



The 2018 Global Fraud and Identity Report

Exploring the links between customer recognition, convenience, trust and fraud risk





Introduction

Being recognised is a simple thing that goes a long way. Recognition takes many forms – whether it's acknowledgement for an achievement or being welcomed in a room as a familiar face. It feels good to be recognised.

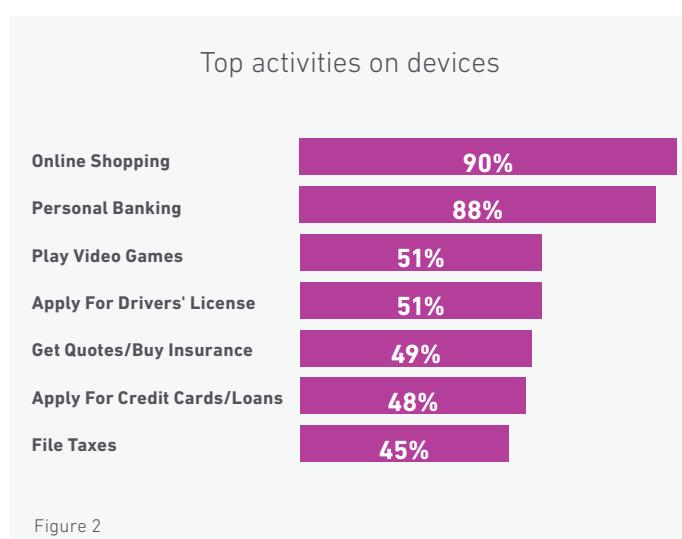
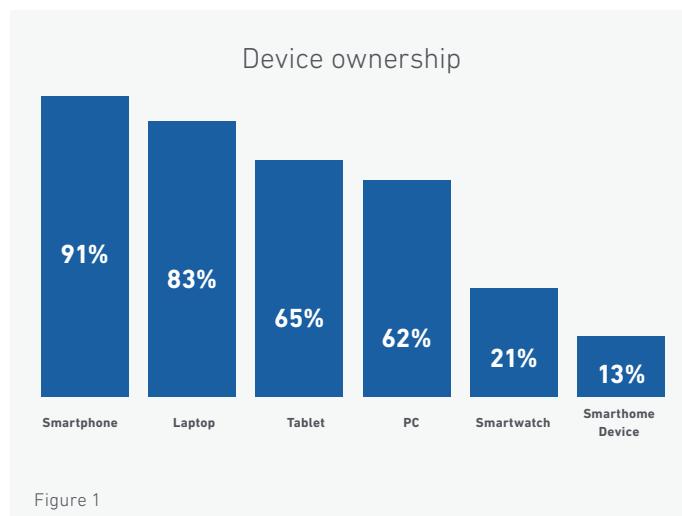
But there's more to recognition than feeling good. Now more than ever there's a commercial value associated with it. In an increasingly digital world, we are trying to recreate in-person recognition across industries and channels to fuel growth and opportunities. In doing this we need to carefully balance customer security and convenience with fraud and friction. Being able to verify someone shouldn't disrupt the way they interact with a business. Experian® believes that any business that can better identify its customers can more easily spot fraud.

Just how well-equipped are businesses at recognising their customers' identities online? What type of investments are they making in customer recognition and to what degree are they able to accurately identify customers and manage fraud risk? Our 2018 Global Fraud and Identity Report, based on input from more than 5,500 consumers and 500 businesses* worldwide, looks at this topic to understand what consumers think of security protocols today and gauges how confident businesses are in their ability to accurately identify their customers.

* Businesses in one of the following sectors: retail banking and credit card, digital only and click-n-mortar retailer, airline industry, consumer technology and electronics, telecommunications worldwide (Australia, Brazil, China, France, India, Singapore, South Africa, Spain, Turkey, the United Kingdom and the United States).

Executive Summary

With most consumers owning smartphone and mobile devices (91 percent), followed closely by laptop computers (83 percent), the digital marketplace is here now (Figure 1). Certainly, technology is supporting the large volume of online interactions between businesses and consumers. But the real currency of digital commerce is trust.



Online activities among consumers reflect widespread embrace of digital commerce as a way to purchase goods and services (90 percent) and conduct personal banking (88 percent) (Figure 2).

As businesses undergo digital transformations in their front and back office operations, they recognise the importance of trust and the need for technology to enable it.

When it comes to online engagement, three-quarters (75 percent) of businesses are interested in more advanced security measures and authentication processes that have little or no impact on the customer. At the same time businesses understand that their customers take comfort in the security measures they already have in place for digital transactions.

75% of businesses want advanced authentication and security measures that have little or no impact on the digital customer experience.

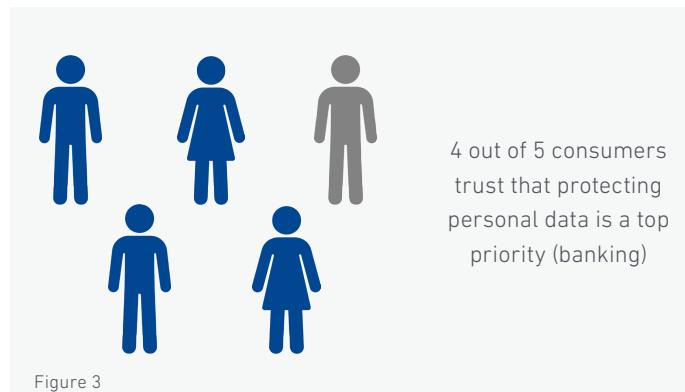


Building trust through technology without disruption is increasingly the goal, but also the responsibility of businesses with online channels. While there are genuine barriers to achieving that goal, it is now more critical than ever to business outcomes.



Consumers expect businesses to protect them

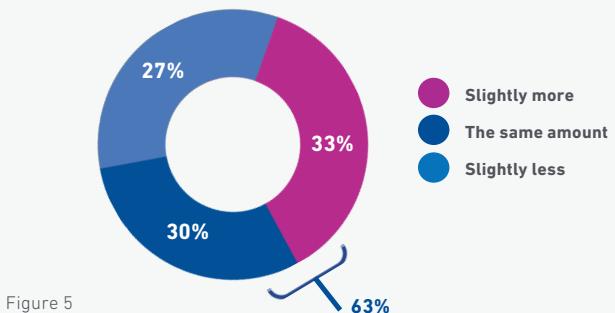
The enthusiastic embrace by consumers of the digital marketplace is predicated on trust. Four out of five consumers trust that businesses are making the protection of their personal information a top priority (Figure 3).



In contrast, almost three-quarters of businesses (72 percent) cite fraud as a growing concern over the past 12 months (Figure 4) and nearly two-thirds (63 percent) report the same or higher levels of fraudulent losses over that same period (Figure 5).

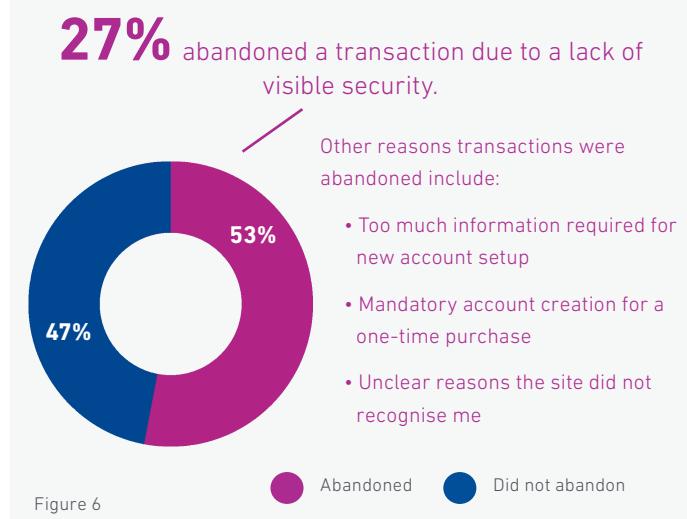


63% of businesses have experienced the same or more fraud losses in the past 12 months



Nonetheless, consumers are feeling reassured. They cite visual signs of security and barriers they encounter when accessing their online accounts as indicators that a transaction is more secure. In fact, the lack of visible security was the number one reason customers abandoned a transaction (Figure 6).

Lack of visible security was the #1 reason customers abandoned a transaction





Nearly two-thirds (66 percent) of consumers surveyed appreciate security protocols when transacting online because it makes them feel protected (Figure 7). In some ways, consumers tolerate the nuisance of common barriers to accessing their accounts (e.g., forgetting their password or having to re-enter other security controls like CAPTCHA or PIN code) concluding that higher friction means better security.

66% of consumers said, "I like all the security protocols when I interact online because it makes me feel protected."

India	S. Africa	Australia	U.S.	France	U.K.
76%	74%	70%	69%	67%	66%
Spain	Singapore	Brazil	China	Turkey	Overall
64%	63%	63%	62%	56%	66%

Q: Please indicate how strongly you either agree or disagree [with each of the following statements] on the scale provided - disagree strongly, disagree, neither agree nor disagree, agree, strongly agree.

Figure 7

Consumer tolerance for friction for the sake of security varies across the 11 countries surveyed. For example, consumers in India and South Africa are more tolerant of security protocols because it makes them feel protected. On the other hand, consumers in Turkey are less tolerant.

Tolerance also varies by age. One-third of consumers surveyed said they would do more transactions online if there weren't so many security hurdles to overcome.

42% of millennials said they would conduct more online transactions if there weren't so many security hurdles to overcome...

...versus **30%** among those 35 and older

Among these consumers, 42 percent were millennials compared to only 30 percent of those 35 and older. In other words, younger consumers are less tolerant of security hurdles and are more inclined to engage online if there was less friction.

So for businesses, there is a delicate balance to achieve. They need to deliver an online experience that instills confidence, with security protocols that make customers feel safe and protected. And, they need to allow for easy and convenient access.

Given the differences in tolerance for friction across different markets and age groups, a global one-size-fits-all solution is difficult to achieve. It is also a moving target, as consumers' tolerance for friction could lessen over time. Not to mention the expectations for a frictionless experience among future generations of digital customers used to an online digital experience that imposes few, if any, visible security protocols.

As security protocols transition to more data-driven, artificial-intelligence powered systems operating behind the scenes, businesses will need to gain and maintain the customer's trust without the familiar perception of security. Solutions that combine device information with other data points such as biometrics could help businesses in the future better recognise their customers rather than challenging them.

"We're starting to look at what are the other ways biometrics could be used. There is a world out there that is quickly evolving."

Strategist, retail banking, United States



Yet businesses seem increasingly daunted by the task

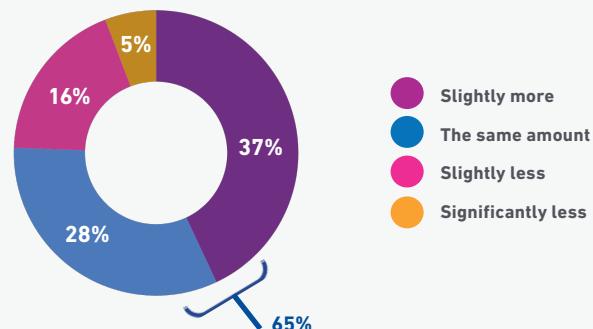
Businesses are aware of the prevalence of fraud in the marketplace, and the degree to which fraudulent activity has an impact on their business. In fact, Sixty-five percent of businesses are detecting the same or more fraudulent activity (Figure 8). Why has fraud become so pervasive and why have businesses struggled to keep up?

The great irony is that the weapon against online fraud is also the source of its vulnerability. The existing account setup process requires consumers to provide extensive personal information, answers to secret questions and passwords. Data breaches have exposed this information to fraudsters. Once stolen, this information can be used to facilitate fraudulent activity, giving personal information genuine value in illicit markets. As the potential windfall from digital fraud grows, so does the cybercriminal's motivation to stay ahead of the latest detection strategies and technologies.

"Our systems are not good – partly because we're taking three different sets of systems and combining them into one." CMO, online/brick and mortar retailer, United States

Cybercriminals are forever advancing the sophistication of their methods. Fraud is now moving between channels — such as web, call center, mobile, etc. — and new schemes, such as synthetic fraud (where criminals combine real and fake information to create a totally new identity), are constantly evolving.

Most businesses are experiencing the same or more fraud losses



Q: In the past 12 months has your business **detected** more, less or the same fraudulent activity?

Figure 8



Business executives aren't very confident about their ability to protect their organisation and their customers from fraud (Figure 9). They admit that any existing measures were the product of reactive rather than proactive initiatives. Legacy technology challenges (integrating new and old solutions) also present barriers.

As businesses make strides in introducing innovative ways for customers to open accounts and/or transact online, they are still faced with challenges to overcome.

Traditional solutions relied on behaviour patterns that helped businesses detect fraud. New solutions mean new online behaviour patterns, and the old benchmarks used in detecting anomalous activity that might signal fraud are no longer reliable. Consequently, as businesses innovate the digital experience, they feel increasingly vulnerable and not very confident in their ability to spot fraud (Figure 9).

54% of businesses are only "somewhat confident," in their ability to detect fraudulent activity compared to only 40% who are very confident

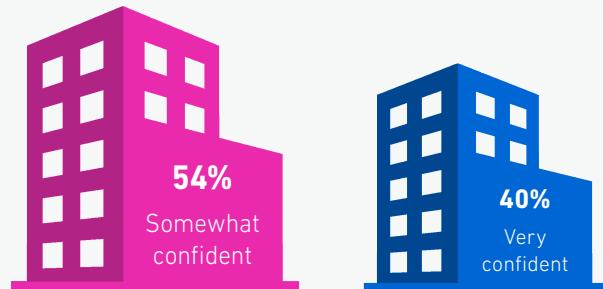


Figure 9





Perfect fraud prevention cannot come at the expense of happy customers

Not surprisingly, pragmatic business executives focus on what they can control. In a climate where businesses aren't very confident in their ability to address the ever-moving target of fraud detection, they choose instead to focus on happy customers as simply a cost of doing business. In other words, many businesses prioritise convenience over security and have come to terms with acceptable levels of losses.

Businesses use a variety of fraud detection and prevention methods, but still rely on passwords as the top form of authentication.



Figure 10

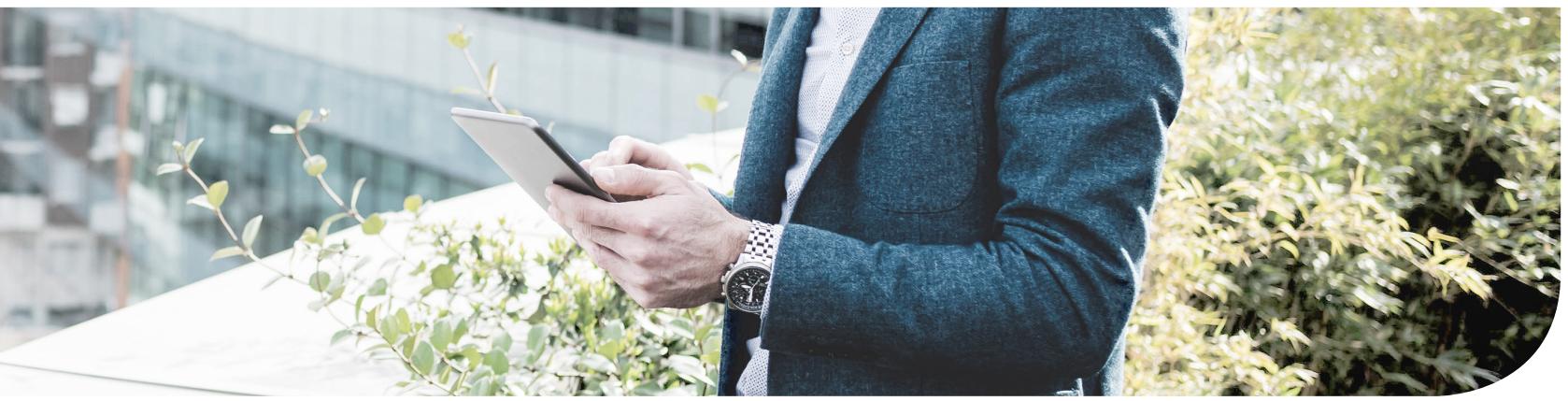
As such, there is uncertainty about how much to invest in advanced fraud detection and authentication solutions out of concern for disrupting the customer experience.

Businesses are forever grappling with the tension between managing fraud and maintaining a positive customer experience. In most cases, the latter wins out, as evidenced by their willingness to accept higher fraud losses from authentication protocols that they concede might be deficient, but do not disrupt the user experience.

Whether it's opening a new account, logging into an existing account or making a transaction, more than 50 percent of businesses say they still rely on passwords as their top form of authentication (Figure 10). Passwords win out among business leaders as their top form of authentication mainly because they are well-understood and customers have grown accustomed to them.

That said, while passwords, security questions and one-time passcodes are all among the top authentication methods used by businesses today (Figure 10), leaders concede that they are not as secure as other options.

They cite lack of resources and budgetary constraints as barriers to adopting these more advanced authentication methods. Ironically, given their focus on the customer experience, it is precisely these advanced methods that will likely enhance that very experience and simultaneously reduce exposure to fraud. So why aren't businesses using them?



Businesses might need to lead customers to better solutions while keeping them happy at the same time

Some businesses say that their slow adoption of more advanced authentication methods reflects their focus on the customer experience. That their customers favor more familiar, time-tested methods like passwords. Ironically, those methods just might be compromising the experience they are advocating for by introducing an unintended nuisance and security risk. One-quarter of consumers have forgotten a username or password within the past six months.

Time-tested methods — like passwords — may do more harm than good for the customer experience



of consumers have forgotten a username or password within the past 6 months

More than a third (37%) change their password less than once a year, with only 19% actually changing their password at the recommended time



Top three barriers encountered when banking online



- 🚫 Forgotten username or password
- 🚫 Locked out for mistyping a password too many times
- 🚫 Secret or personal questions prior to access being granted.

Figure 11

More than a third (37 percent) change their password less than once a year, with only 19 percent actually changing their password at the recommended time. Further, the top three barriers encountered when banking online are forgetting a username or password, being locked out for mistyping a password too many times, or having to answer secret or personal questions prior to access being granted (Figure 11).

It's not as if businesses are resigning themselves to fraud. Quite the contrary, their approach to fraud prevention errs on the side of suspicion and detection (71 percent) versus permission and trust (29 percent) (Figure 12). They are clearly sensitive to the costs associated with fraud in dollar terms. Over 67 percent say that a "fraudulent transaction not declined" is costlier to the business than a "legitimate transaction that is declined" perhaps not taking into account the cost of a negative experience (Figure 13). However, 69 percent are also concerned with the number of incorrectly declined customer transactions (Figure 14) from overzealous fraud detection. That concern likely stems from the possibility of lost revenue, lost potential new customers and a compromised experience for existing customers.

"Our service desks are getting tons of calls, most to do with password changes or help because users forgot their password. If we can do more on the self service end, it would be tremendous, a reduction in the call volume." CIO, online retailer, United States



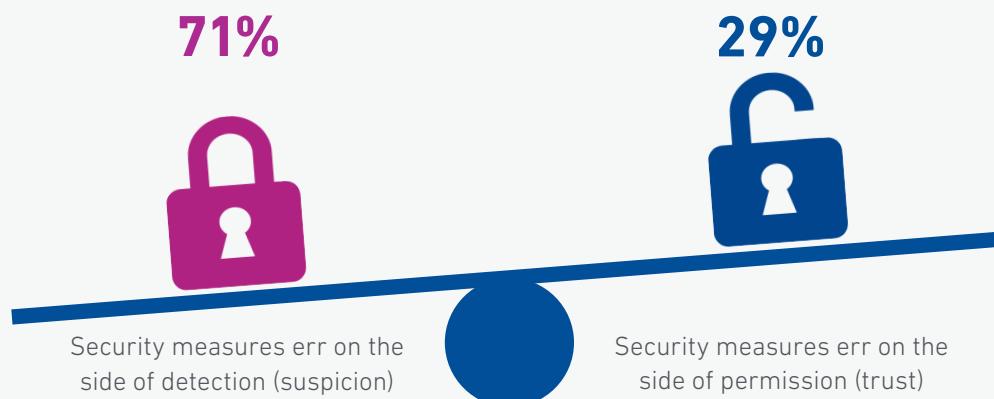
Business executives are looking at the costs and benefits when considering more advanced authentication methods. Ultimately, they agree. The ability to more precisely identify the customer (versus detecting the fraud) will drive revenue. However, they are concerned that costs associated with more modern fraud detection would offset any gains from the incremental transactions.

Thus, a conscious choice to prioritise the customer experience explains why business executives stick with existing, and sometimes inadequate, solutions.

When considering their authentication methods, businesses also recognise the need to bring the customer along. Most business leaders we spoke to agreed that consumers would need some sort of incentive to change or adopt new measures (such as biometrics), unless otherwise led on a mass scale by brands like Apple, Google, Amazon or Facebook to a new customer experience feature that dramatically improves their own experience.

The majority of companies plan to be competitive in fraud detection and mitigation, while only 35 percent plan to be a leader (Figure 15). Among those businesses identified as "slow to follow," banks seem slightly more comfortable than retailers in introducing advanced authentication methods. While still taking a conservative approach to introducing these more advanced methods, banks are particularly keen to improve the clunky, high-friction digital onboarding experience most customers feel when opening a new account on their mobile device.

When it comes to the impact on revenue, businesses look at the impact of both detection and permission-based security measures

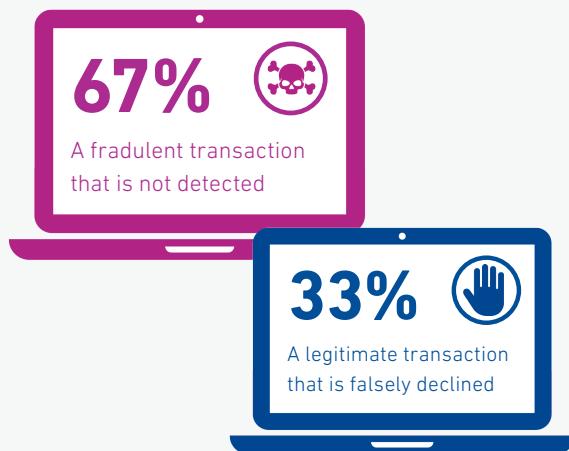


Q: What is your best guess as to the impact your security measures are having for preventing fraud? Security measures that err on the side of detection (suspicion) and probably declining more transactions than warranted based on incorrect assessments of these transactions as fraudulent when in fact they are legitimate? Or, security measures that err on the side of permission (trust) and are probably approving more transactions than warranted based on incorrect assessments of these transactions as legitimate when in fact they are fraudulent?

Figure 12



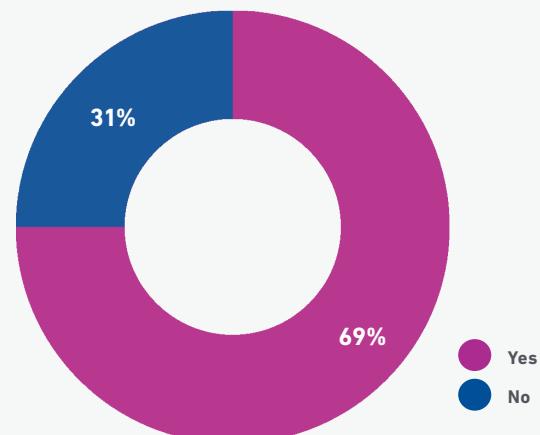
Businesses err on the side of suspicion and detection versus permission and trust



Q: Which is more costly to your business?

Figure 13

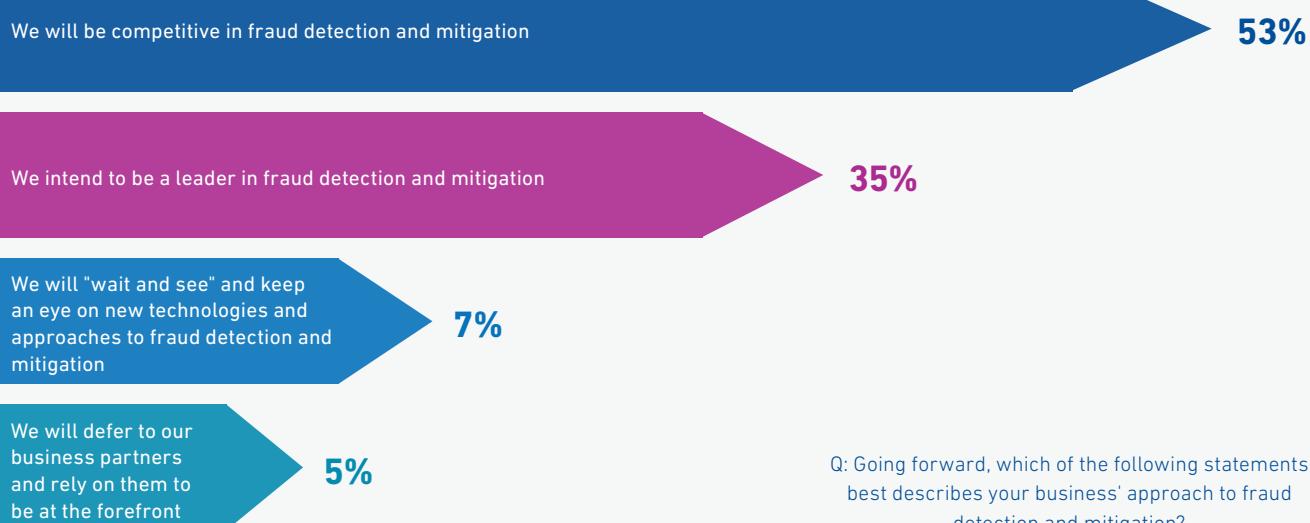
Businesses are concerned with the number of incorrectly declined customer transactions



Q: Is the legitimate number of transactions that are incorrectly declined a concern to your business?

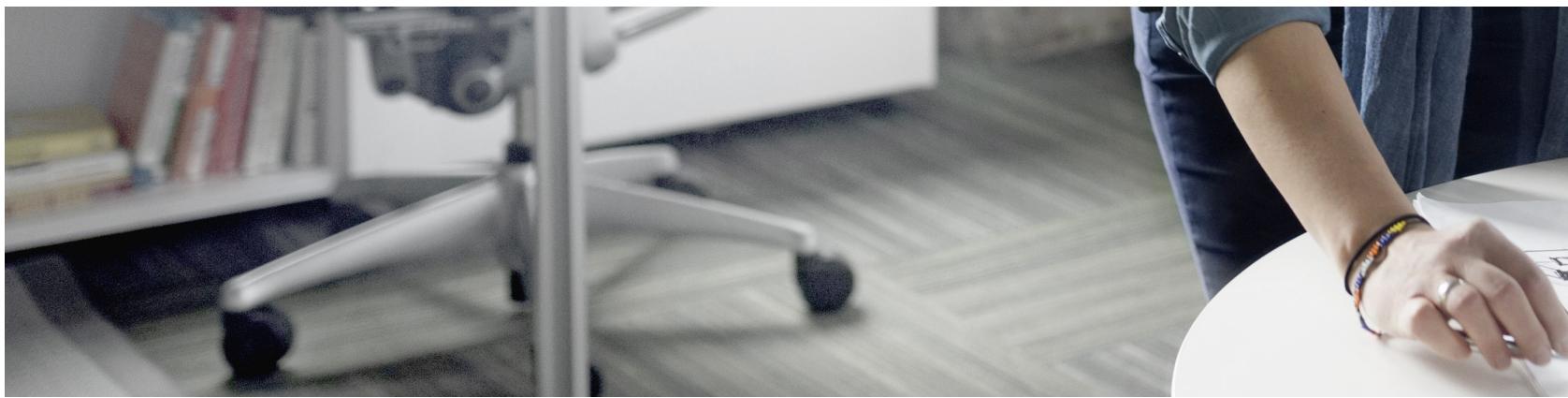
Figure 14

Most companies will be competitive in fraud detection and mitigation, not a leader



Q: Going forward, which of the following statements best describes your business' approach to fraud detection and mitigation?

Figure 15



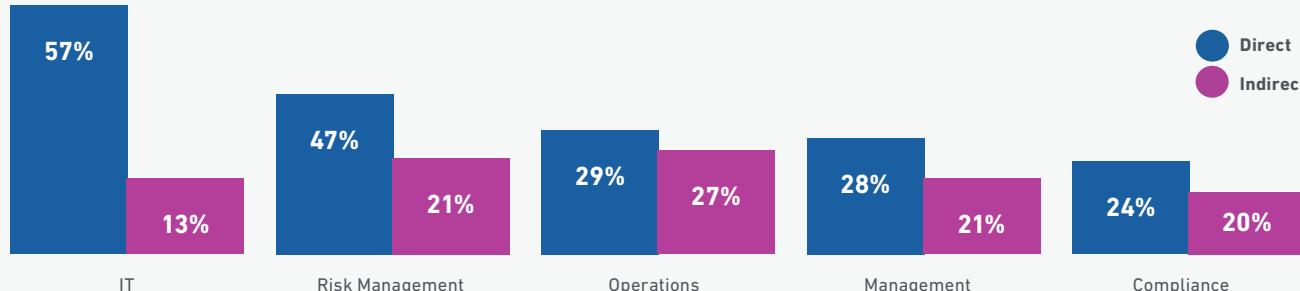
Businesses are conservative when it comes to trying new solutions

Eighty-four percent of businesses said that the burden of fraud risk mitigation would be reduced if they were certain about the identity of a customer (Figure 19). The good news is that businesses across functions want to be more proactive and implement a more progressive approach to fraud risk management that balances detection with the customer experience. Who can help align these goals to ultimately benefit the consumer? Businesses lean on IT when making decisions for investing in both fraud risk management and customer experience solutions (Figure 16). Considering all of the teams directly and indirectly involved, IT serves a critical role in bringing multiple solutions together. However, these teams require time and resources to integrate new solutions. If under-resourced, these teams can become a hindrance to the timely adoption of more modern and advanced approaches to fraud risk management.

Business executives have expressed concern of their customers perceiving that they have fallen behind in providing comprehensive protection. Seventy-five percent expressed interest in more advanced measures that had no impact on the digital customer experience (Figure 17). This varied across the 11 countries with the United States, India, South Africa and China making this a significantly higher priority.

Yet while more passive authentication and fraud prevention methods are available, businesses are not using them as frequently. Internal challenges remain when it comes to prioritising authentication and fraud prevention measures versus other aspects of the customer experience that might be easier wins (namely customer engagement projects such as instant email confirmation or a transaction summary screen before purchase confirmation features) (Figure 18). Not only are IT teams required for evaluating and integrating the new technologies, represented across multiple groups, their involvement as a key stakeholder in those investments decisions is increasingly critical.

Businesses lean on IT teams when it comes to investing in fraud and customer experience solutions



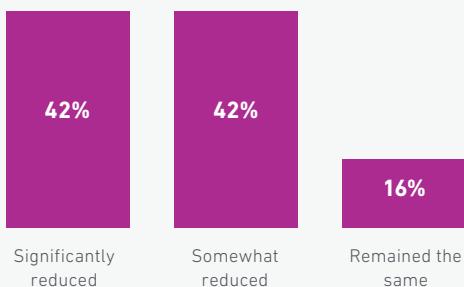
Sales, finance, marketing and accounting teams round out the list, with indirect involvement in decisions.

Q: Please indicate which department or business group has direct responsibility for customer authentication and fraud prevention. Now, please indicate which department or business group has indirect responsibility. [from list shown]

Figure 16



84% of businesses said that if they were certain about a customer's identity, the need for fraud risk mitigation would be reduced.



Q: How much risk mitigation work would be reduced if you were certain about the identity of your digital customer? Remained the same, somewhat reduced, significantly reduced.

Figure 19

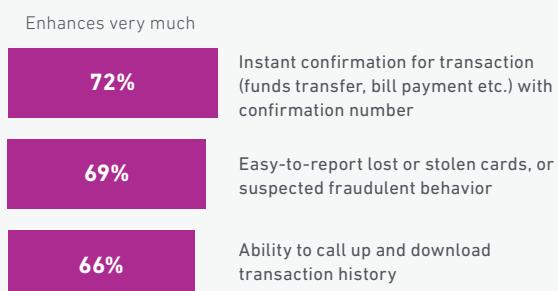
75% of businesses said, "We would be very interested in more advanced security measures and authentication"

US	India	S. Africa	China	Spain	Brazil
88%	87%	84%	79%	78%	77%
Australia	UK	France	Singapore	Turkey	Overall
75%	66%	65%	65%	59%	75%

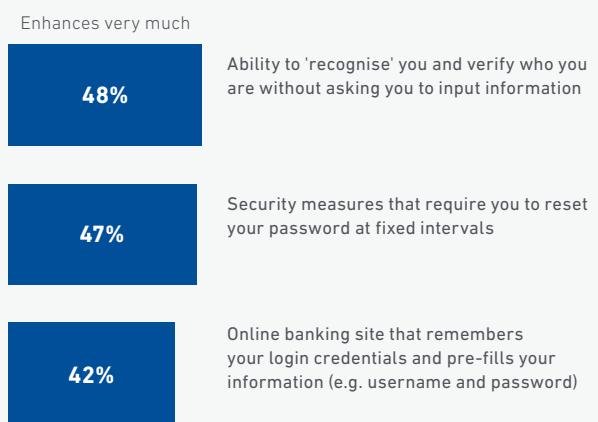
Q: Please indicate how strongly you agree or disagree [with the following statements] when it comes to the digital experience you are offering customers using the following scale - disagree strongly, disagree somewhat, neither agree nor disagree, agree somewhat, agree strongly.

Figure 17

Top three features that would enhance the online banking experience for customers, and make them feel secure



In contrast, while aiming to provide security, these features do less to enhance the online customer experience



Q: To what extent do each of the following either enhance or detract from your online banking experience? [from list of predetermined activities]

Figure 18



Conclusion

Fraud is an ever-present and growing risk. For digitally-minded businesses, managing fraud risk is a delicate balancing act between fraud detection and the customer's digital experience. While consumers currently tolerate friction to varying degrees in the interests of their own protection, the future state of eCommerce can promise a frictionless customer experience that proves as secure, if not more secure, than their experience today.

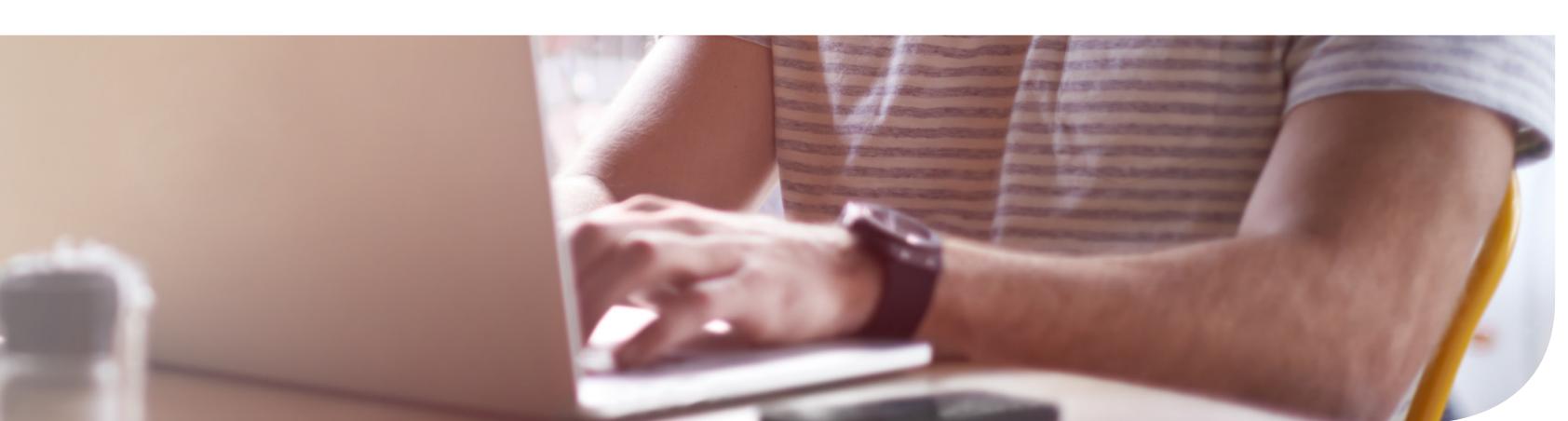
To keep up, businesses could make meaningful investments in customer recognition tools. They could set their sights on building trust through technology without disruption to protect the customer experience. But will they?

We understand that some businesses are finding it difficult to proactively implement advanced authentication methods that will accurately identify their customers, out of concern for disrupting the customer experience. Customers are used to the current level of friction. It makes them feel protected. While customers would be happy with greater convenience, like using a fingerprint instead of a password, they aren't ready for the visible signs of security to completely go away.

Customers want to be recognised and businesses want to address the growing fraud they are experiencing. Advanced authentication methods — such as device intelligence or behavioural biometrics — could help address both without adding friction to the online experience.

We believe that the more certain you are about a customer's identity, the easier it will be to spot fraud. Simply put, if you can recognise your customer, you can recognise fraud. When it comes to managing fraud risk, there is not a global one-size-fits-all solution. But there is a promising way forward. As we see it, customer recognition delivered through advanced, multi-layered solutions tailored to the customer experience is the future of fraud prevention.





Methodology

In June to October 2017, Experian conducted research among 5,500 consumers ages 18 — 69 and 500 businesses across banks, financial institutions, card and payment providers, online and mobile retailers in 11 countries including the United States, United Kingdom, Brazil, Singapore, China, India, Australia, France, Spain, Turkey and South Africa. Findings were further validated by over 20 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).

Related research

[Fraud Management Insights 2017: Trust, Identity and Engagement in a Digital World, Experian APAC](#)

[Annual Fraud Indicator Report 2017, Experian UK](#)

[The New Frontier: Unlocking the Power of Data, Experian EMEA](#)

[Synthetic Identities: Getting Real with Customers, Experian US](#)



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 organisation fight fraud?
Contact us or call (888) 727-8330**



www.experian.com/da

© 2018 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.

01/18