Our solutions are built using data, technology and analytics to stop fraudsters without stopping good customers. Now, fraud prevention contributes to growth and a positive experience.

Contact us

Corporate headquarters

Experian plc
Newenham House
Northern Cross
Malahide Road
Dublin 17
D17 AY61
Ireland
T +353 (0) 1 846 9100
F +353 (0) 1 846 9150

Operational headquarters

Experian
The Sir John Peace Building
Experian Way
NG2 Business Park
Nottingham
NG80 1ZZ
United Kingdom
T +44 (0) 115 941 0888
F +44 (0) 115 828 6341

Serasa Experian
São Paulo
Avenida das Nações Unidas,
14.401 Torre Sucupira –
24º andar
Chácara Santo Antônio,
São Paulo, SP
CEP: 04794-000
T +55 11 3373 7272

Corporate office

Experian
Cardinal Place
80 Victoria Street
London
SW1E 5JL
United Kingdom
T +44 (0) 20 304 24200
F +44 (0) 20 304 24250

Experian
475 Anton Boulevard
Costa Mesa
CA 92626
United States
T +1 714 830 7000
F +1 714 830 2449

