2020 Global Identity and Fraud Report

Challenging businesses to think differently about customer engagement

experian™

Challenging businesses to think differently about customer engagement

Businesses often talk about creating the ultimate digital experience for customers, but far less about the interrelationship between security, convenience and personalisation. This has resulted in siloed security measures at major decision points in traditional customer lifecycles – when customers sign up, return and log in, and transact within those accounts. It's a disconnect that's perpetuated through equally isolated CRM systems that strive to identify customer preferences, but largely fail to achieve this in cohesive, consistent and appealing ways. Customers can therefore find themselves dragged into a maze of security and risk requests, while being up-sold or cross-sold products and services that they don't necessarily need or want. In short, they often experience the antithesis of convenience.

Experian's 2020 Global Identity & Fraud Report explores inconsistencies between businesses' views of their ability to meet their customers' needs, and customer experiences with those businesses. It also underscores the opportunity for companies like yours to differentiate from the competition through the ways you engage with customers, with emphasis on how you identify and recognise them each time they interact with your business. Experian appreciates that many companies find it challenging to evolve traditional business models in order to meet the expectations of 'always-on' customers. But we also believe that customers' identity verification and ongoing recognition (re-recognition) can be driving forces for greatly improved and more profitable customer relationships.

Input from over 6,500 consumers and 650 businesses worldwide has underlined the complex relationship that people and businesses have with identity. Our research shows that the desire for a better experience, and concerns around security, still shape the digital relationship between consumers and businesses, while the challenge of identity finds its way into every customer decision. The data indicates that businesses are beginning to get a handle on regulatory compliance for privacy and security, so they're shifting their focus to personalised customer experiences. In fact, over half of the businesses surveyed are prioritising the creation of targeted products and offers, while collecting more personal information to do so.

At the same time, most consumers seem to be aware of the changes businesses are making to improve their experiences. However, two thirds of them said security is still the most important factor when deciding to engage a business, followed closely by ease of access to their accounts.

Notably, that sentiment hasn't changed across the past four years of our study, sending a clear message to business leaders worldwide: there's a great opportunity to achieve customer-centricity by understanding and addressing consumers' top priority – security.

Last year we revealed that 70 percent of consumers would be willing to give more personal information for a perceived value such as increased security, improved convenience or personalisation[1]. Yet this year's study shows that regardless of the amount of data captured and stored by businesses to identify their customers – whether for protection, accessibility or experience – more than 50 percent customers still don't feel recognised. What's more, 57 percent of businesses are reporting higher losses associated with account opening and account takeover fraud in the past 12 months, compared to 55 percent in 2018 and 51 percent in 2017. Considering this data, one might wonder: how can 95 percent of businesses claim to be confident in their ability to identify and re-recognise their customers?

Expectation for customer engagement

Identity is the foundation for providing security, convenience and personalisation that enables you to engage your customers in a meaningful way.

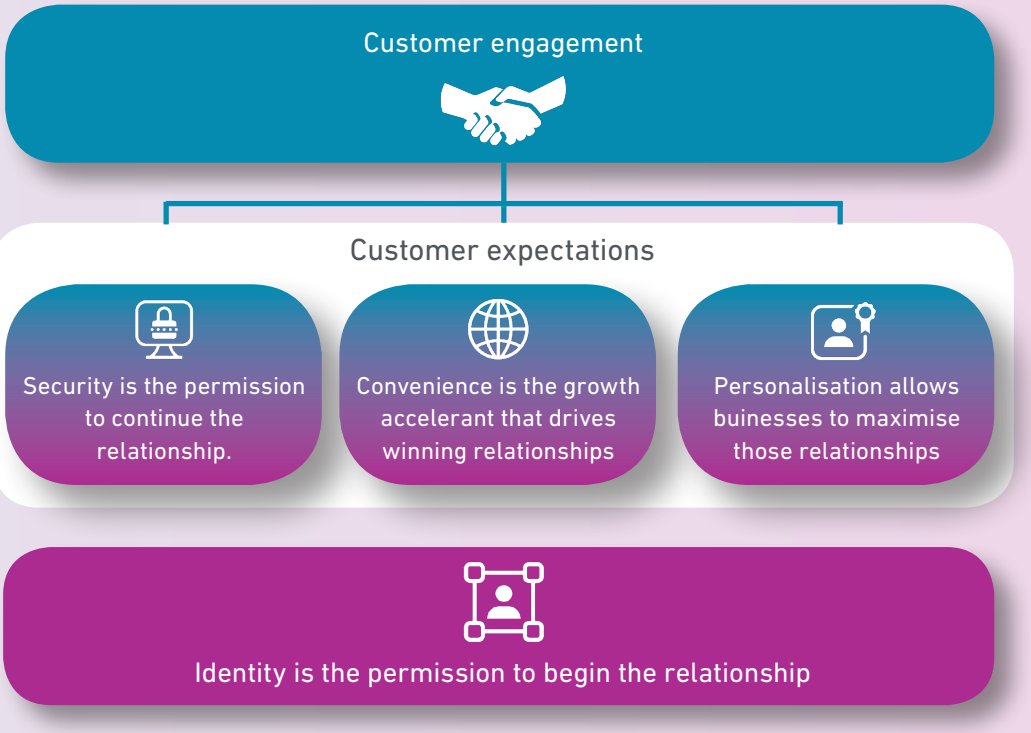


Figure 1

[1] Experian's 2019 Global Identity & Fraud Report: Creating Meaningful Relationships Online, January 2019

Competitive differentiation is founded on how you engage customers, at every interaction

The big data boom has brought challenges as well as the chance of enhanced customer relationships with it, and its opportunities need to be balanced with a serious concern for security issues. Our research suggests that businesses' broad faith in their customer recognition systems doesn't necessarily stand up against the backdrop of rising levels of online fraud. However, inventive approaches and advanced tools are already delivering favourable outcomes for customer identification and re-recognition. In conjunction with a rethinking of the size and shape of customer journeys, and a renewed emphasis on transparency and trust, there's significant scope for digitally progressive businesses to stand out from the crowd.

As data's value grows so does the risk of fraud

Consumer adoption of digital channels has generated, and unfortunately exposed, a great deal of data. Some estimates predict an excess of 79.5 zettabytes (or 79.5 billion terabytes) of generated data by 2025[2], and that number continues to increase with the growth of connected devices. This figure largely consists of people's digital exhaust – the data created from their online activity, behaviours and transactions. Part of the promise of 'big data' solutions was to make sense of all this digital information, but a failure to fully realise that aim has turned data lakes into data swamps. Businesses seem to know that advanced tools like artificial intelligence and machine learning can enable better risk decisions across the customer journey, with 86 percent considering analytics to be a strategic priority and 84 percent believing it's their core strength. But businesses are not alone in recognising both the growing value of personal data and the growing risk of fraud – consumers are now aware of these twin factors too.

A false sense of confidence regarding customer recognition

Our research findings indicated a seemingly positive trend, with 95 percent of businesses claiming to have high confidence in their ability to identify and re-recognise their customers at every interaction. Indeed, this strength of belief only ever reached a low of 82 percent in the Netherlands. It was a particularly encouraging finding since 84 percent of businesses surveyed in our 2018 study[3] stated that if they could accurately recognise customers, they could mitigate downstream fraud.

With such confidence among businesses in relation to recognising customers, we expected to see a decrease in fraud incidence. Instead, we found significant indications that business concerns around rising fraud persist, with nearly three in five businesses saying it's increased in the past 12 months. 57 percent of businesses are experiencing rising year-on-year fraud losses, despite claiming to be able to identify their customers. This significant disparity raises several questions regarding the ways in which businesses understand 'customer recognition.' They might be considering 'recognition' in terms of their marketing initiatives, where a cookie may be used to consistently re-identify a customer. Or they may be equating the presence of authentic, but stolen, credentials – such as usernames, passwords, one-time passcodes or knowledge-based authentication – as 'recognition.' This is an even bigger issue, as the sizeable increase in fraud incidence suggests that businesses' confidence is misplaced, but also hints that they may in fact be recognising fraudsters impersonating legitimate customers. Regardless, it's clear there is a problem, given that 55 percent of customers still don't feel recognised (Figure 2).

[2] IDC's Worldwide Global DataSphere IoT Device and Data Forecast, May 2019

[3] Experian's Global Identity & Fraud Report: Exploring the links between recognition, convenience, trust and fraud risk, January 2018

95% of businesses are confident in their ability to recognise their customer

55% of consumers don't feel recognised by business

	Global	US	Brazil	Columbia	UK	Netherlands	France	Spain	Germany/ Austria*	Japan	Indonesia	Australia	India	China
Business confidence in ability to identify customers	95%	96%	100%	98%	88%	82%	94%	98%	94%	88%	100%	96%	100%	98%
Consumers who don't feel recognised by businesses	55%	45%	39%	54%	58%	67%	69%	58%	66%	86%	36%	61%	35%	45%

Figure 2

*To obtain a statistically relevant sample to evaluate, responses from Germany and Austria were combined.

The challenge businesses are facing in this area is that traditional credentials or methods used to identify or 'recognise' consumers in digital channels are considered strong, but they're rigid and brittle. Because once compromised, they offer full access to whichever party is presenting the credentials, which can ultimately mean the wholesale loss of assets or manipulation of the account. On top of that, adding more of these types of approaches to the authentication process, whereby a business stacks rigid method upon rigid method, doesn't always equate to better security, but almost certainly amounts to more friction for the consumer.

Friction remains a challenge

Businesses are required to continue the use of Know Your Customer (KYC) and Customer Identification Program (CIP) methods to achieve regulatory compliance. Despite being required they're insufficient (on their own) for stopping the growth of fraud and often require significant customer involvement, which can translate into frustrating consumer experiences. We also found that businesses continue to rely on traditional fraud mitigation and authentication methods, like the use of passwords and one-time passcodes, which may be vulnerable to compromise. However, where businesses use an approach to customer identity and recognition that involves layers of data, and the application of advanced analytics to create more accurate and less intrusive experiences, we see them succeeding in the creation of secure and trusted customer engagement.

More dynamic approaches to advanced authentication like this seem to hold tremendous promise, by simultaneously allowing businesses to recognise their customers, reduce fraud risk and create relevant, positive relationships. Our research found that 86 percent of businesses claim advanced analytics is a strategic priority. Surprisingly, only 67 percent of businesses consider the use of advanced analytics, like artificial intelligence, to be important for fraud prevention and only 57 percent for identifying customers. Even less, are actively pursuing a hybrid of machine learning leveraging both unsupervised and supervised models with business rule logic – 45 percent globally and with the United States and Japan as the outliers at 58 percent (Figure 3). Yet more sophisticated authentication strategies and advanced fraud detection tools will allow businesses to accurately identify and continually re-recognise their customers, reducing their exposure to risk and ultimately leading to increased trust in such organisations.

Strategic priorities for advanced analytics

Advanced analytics that businesses currently use for identity authentication

Top analytics methods used	Global	US	Brazil	Columbia	UK	Netherlands	France	Spain	Germany/ Austria	Japan	Indonesia	Australia	India	China
Business rule logic	51%	58%	56%	54%	44%	50%	46%	38%	40%	50%	58%	48%	64%	56%
Supervised machine learning models	50%	48%	58%	64%	40%	34%	48%	60%	28%	40%	64%	44%	66%	48%
Unsupervised machine learning models	35%	32%	46%	32%	46%	34%	32%	30%	36%	34%	42%	18%	40%	32%
A hybrid of supervised/ unsupervised ML + business rules	45%	58%	46%	22%	40%	42%	40%	42%	48%	34%	56%	52%	54%	58%

Figure 3

Trusted relationships – reaping the benefits of accurately identifying and re-recognising customers

Executives have indicated that consumers trust businesses most when they feel recognised and understand what the business is doing with their data. Yet while 95 percent of businesses claim to accurately identify their customers, 55 percent of consumers disagree. So, the ability of businesses to accurately identify and re-recognise customers, demonstrate transparency in the use of their data and effectively manage fraud, are all important driving forces that will continually improve and safeguard consumers' sense of trust over time.

As businesses transform their strategies and operations to meet the expectations of the digital consumer, the traditional model for customer lifetime management is also changing. The macro view of a single customer journey once defined a customer's relationship with a business over a relatively large period. This thinking is starting to give way to a fresh concept: micro-journeys. Micro-journeys are 'moments of truth' that happen during every interaction with the customer. They offer opportunities for businesses to meet customer expectations, as well as capture information to help improve the delivery of their needs and preferences. All of which should be positive news, as business executives agree that their ability to deliver the best digital experiences requires not only the modernisation of their legacy systems, but also their approach to how customers engage with their businesses.

The idea that identity authentication becomes the permission to begin and continue the relationship with a customer is also supported by the concept of a micro-journey. As data is collected across the customer journey, it builds a clearer picture of each individual customer and augments recognition of them. In other words, the data collected over the course of multiple micro-journeys fosters recognition and re-recognition, which in turn breeds familiarity. This enhanced familiarity eventually reduces unnecessary friction by 'freeing' every subsequent digital interaction from burdensome security protocols and creates a more positive customer experience.

Key to it all, however, is consistently delivering a positive experience. As customers have more positive experiences with businesses, and those businesses are open and clear about how they use personal information for security, convenience and personalisation, they become more comfortable sharing data with these businesses. In fact, previously we found that 72 percent of consumers would be willing to give more personal information if it meant easier access to accounts later.

This leads to businesses being able to identify customers more accurately, further reducing the amount of friction that customers experience, which in turn bolsters confidence. Ultimately, it creates a level of bilateral trust between the two parties that forms part of a virtuous cycle of trust (Figure 4).

We believe businesses can leverage data, passively observed from consumers' interactions (device configurations, user-device-behaviour (behavioural biometrics), cross-business transactional history, shopping and purchasing habits, location data, and many others), to build a more dynamic, less rigid approach to recognition. The benefits to consumers are broadly twofold. Firstly, it means more secure engagements, because spoofing the wide variety of attributes listed above is much more difficult than stealing Personally Identifiable Information (PII), usernames or passwords, making it virtually impossible for fraudsters to impersonate the consumer. Secondly, it translates into better user experiences, because businesses can more accurately identify consumer preferences and habits. Many of the technologies and much of the data for achieving these capabilities may already be available to businesses today but may not be effectively harnessed.

72% of consumers would be willing to give more personal information for easier access to accounts

84% of businesses believe if they can better identify customers, then they will more easily spot the fraud

Cycle of trust: Creating meaningful relationship between businesses and consumers

Recognition, transparency and confidence provide a positive customer engagement that creates mutual trust between businesses and consumers

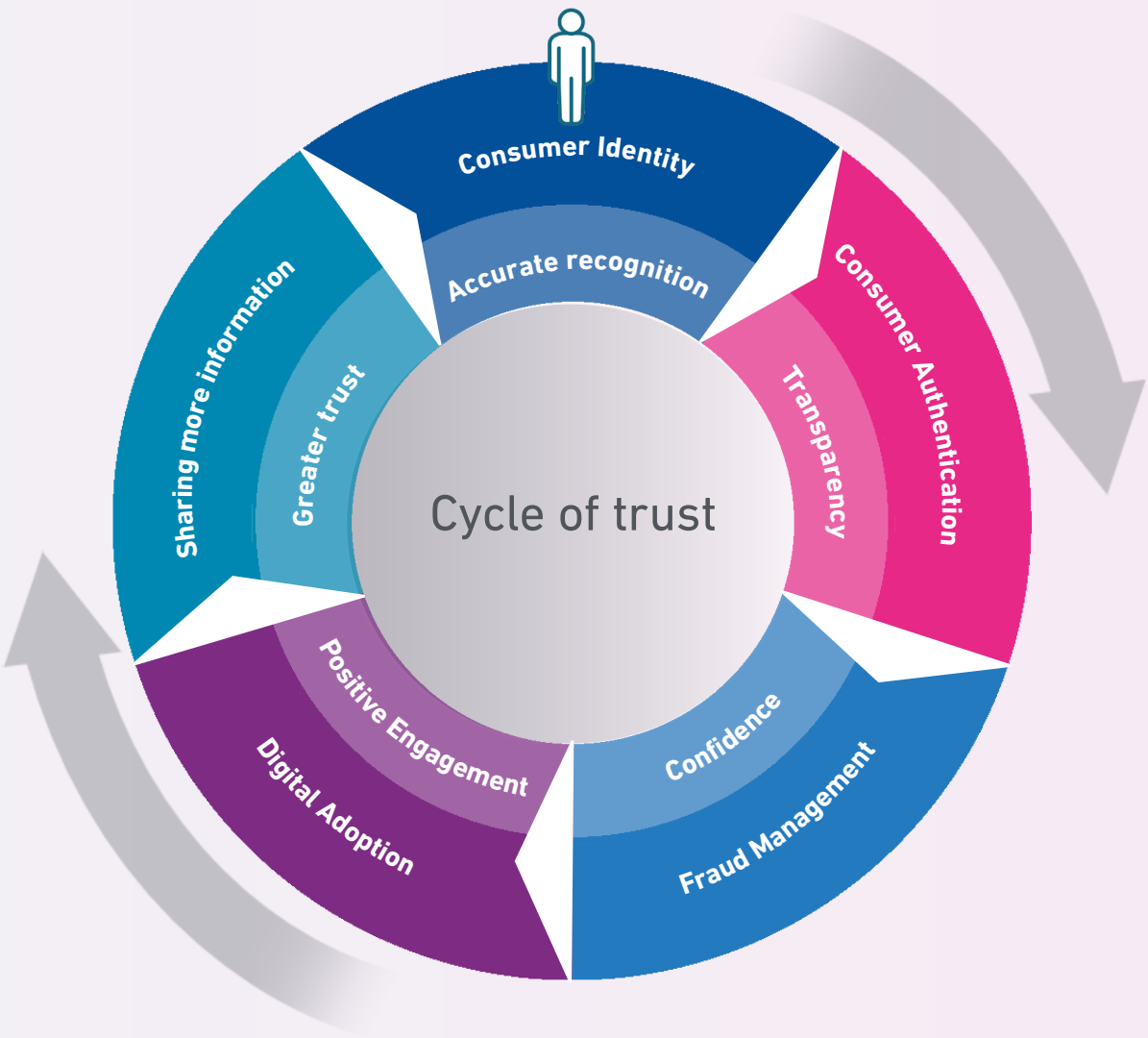


Figure 4

"Our customers expect that their information is cared for and protected. We use their data to try to provide a unified experience so it feels common and expected. We don't want to be overbearing with our authentication controls and try to avoid looking at each transaction monolithically. More information helps us decide what controls to put in place to authenticate a customer and provide an experience that is as frictionless as possible."

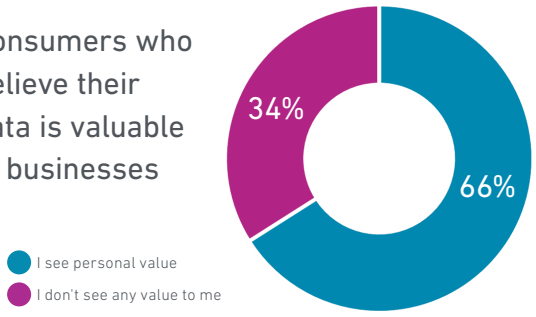
- Vice President, IT of Top 10 U.S. Retail Bank

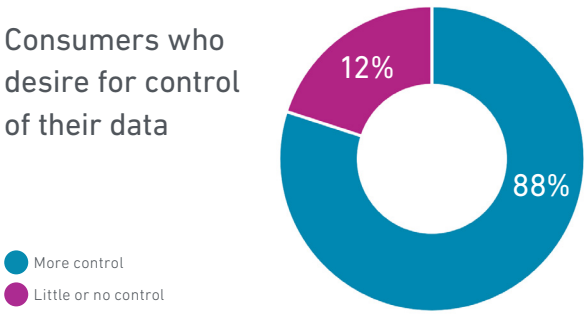
Businesses want better data, consumers want control

Executives find data quality challenging and acknowledge that they could make better decisions with better quality data. Meanwhile, consumers are willing to give businesses more personal information if there's a benefit for them and when there's transparency regarding how businesses will use it.

Indeed, consumers seem to have a heightened awareness about the value of their information generally, with 66 percent of consumers seeing value in it for them personally (this is highest in Indonesia at 85 percent, and lowest in Germany at 50 percent). The percentage of consumers saying they like the changes being made to the customer experience as a result of their data being used, and that it improves their perception of the relevant businesses, is significantly higher: 88 percent globally, with the highest level among Colombian consumers at 96 percent. This sends a healthy signal to businesses that consumers, although cautious, are becoming aware of and open to the benefits available from sharing their data. Organisations can embrace this opportunity by leveraging this willingness in order to strengthen and enrich their authentication and security methodologies, while also achieving consumers' desire for convenience. Consumers are signalling their readiness to share more: it's up to businesses now to act in good faith in the light of their customers' confidence and to lead their relationships into the virtuous cycle of trust that will present benefits to both parties. Also, 88 percent of consumers want more control over the use of their data, an echo of their desire for increased transparency in this area (Figure 5).

In many markets regulatory compliance has put in place guidelines for better consumer data protection and privacy, yet they haven't provided a simple way for consumers to act upon and take advantage of those programmes. Some businesses have tried to extend control to consumers, with seemingly little uptake. In fact, two thirds of businesses are working to put plans in place that could empower consumers with more control over their data. However, current attempts appear to get too tactical and consumers lose interest, or don't fully understand what it means to control their identity data and how to go about doing so. It's apparent that there isn't an easy, overt way for consumers to manage their identities yet: but while this presents a challenge (not being able to fulfil the request) to businesses, it's also very much an opportunity (more meaningful and profitable customer relationships) for those that can figure it out.





Consumers who see value of their data	Global	US	Brazil	Columbia	UK	Netherlands	France	Spain	Germany/ Austria	Japan	Indonesia	Australia	India	China
Yes	66%	74%	68%	57%	63%	62%	55%	59%	50%	79%	85%	59%	69%	78%
No	34%	26%	32%	43%	37%	38%	45%	41%	50%	21%	15%	41%	31%	22%

Figure 5

Emerging identity propositions are promising security and convenience

Creating a trusted, best-in-class customer experience is achievable with the right levels of security and reduced friction, which together provide easy access to accounts when and where the consumer wants it. Numerous new identity propositions are emerging worldwide to achieve consumers' desire to be known (identity) and recognised at every interaction (re-recognition). These include:

- Reusable IDs – a set of identity attributes or identity claims that, when validated by one party, can be re-used via a method in which the consumer authorises the first party to share those attributes with a different service provider.
- Federated IDs – offers the ability to transmit any identity data or authentication credentials across an ecosystem of services with common management policies (e.g. Single Sign-on – SSO).
- Tokenised IDs – converts identity data or credentials into representative token values that can be used in place of actual identity data. Often these are associated with digital interactions where clear-text data is not required to fulfil the transaction.
- Decentralised IDs – uses distributed ledger technologies (DLT) like blockchain to ensure that identity data is not tampered with or modified. The person's identity data is not stored in any single repository, or controlled by one entity or service provider, but is rather maintained consistently across a distributed network of them.

Over 90 percent of businesses feel these new identity propositions play an important role for re-recognising their customers but no one approach has broadly taken hold yet. Many businesses are familiar with their emergence and are in 'wait and see' mode as the technology evolves and consumer interest grows. Regardless of which identity proposition is adopted by a business, the need to establish the verifiable claims that constitute a person's identity is fundamental to doing business digitally.

This happens at both the point of enrollment into an identity proposition and ongoing to ensure the identity hasn't been tampered or compromised. Geographically speaking, different countries are at different levels of maturity when it comes to such identity propositions. Each nation is driven by what's useful about identity and reflects different drivers and their perspectives, be that financial services, government, telecommunications, healthcare or social media (to name a few). The most functional driver for each country is being prioritised, which is leading to the creation of different identity propositions and differing maturity levels across the globe. The UN and World Bank, meanwhile, envision that by 2030 every individual in the world will have a digital identity[4]. Highlighted below are four notable programmes to watch:

- Thailand: The government's Thailand 4.0 initiative involves a national digital identity approach which enhances security and accessibility to bank accounts using eKYC authentication with facial recognition and blockchain-powered technology.
- India: Aadhaar is a large government-led initiative to create a national identity and promote a secure, digitally empowered society and knowledge economy. It's based on the use of biometric and geographic data.
- Nordics: Federated e-IDs across the Nordic region (Norway, Sweden, Denmark, Finland) have evolved with different programme names, but have one thing in common: collaboration amongst banks versus government or third-party solutions.
- Africa: Good ID framework holds the promise of improving the quality of Africans' digital identities and boost the economy, with important safeguards embedded in technology (including biometrics), policy and practice.

[4] https://www.csis.org/events/digital-identity-and-future-africas-digital-economy

All of this leads us towards an inflection point

Businesses are prioritising personalisation over security, whereas consumers are prioritising security. At the same time, organisations' seemingly misplaced confidence in their ability to identify and re-recognise customers is contributing to higher fraud losses and a subsequent lack of trust. It's a problematic situation that can't be ignored.

Although some might see it as impossible to fulfil both priorities, Experian believes you can achieve both security and convenience when you accurately identify your customers. Furthermore, accurate identification of your customers can be the cornerstone of personalised experiences. Whereby businesses can offer customers protection and easy-to-use products and services by leveraging the vast amounts of digital data already available to them and by using advanced tools, like artificial intelligence and machine learning, to make more meaningful decisions.

We know that many businesses are focused on customer-centricity as a strategic priority to enable changes to the ways they interact with customers throughout their journeys. However, customer-centricity needs to go beyond personalisation. It should represent a new way of engaging customers and delivering on expectations at every moment of truth, or micro-journey. It's where identity is the permission to begin and continue the relationship, convenience is the growth accelerant that drives its quality, and personalisation allows a business to maximise its potential.

And it's in this virtuous cycle of trust that consumer engagement will flourish, customer loyalty will strengthen – and you'll meet the next generation of digital customers.

Methodology

From July to November 2019, Experian conducted research among 6,500 consumers ages 18-69 and 650 businesses across banks, card and payment providers, telecommunications providers, online and mobile retailers in 14 countries including United States, United Kingdom, Germany/Austria, France, Spain, the Netherlands, Brazil, Colombia, Mainland China, India, Japan, Indonesia and Australia. Findings were further validated by over 26 in-depth phone interviews with senior executive leaders with decision making responsibilities for the strategic planning process for digital customer experience, technology and innovative, or fraud risk management across a range of functions, including product, marketing, operations, information technology, general management and finance. This is the fourth year of the study.

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

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

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

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

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

Serasa Experian
Alameda dos
Quinimuras, 187
CEP 04068-900
Planalto Paulista
São Paulo
Brazil
T +55 11 3373 7272
F +55 11 2847 9198

Experian Singapore Pte. Ltd.
10 Kallang Avenue
#14-18
Aperia Tower 2
Singapore 339510
T (65) 6593 7500

Related research

Global Identity & Fraud Report 2019: Creating Meaningful Relationships Online

Asia-Pacific Identity & Fraud Report 2019

EMEA Fraud Report 2019

Exploring Trends and Traits of Fraud 2019, UK&I

Synthetic Identity Theft in the U.S.: Why it won't stop

www.experian.com/da

01/20