2019 Global Identity and Fraud Report

Consumer trust: Building meaningful relationships online

Introduction

Trust is a precious commodity that is earned over time and difficult to build between consumers and businesses in an online world. When interacting with a business online, customers expect to be recognised and met with a personalised experience. This requires that businesses are applying the right tools and relevant information to recognise them. And unlike face-to-face encounters, these digital interactions lack the human touch and subtle visual cues that typically allow for trust to be built.

The anonymous nature of digital interactions means that businesses and consumers must mutually find ways of establishing bilateral trust. To accomplish that today, consumers look for things like visual signs of security when interacting with a business whereas a business will simply ask a consumer for more personal information. However, digital commerce is expected to grow globally at 20 percent CAGR by 2022, reaching nearly US$5.8 trillion in value[1] and digital banking users (online and mobile) exceeded 2 billion in 2018 with an expected 11 percent CAGR (2019-2023), where mobile banking users are expected to be 58 percent of the global banked population in 2019[2]. That means it's imperative that businesses build meaningful digital customer relationships based on trust.

What does it take to build trust online? Practically speaking it is about maximising both security and convenience – auto-fill forms for quicker access, more relevant product recommendations based on shopping behaviours, and the ability to store payment information securely for faster checkout.

All of this is made possible using information that consumers share with businesses. However, the propagation of this information across multiple businesses is what increases the risk of fraud.

Consumers are opening more and more digital accounts; some studies suggest upward of 100 digital accounts per person. If a customer's account is compromised with any one of these businesses, it potentially impacts the security of their information with other businesses as people often re-use a small set of passwords and security questions. That said, while 60 percent of consumers globally are aware of the risks involved with giving their personal information to banks and retailers online, still more than 70 percent would provide even more information if there was a perceived benefit. Furthermore, transparency about how consumers' information is used to protect them and create a better overall experience is paramount for creating this trusted relationship with nearly 80 percent of consumers saying that the more transparent a business is about the use of their information, the greater trust they have in that business.

Businesses already have a lot of consumer information, data they have gathered either during an account setup or ongoing digital interactions. This includes traditional information, such as name, address, email and phone and more dynamic digital data, such as device details, biometrics and channel preferences.

1 https://www.forbes.com/sites/jordanmckee/2018/09/11/global-digital-commerce-sales-to-near-6-trillion-by-2022/#6889ffef4c5a

2 Juniper Research, "Retail Banking" Q4, 2018 Update

Businesses also have access to a lot of additional information – contextual, behavioural and geolocation data – that can complement the personal information a customer provides. So why are customers being asked to prove their identity by repeatedly providing the same or more personal information, exposing them to greater risk of fraud? Are businesses doing enough with the information they already have access to? Are they using it to better recognise and deliver the experiences their customers expect?

In this year's Global Identity & Fraud Report we explore the key factors that matter most to consumers for gaining trust and confidence in an increasingly digital world, and how businesses are responding. We surveyed more than 10,000 consumers across 21 countries representing nearly 40,000 devices, 85,000 online accounts and more than 480,000 online transactions in the past year. We also surveyed more than 1,000 businesses representing average annual revenues of US$3.1 billion (US$3.4 trillion total), of which US$2.3 trillion is generated globally through the digital channel.

Fraud risk is still a growing threat

Fraud risk is still a growing threat

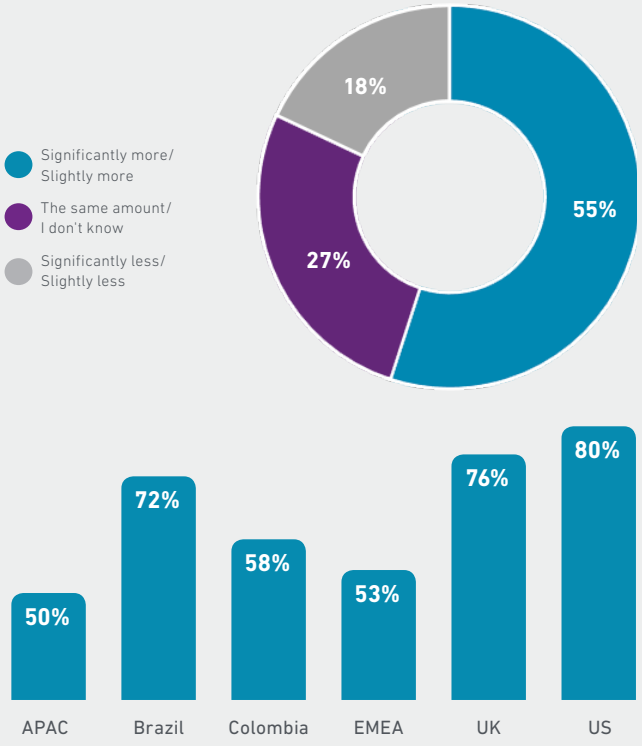
More than 2 in 5 consumers worldwide have already experienced a fraudulent event online at some point in their lives, with the highest incidence occurring in the United States and the lowest in the Europe, Middle East and Africa region. That means that even the marketplace that is most effective in mitigating online fraud has potentially left a full third of its digital customers vulnerable.

Fifty-five percent of businesses surveyed reported an increase in online fraud-related losses over the past 12 months, predominantly around account origination and account takeover attacks – both particularly damaging to brand reputation (Figure 1). This issue is particularly acute in the United States where 80 percent of businesses have seen their online fraud losses increase from 2017 to 2018. This could be the result of fraud moving from card terminals to online and mobile channels since the adoption of EMV. Actual losses aside, more than two-thirds of businesses worldwide reported an increased concern for fraud this year. This concern is highest among United States businesses and lowest among businesses in Colombia, followed by Asia-Pacific. Despite these regional variations, there is no disputing that fraud is a universal concern.

Yet this hasn't appeared to have much material impact on channel preference among consumers. Consumers remain tied to the digital channel, with 91 percent having purchased goods and services online (a slight increase from last year's incidence of 90 percent). Similarly, nearly 9 in 10 report conducting personal banking among their top online activities, unchanged from last year. Despite the risk of fraud facing consumers and businesses, we continue to depend on the digital world.

Online fraud losses have increased in the past year

Q: In the past 12 months, has your business experienced more, less or the same in fraud losses?



APAC countries surveyed include: Australia, China, Hong Kong, India, Japan, New Zealand, Singapore, Indonesia, Malaysia, Thailand and Vietnam

EMEA countries surveyed include: Germany, Austria, France, Spain, the Netherlands and South Africa

Figure 1

"A well-known international airline had major data issue that was recently announced where customer details were taken from the actual payment page. The airlines, banks and other companies collaborated to make sure consumers are protected and feel safe using the digital channel. Internally, teams across my company came together to figure out whether our systems were vulnerable in any similar way to that airline."

- Head of Digital Banking, Top 10 Retail Bank, U.S.

Businesses are investing more to combat fraud and better understand its widespread impact

Businesses are investing more to combat fraud and better understand its widespread impact

Half of businesses globally report an increase in their fraud management budgets over the past 12 months. The United States and United Kingdom lead the pack, with three quarters of businesses budgeting more for fraud management than they did a year ago. As businesses adopt the online and mobile channels, fraudsters can exploit weaknesses in the new services and features being offered to consumers. However, technology has helped businesses not only anticipate their customer's needs and behaviours, but also protect them. The perception is that increased investments are paying off, with nearly 75 percent of businesses globally reporting an improvement in their online security over the past year. However, businesses have experienced increased fraud losses and new fraud attacks during that period as well – leading us to believe businesses may be investing in the wrong capabilities.

Driven by the growing levels of concern for fraud, businesses are also focusing resources on analysing the impact fraud has on their bottom line. Only half of companies believe that they have a high level of understanding about how fraud affects their business. Which may explain why most businesses continue to invest in capabilities and point solutions that are less effective rather than looking at the problem holistically. The impact is both immediate – in the cost of fraud losses incurred – and enduring as it manifests itself in ongoing operational costs for fraud prevention. And, let's not forget about the reputational capital that fraud puts at risk – such as trust.

50% of businesses report an increase in their fraud management budgets

Typically, designing an enhanced customer experience meant reducing onerous security controls, often positioning IT, marketing and fraud at odds with one another. When speaking with executive business leaders, however, we found that when the brand was put first (i.e., reputational risk), stakeholders expanded from IT to include both marketing and fraud prevention teams. This suggests that the tension between customer experience and data security is abating, giving way to cross-functional alignment and integration among teams to deliver both security and convenience.

Only half of companies believe that they have a high level of understanding about how fraud affects their business

"We now have an integrated team that works together when it comes to online customer experience. It involves teams from technology, security, fraud, risk management and the customer experience teams working together as a single team rather than working in silos. This has improved the overall expectations for bringing in proper security into the digital channels and also being able to dynamically improve customer experience."

- VP of Risk Operations, Top 5 Retail Bank, Australia

Consumers want both security and convenience

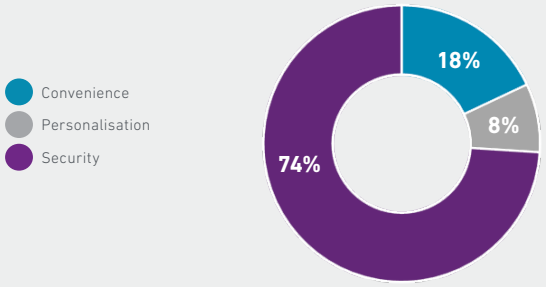
Consumers want both security and convenience

Consumers expect a secure and convenient experience but security and convenience have often been at odds with one another. Traditionally the perception has been that they must be balanced one against the other. The more you concede on security, the more seamless and relevant the customer experience. Conversely, the more you concede on convenience, the better your customers are protected against fraud. Our research highlights this tension: 74 percent of consumers cited security as the most important aspect of their online experience (Figure 2), whereas 72 percent said they would be willing to go through a more thorough enrolment process at account opening if it meant easier access to their accounts later (Figure 3). The information collected to serve each of these objectives is not typically shared across the businesses which perpetuates two challenges – requiring customers to repeatedly provide their personal information for verification and increasing the amount of information available for potential data compromise. The newfound enthusiasm for cross-functional team collaboration suggests that businesses are making progress to solve this issue and find ways to deliver on consumer expectations to meet both needs.

Categorically, consumers ranked greater functionality (e.g., ease of navigation, visible signs of security and seamless access to accounts) and more sophisticated security measures (e.g., physical and behavioural biometrics) as the top factors contributing to a better online experience. In contrast, consumers were most frustrated by burdensome features, such as the setup of login credentials that require complex password guidelines and mandatory account creation for a one-time purchase.

Most important elements of a consumers' online experience

Q: Which of the following services is most important to you when it comes to your online experience?

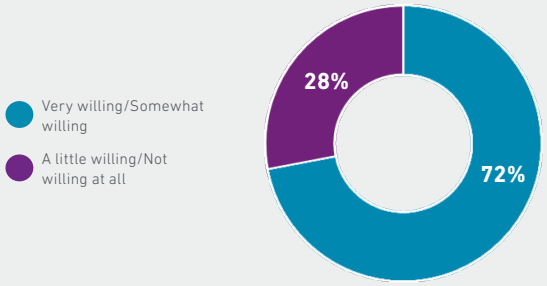


	APAC	UK	EMEA	Brazil	Colombia	US
Convenience	21%	18%	17%	10%	5%	18%
Personalisation	9%	8%	6%	6%	7%	9%
Security	76%	74%	77%	84%	87%	70%

Figure 2

Consumers are willing to share more data if it means a seamless access to their account later

Q: When it comes to opening an online account with an organisation, if you were to know that a more thorough process to confirm your identity would result in a more seamless account access in the future, how willing would you be to undergo that more thorough process?



	APAC	UK	EMEA	Brazil	Colombia	US
Very/ Somewhat Willing	72%	66%	70%	72%	84%	70%
A Little/Not Willing	28%	34%	30%	28%	16%	30%

Figure 3

> "The more customer data we have, the better it is for creating the optimal customer experience."
>
> - Senior Director of IT/Risk Management, Global Retailer, U.K.

Consumer confidence in visible signs of security is still high

Consumer confidence in visible signs of security is still high

Consumer confidence in traditional security methods – those that provide some visible signs of security (and friction) – remains important for 66 percent of consumers worldwide (Figure 4). Additionally, 74 percent of consumers indicated greater confidence in a business that uses physical biometrics. The use of biometrics seems to have the biggest positive impact on organisational trust in Colombia and the United States.

The importance of having visible signs of security is made clear when we see how likely consumers are to abandon online transactions on websites that lack visible signs of security. By contrast, they will work through the following friction-inducing, but confidence-inspiring security methods to complete a transaction: A PIN code push notification to their smartphone, forgotten account username and/or password, a PIN code push notification to their e-mail and reselecting images when they got CAPTCHA wrong.

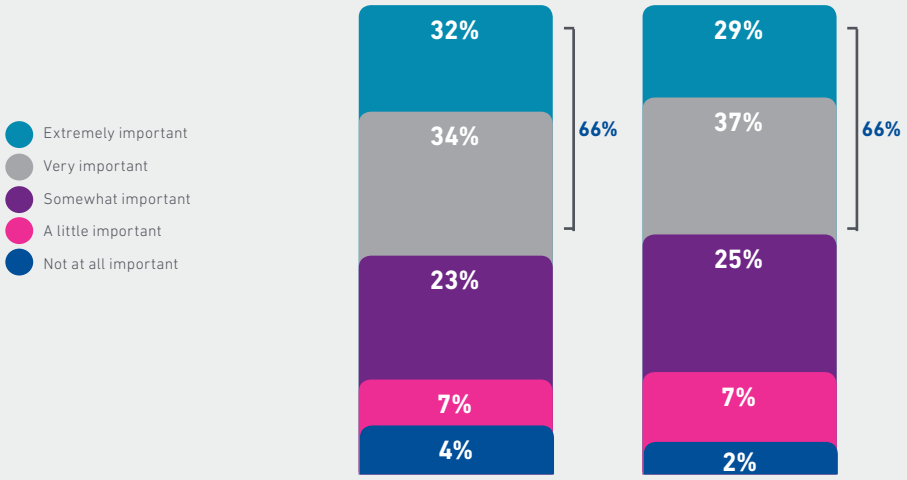
Consumer tolerance for these friction-inducing security methods is likely perpetuated by businesses that continue to use them. Data reveals that while there are pockets of use of advanced authentication methods, businesses have yet to mount a concerted and comprehensive adoption of such tools. Passwords, PIN codes and security questions remain the authentication methods most widely used by businesses, followed by document verification, physical biometrics and CAPTCHA. All regions in our global survey show businesses using the same top three authentication methods except for Latin America where CAPTCHA, physical biometrics and customer identification programs make up the top three.

74% of consumers have more confidence in a business that uses physical biometrics for security

Unlike standard authentication tools that typically require username and password, advanced authentication solutions aggregate digital data, including passive device information, behavioural biometrics, and network characteristics. These solutions can apply the right response by intelligently stepping up or stepping down the required level of challenge based on the level of risk. Customers may not see these passive security controls in play but they provide a stronger defence against fraud attacks and improve the experience for true customers.

Consumer confidence in visible signs of security is still high

Most important features in online banking



Top Two Box

	Demonstrations of security	Seamless access to my account within the banking digital platform(s)
APAC	64%	64%
UK	55%	64%
EMEA	66%	64%
Brazil	85%	75%
Colombia	84%	87%
US	65%	66%

Figure 4

Consumer confidence in visible signs of security is still high

Consumer trust and confidence soar in response to sophisticated security measures

Consumer trust and confidence soar in response to sophisticated security measures

In the near term, businesses foresee continuing to use traditional authentication methods, even if they believe in the greater effectiveness of more advanced methods (e.g., physical biometrics, multifactor/two-factor authentication, Know Your Customer procedures, internal data, and customer identification programs). Their continued reliance on these traditional authentication methods is a delicate balance. They need to deliver an online experience that instils confidence, with security controls that make customers feel safe and protected. And they need to allow for easy and convenient access. That said, data suggests that businesses are beginning to embrace the changing tides enabled by technology. Two-thirds contend that they already have 'the most up-to-date security measures for digital and mobile access' and express considerable interest in 'learning more about advanced authentication methods.'

In the meantime, consumers continue to have confidence in passwords, PIN code push notifications to smartphones, and security questions (Figure 5).

"We used to ask consumers to go through a friction-heavy process to vet themselves. This wasn't very good for an agile and fluid customer experience. We are much more customer-driven, always keeping an eye on the front-to-back customer journey and trying to make it easier for them."

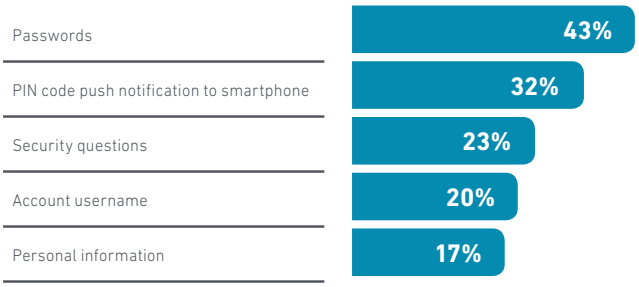
- Global Head of Infrastructure & IT, Top 5 Retail Bank, U.S.

However, when exposed to more advanced authentication methods such as physical biometrics, their confidence increased significantly (Figure 6). Furthermore, when they encounter such advanced methods, they seem to become more 'trusting' of their bank's ability to protect their personal data. In fact, the use of physical biometrics seems to have the largest positive impact on trust, particularly in Colombia and the United States.

This indicates that consumers may be eager to embrace advanced authentication methods because they instil trust, and trust is the foundation of their (digital) relationship with the brand. Businesses are coming around, seeing that the consumer's desire for both convenience and security is a tall order, unachievable without the latest technology and authentication methods.

Consumer confidence in traditional authentication methods

Q: Looking at each of these methods you have encountered in the past 6 months to confirm your identity as a customer, which are the top three methods in which you have the most confidence in its ability to protect you against identity theft and online fraud?



	APAC	UK	EMEA	Brazil	Colombia	US
Passwords	40%	47%	46%	44%	53%	44%
PIN code push notification to smartphone	34%	23%	29%	20%	49%	25%
Security questions	22%	37%	20%	18%	31%	38%
Account username	19%	22%	18%	27%	23%	26%
Personal information	18%	18%	14%	26%	17%	17%

Figure 5

Consumer confidence in alternative security methods

Q: You mentioned that you had encountered the below events at some point in the past six months during your online banking transactions. Please indicate on the scale below how these events made you feel about your bank.

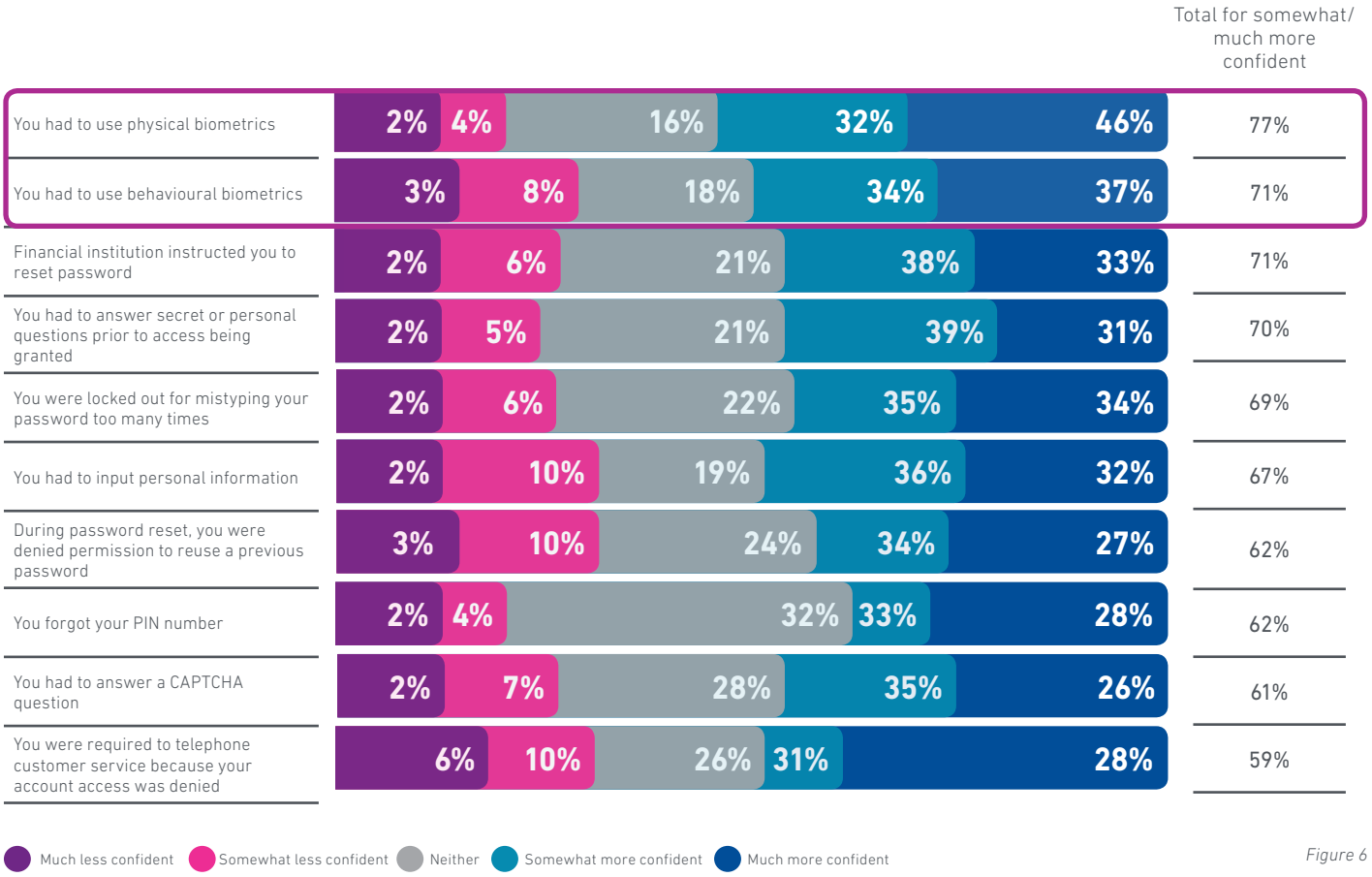


Figure 6

Percentages do not add up to total due to rounding.

Industry leaders that foster consumer trust may be the most well-placed to seed more advanced tools

Industry leaders that foster consumer trust may be the most well-placed to seed more advanced tools

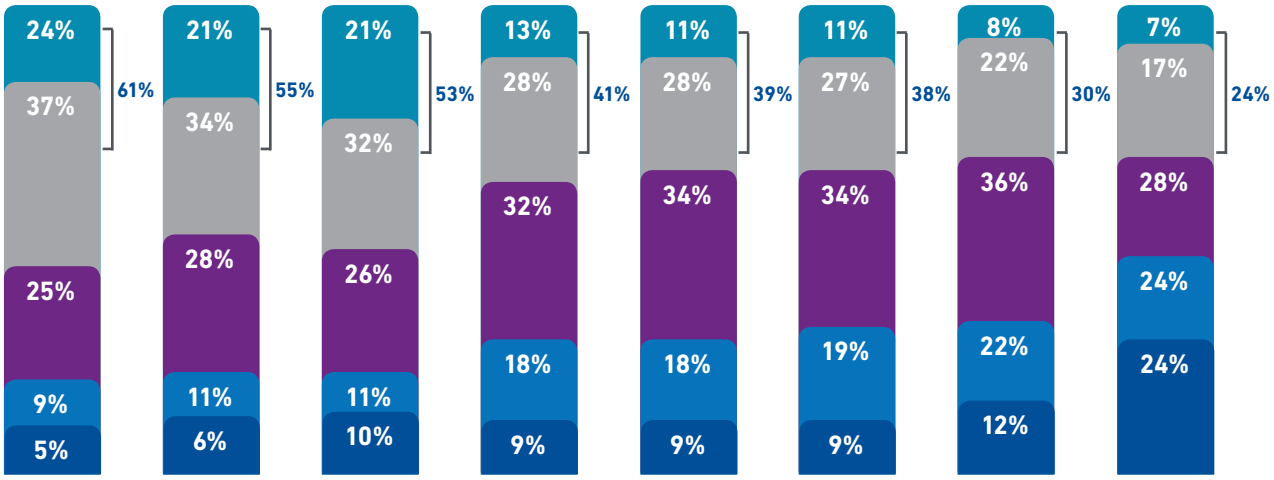
Trust varies considerably depending on the country and the type of business. Sixty-one percent of consumers across most regions trust banks and insurance companies, followed by payment providers at 55 percent and government agencies at 53 percent (Figure 7). However, as seen in the figure, this order differs across Brazil, Colombia and the United States.

Online retail and social media sites lag considerably behind other industries regarding trust. In fact, trust in social media sites has continued to erode over the past 12 months, a possible reaction to perceived data misuse and lack of transparency for how consumers' data is collected and used.

> "To earn the trust of our customers, there are two dimensions that are very important from a customer perspective – security and stability. Where you can destroy a lot of trust and confidence is by not having a stable online system. If it crashes a lot or gets hacked, trust can be lost immediately."
>
> - Head of Strategic Risk Management, Top 5 Retail Bank, Austria

Consumer trust by industry

Q: The following are organisations may collect, use and store personal data. Please indicate on the scale below the degree to which you trust each in collecting, using and storing your personal data.



% Trust completely	Banks, insurance companie	Payment system providers	Government agencies	Tech providers	Telecommunications companies	Electronic/ Mobile commerce marketplaces	Online retail sites/ apps	Social media sites/apps
APAC	24%	21%	23%	14%	12%	11%	9%	9%
UK	23%	18%	24%	11%	11%	12%	9%	6%
EMEA	22%	20%	19%	7%	7%	7%	5%	4%
Brazil	32%	32%	20%	22%	13%	16%	13%	13%
Colombia	29%	21%	11%	14%	9%	10%	6%	5%
US	32%	28%	22%	19%	16%	21%	13%	11%

Trust completely · Trust a lot · Trust somewhat · Trust a little · Do not trust at all

Figure 7

Transparency can lead to greater levels of trust

Transparency can lead to greater levels of trust

Businesses collect a lot of information on their customers at every stage of the customer journey, and more than 75 percent globally are taking steps to comply with GDPR or similar local regulations. The robustness of these plans varies greatly – from meeting regulatory requirements to proactively exceeding them. There are many possible reasons for the variance in robustness – some view it as a driver for re-examining their customer experience approach, and others may view it as onerous. But with a two-year grace period to become compliant, it may be too early to speculate.

What we are starting to observe is the possible value created by being more transparent and open with customers about the use of their information, and customers' willingness to participate in that value chain. Ninety percent of consumers are aware that businesses are collecting, storing and using their personal information. Most consumers have also resigned themselves to the fact that providing their personal information increases their risk of fraud as the price they pay for convenience. Despite the potential risks, more consumers are willing to share information in exchange for perceived value.

Sixty percent are willing to share more information for better security and/or convenience and believe the benefit is greater than the perceived risk, and 67 percent are willing to share for more personalised goods and services.

Despite the business drivers for increased transparency, nearly 80 percent of consumers globally feel strongly that businesses are being fully transparent about how their information is being used. Businesses are on the same page – 51 percent have already made significant investments in initiatives to be more transparent with consumers. In the past six months, the United States appears to have invested the most, and 56 percent of businesses intend to invest more in the next six months (intent is highest in Colombia and lower in the Europe, Middle East and Africa region). Businesses are taking tangible steps in that direction through a variety of transparency-inspired initiatives – educating consumers, communicating service terms more concisely and helping consumers feel in control of their information. Four out of 5 consumers have a favourable opinion of businesses executing these initiatives.

8 out of 10 consumers believe it's important for a business to be transparent about the use of their personal data

51% of businesses have made significant investments in the past 12 months

56% of businesses intend to invest more in the next 6 months

Top 3 transparency-inspired initiatives

Educating consumers about the use of their information

Communicating service terms more concisely

Helping consumers feel in control of their information

Conclusion

The cultivation of trusted relationships online is predicated on the capacity to provide a secure place to bank or buy goods and services with confidence. The historical perception has been that security and convenience must be balanced one against the other, but our research suggests consumers and businesses can have both without the trade-off. The value exchange – more personal information for a better online experience – begs a better business response.

It may begin with a business's ability to identify its customers and deliver relevant, convenient experiences without increasing their risk exposure by demanding more from the information it already accesses. More sophisticated authentication strategies and advanced tools and technologies can help recognise and deliver the online experiences that consumers expect.

Creating transparency regarding how businesses use their customers' information can go a long way toward creating more trust.

Across the world, businesses and consumers seem to recognise the growing fraud risks. Businesses are investing more time and resources in fraud management and collaborating across organisational teams to understand the impact of delivering secure and convenient online experiences. Surprisingly, consumers themselves might just become the biggest advocates for businesses to adopt better security measures. Banks and insurance providers are not off the hook. These global leaders of digital consumer trust may have a very important role ahead: Untethering consumers from the visible signs of security they believe provide strong protection, but ultimately hinder the customer experience.

Methodology

In July to November 2018, Experian conducted research among 10,892 consumers ages 18 – 69 and 1,097 businesses across banks, financial institutions, card and payment providers, online and mobile retailers in 21 countries including the United States, United Kingdom, Germany, Austria, France, Spain, the Netherlands, South Africa, Brazil, Colombia, Australia, China, Hong Kong, India, Japan, New Zealand, Singapore, Indonesia, Malaysia, Thailand and Vietnam. Findings were further validated by over 40 in-depth interviews with senior executive leaders with decision making responsibilities for the strategic planning process for digital customer experience and/or fraud risk management across a range of functions (including product, marketing, operations, information technology, general management and finance).

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.

Our fraud team – nearly 300 experts around the world – works with businesses to do exactly that. 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. 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 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

Ready to learn how Experian can help your business better identify its customers?
Contact us

Related research

2018 Global Fraud and Identity Report: Exploring the links between customer recognition, convenience , trust and fraud risk

Drivers of identity risk fraud: The trends impacting account takeover fraud. Experian US

UK&I Fraud Report: Covering banks and insurance companies, Experian UK

Digital consumer insights: Convenience, privacy and consumer fraud response cycle, Experian APAC

www.experian.com/da

© 2019 Experian Information Solutions, Inc. • All rights reserved

Experian and the Experian marks used herein are trademarks or registered trademarks of Experian Information Solutions, Inc.Other product and company names mentioned herein are the property of their respective owners.

01/19