2019 Experian Identity and Fraud Report

Asia-Pacific Edition

Introduction

Experian conducted research among more than 10,000 consumers and 1,000 businesses across 21 countries, globally. The findings were published in the 2019 Global Identity & Fraud Report earlier in the year. Given that the Asia-Pacific represents such a diverse set of markets, we have conducted a separate analysis and dedicated a report to the region.

Asia-Pacific is a unique place in the global financial, consumer and digital technology landscape. Within this vast region, is a wide range of markets that vary in size and economic maturity. It has little in the way of legacy that holds it back from fully embracing available technologies to create more meaningful relationships between consumers and businesses online. Adoption for digital banking and commerce is highest in the world among some countries in Asia-Pacific and growing rapidly in others. Nearly 90 percent of consumers surveyed who have access to an internet-enabled device reported personal banking as one of their top online activities. This is only surpassed by online shopping for goods and services, an activity that consumers in emerging and developed countries alike rank as their number one activity online. For the most part, businesses are doing a good job of delivering their products and services via the digital channel but now is the time to look at how businesses and consumers trust the online channels and how can they create greater value.

Building trust between consumers and businesses online is difficult. Unlike in-person or over the phone interactions, digital interactions lack visual and audible cues that instil trust. Customers like to be recognised and expect to be met with a personalised experience at every interaction. The top two online activities for consumers in the Asia-Pacific region are shopping followed by banking and they expect both industries to deliver relevant, convenient and safe experiences.

Yet businesses struggle to deliver on those expectations because they do not recognise their customers. When the information they hold is not aptly utilised to identify the customer – either to protect them or create personalised offers – this can create distrust. Furthermore, distrust between consumers and businesses can lead to increased customer abandonment per transaction, or worse, a damaging brand reputation.

Eighty-nine percent of consumers are aware that businesses are collecting and using their personal information and 63 percent of consumers understand the risks involved with doing businesses digitally – resolved to thinking "this is the price I pay to do things digitally." Identifying customers often relies on the personal information they have previously provided such as name, email and phone number. But businesses can put consumers at greater risk for fraud by repeatedly asking for the same information. This is because consumers tend to rotate through a small set of passwords to manage all their online accounts – regardless if it is a financial or social media account. With more available data and innovative technologies, businesses can better identify their customers and more easily spot fraud. Incorporating advanced data such as device and contextual information and new technologies such as biometrics and artificial intelligence into customer authentication and fraud management strategies can help business create a positive engagement.

Many countries have passed regulation and/or created independent programmes to create a "single source of truth" and provide banks and retailers with verified customer digital identities. Examples are, Malaysia's MyKad, Singapore's MyInfo and Thailand's Digital ID, all designed to facilitate and speed up identity verification.

Programmes like these, help to verify customer identities and meet regulatory requirements for electronic Know Your Customer (e-KYC) processes. Customer digital identities are key in balancing security and convenience for online transactions but businesses still need to be open and transparent with customers on how they use their data to instil trust and promote acceptance for data collection. Close to 60 percent of consumers express hesitation in sharing their personal data with businesses, as unease around data privacy is widespread.

In fact, 81 percent of consumers feel strongly that it is important for businesses to be transparent about how their personal information is being used. Countries globally are adopting similar Open Banking regulations first started in the United Kingdom and in Asia-Pacific we see this happening in Australia and Hong Kong. Among consumers, these regulations are viewed very favourably which has led other businesses to take notice and proactively create more transparency-inspired initiatives such as communicating terms more clearly and providing the consumer with a sense of control over the use of their information.

Consumers share a lot of personal information with businesses. While independent and government agencies and regulatory committees might be viewed to "normalise" the industries' approach to data protection and privacy, creating trust isn't about verification and transparency alone.

Fast-growing digital adoption is changing consumer behaviour across Asia-Pacific

The fast-growing adoption of smartphones and increased internet penetration has created an ecosystem that enables consumers to embrace digital technology across multiple areas of their life. One of the most embraced activities is shopping online for goods and services. Over 90 percent of surveyed consumers have made online purchases, with the most active online shoppers in Thailand (98 percent), Indonesia (98 percent) and China (96 percent). Consumers in Asia-Pacific generate some of the world's fastest growing eCommerce revenue. McKinsey & Company (2018) projects the value of Indonesia's e-commerce market alone to rise nearly eight-fold between 2017 and 2022, to an annual spend of USD65 billion[1]. Similarly, an area that is seeing a significant shift in consumer behaviour is banking, the second most cited online activity among our survey participants. 86 percent of consumers, who have access to internet-enabled mobile or desktop devices, said they conduct personal banking online, with that number being higher in countries with a well-established digital banking environment, like Australia, Hong Kong, New Zealand and Singapore, as well as fast-growing countries like India.

Despite the fast-growing adoption of digital channels, there are striking differences across the region in terms of digital readiness and capability. In emerging Asia-Pacific, government agencies and businesses are looking to improve the physical and regulatory infrastructure and availability of skilled talent and thus, tackle challenges surrounding financial inclusion, access to basic services and cyber-security. Traditional payments methods, such as cash-on-delivery, still dominate but change is underway. For example, in Thailand and Indonesia, governments have embarked on nation-wide programmes to establish the infrastructure and ecosystem necessary to enable digital payments and facilitate online trade (Spotlight 1).

Emerging economies are not the only examples where regional differences persist. As a mature economy, Japan has no shortage in advanced technology and digital infrastructure, but remains a cash-based society, dominated by traditional payment and banking channels. Automatic Teller Machines (ATMs) are wide-spread and cash continues to be regarded as a convenient and safe payment method and store of value. But change is slowly gaining momentum in Japan too, as the government seeks to double the share of digital payments from 20 percent in 2016 to 40 percent by 2027[2].

The rapid pace of digital adoption is largely driven by the millennial population and affluent members of society. As more consumers come online and establish new habits, businesses can benefit from the cost and reach advantages that digital services offer. Unlocking the benefits of new digital lifestyles will be rewarding for businesses and consumers, but is not without challenges. Consumers have higher than ever expectations for their experiences online and demand more, better and securer services. At the same time, digitally transforming service and product offerings and with it critical infrastructure can create new types of vulnerabilities. One of the main concerns among businesses in our survey is the growing risk of online fraud.

Spotlight 1: **Businesses and government agencies in emerging Asia-Pacific economies are tackling financial inclusion:**

One example of a rapidly changing economy is Indonesia – with 265 million, one of the most populous countries in the region. According to the World Bank's Global Financial Inclusion (Findex) Database, only 49 percent of the adult population in Indonesia had access to the official financial system in 2017. Businesses and regulators are working to change this. Key enablers for increasing financial inclusion are the digital transformation of services such as banking, payments and government welfare systems as well as the potential from widespread access to mobile phones. The government has formed a National Secretariat for Financial Inclusion to drive an inclusion agenda. Part of its roadmap is to link Indonesia's national biometric ID programmes to the payment system.

1 Kaushik Das et al., "The digital archipelago: How online commerce is driving Indonesia's economic development.", McKinsey & Company, August 2018.

2 Kazuaki Nagata, "Japan hesitantly moves toward a cashless society", The Japan Times, December 3, 2018.

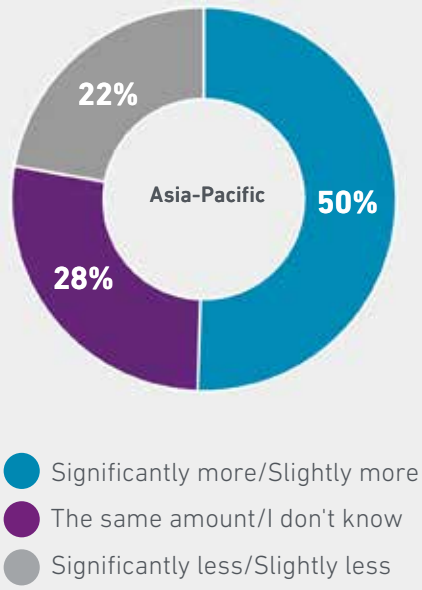
Fraud losses are a growing concern for Asia-Pacific

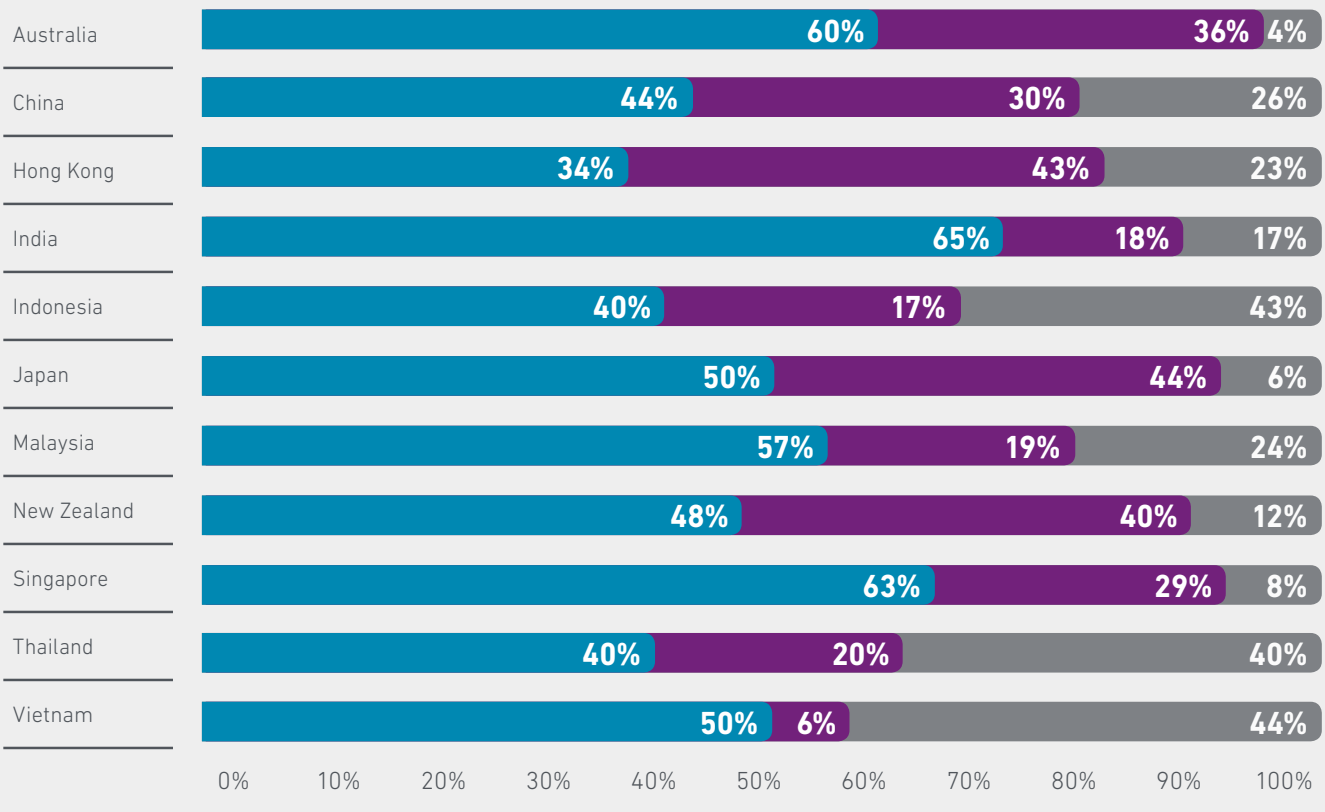
50 percent of businesses surveyed in Asia-Pacific have seen an increase in fraud losses over the past 12 months from account originations and account takeovers – both potentially damaging to brand reputation. This is slightly lower than the global average of 55 percent. Fraud losses were particularly prominent in India at a reported 65 percent and lowest in Hong Kong at 34 percent. Despite fraud losses being among the lowest worldwide (the U.S. has the highest incidence at 80 percent), businesses across all markets in the Asia-Pacific region can agree on one thing – fraud is a major concern. More than two-thirds of businesses reported an increased concern for fraud losses since last year.

67% of businesses report an increased concern for fraud losses since last year

Figure 1: Online fraud losses have increased for 50% of surveyed businesses in Asia-Pacific in the past year

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





This concern is likely fuelled by significant security incidents and breaches in recent times. While not the only examples, India and Singapore suffered from security incidents in 2018 that led to wide-spread discussions in the industry (Spotlight 2). In both countries, a particularly high share of surveyed businesses, 87 percent and 80 percent, respectively, expressed heightened concern about the potentially damaging impact of fraud on their businesses.

"The reputational damage from fraud can put the existence of our business in question."

- SVP Risk Management, Top 5 Retail Bank, Thailand

Spotlight 2: SingHealth, Singapore's electronic medical records (EMR) system, revealed that it was subject to a cyberattack in late June 2018. It is believed that the attack resulted in the theft of personal information belonging to 1.5 million patients, including the personal particulars of Singapore's prime minister. The aftermath of the attack revealed significant cyber-security shortcomings. As a result, a new set of rules for the protection of critical infrastructure systems is being implemented to minimise the risk from future attacks.

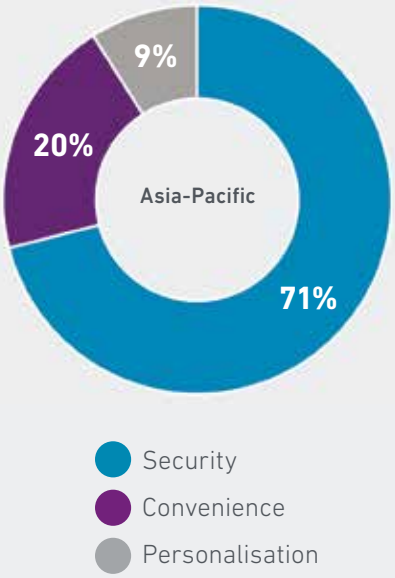
The government in India is pursuing various initiatives to drive digital adoption and secure access to basic services. The introduction of safe standards is, however, a gradual process achieved over time and with the increasing sophistication of attacks, security and losses from fraud remain a concern. This was evidenced by a security risk discovered in March 2018 in India's national identity database Aadhar, which made the identity and biometric data of more than 1.1 billion residents enrolled for the programme vulnerable to fraud through identity theft.

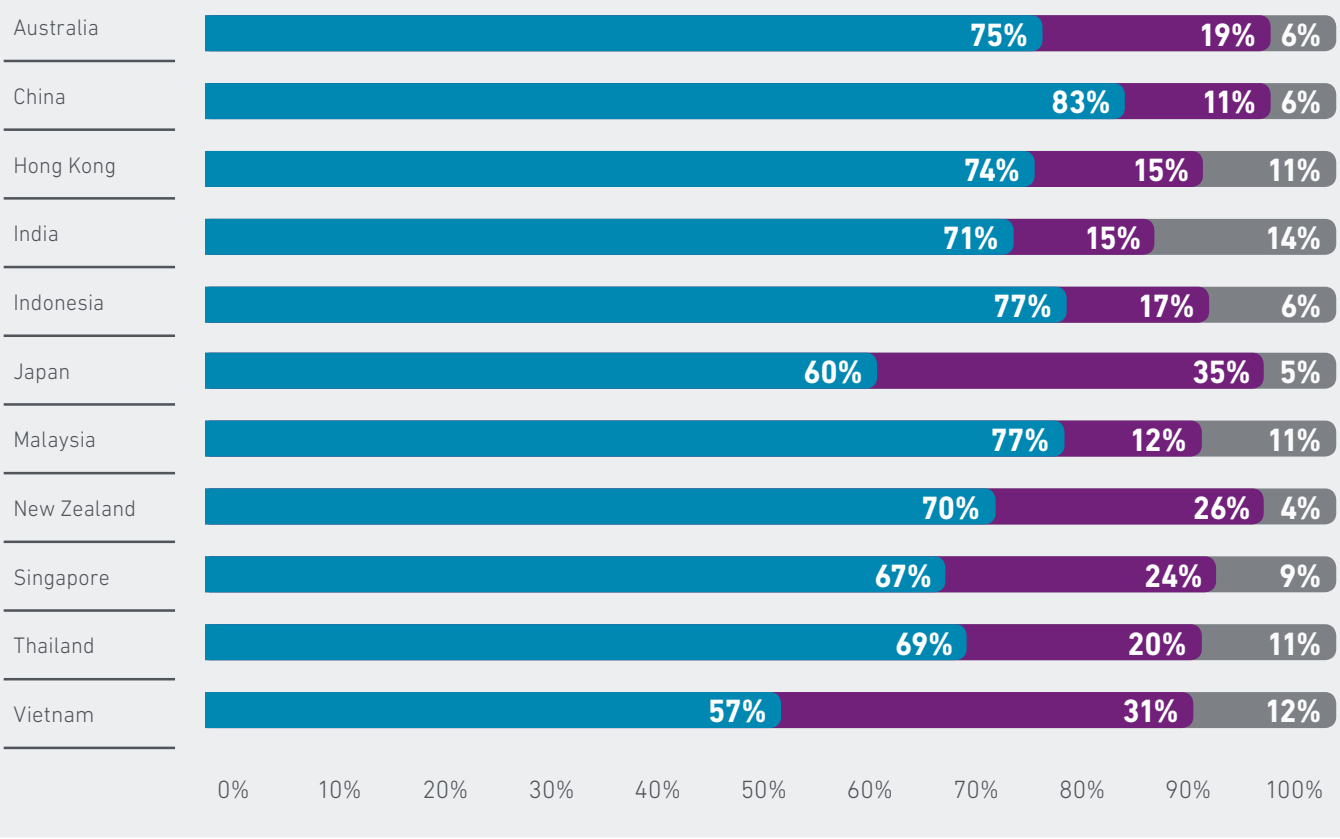
Consumers want greater security without giving up on convenience

71 percent of consumers say security is their number one priority during their online experience, followed by convenience and personalisation, at 20 percent and 9 percent, respectively (Figure 2). Security scores particularly high in emerging markets like China (83 percent), Indonesia and Malaysia (both at 77 percent), but also developed markets like Australia (75 percent). However, most businesses tend to focus on offering a convenient experience first. 58 percent of businesses believe it's better to err on the side of permission and, as a result, risk the cost of fraudulent transactions as part of doing business online to create a more convenient online experience. By comparison, 54 percent use the information to create a more secure transaction. This suggests a mismatch between what is ultimately important to a customer in their online experience illustrating a tension between security and convenience.

Figure 2: Security is the most important element of a consumer's online experience

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





Many countries have passed regulation to make online activities more secure and/or launched independent programmes that create a "single source of truth", providing banks and retailers with verified "customer digital identities" (Spotlight 3). Digital identity programmes are crucial enablers for online banking and meeting e-KYC requirements. They help to verify consumer identities and to match security considerations of banks and eCommerce players while promoting convenience for consumers.

Spotlight 3: **Government agencies and industry collaboration in Asia-Pacific are a driving force in making online activities more secure:**

In India, government agencies, such as the Reserve Bank of India (RBI), are approaching consumer online security in a proactive manner. RBI has been diligently putting measures in place to ensure that digital transactions in India are protected, for example, by making two-factor authentication and static step-up authentication mandatory online protection measures. In addition, regulatory bodies in India have reprimanded large industry players in the past 12 months for unauthorized use of personal data, sending a message to Indian consumers that there is someone looking out for their online security and protection.

In Singapore, the Cybersecurity Act 2018 came into force in August 2018, creating a framework for monitoring and reporting of cybersecurity threats and a licensing regime for data security service providers. The act aims to lay the foundations for increasing Singapore's resilience to cybersecurity threats.

Examples of digital identity programmes in Asia-Pacific:

Malaysia introduced MyKad ID in 2001, the first ID card to feature a photo and biometric data, which can be used as an ATM card and electronic purse among other applications. In 2016, Singapore launched MyInfo, which allows residents to manage their personal data profile which can then be used to pre-fill transactions for government services or other digital service transactions, such as banking applications. In India, the Unique Identification Authority of India (UIDAI) established Aadhar in 2009, one of the world's largest biometric ID systems, to replace paper-based KYC. The system makes it possible to link bank accounts, mobile sim cards and a host of other services with a unique Aadhar identity to ensure safe authentication of individuals in real-time. Thailand plans to introduce Digital ID in 2019, a system to facilitate and expedite the processes of identity verification via an online platform which will reduce the need for businesses to repeatedly verify customers at every transaction.

"Identifying the customer is one of our top priorities. If you are unable to authenticate or authorise a specific customer this can lead to massive other issues in terms of risk and fraud."

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

Consumers and businesses embrace advanced authentication methods

Sixty-six percent of businesses believe their customers are confident in their ability to protect them and they use the most up to date security measures. Over three-quarters of businesses believe that this is an improvement of consumer sentiment in the last year, however, consumer confidence in businesses' ability to safely confirm their online identity is moderate. Only 42 percent of consumers indicate that they have complete or very high confidence, with consumers in India being the most confident (64 percent) and consumers in Hong Kong (21 percent) and Japan (13 percent) expressing the least confidence.

The top four security methods that consumers encounter today are: passwords, PIN codes, physical biometrics and security questions. While consumers have continued confidence in traditional methods, consumers that have been exposed to advanced authentication methods like physical or behavioural biometrics, account information, artificial intelligence and customer identification programmes tend to have a greater confidence in these methods than consumers without prior exposure.

Physical biometrics authenticate consumers through scanning of fingerprints, retinal eye or recognition of facial features or other physical identifiers.

Examples for this are China and India. At least one third of Chinese and more than 40 percent of Indian consumers encounter advanced authentication methods regularly. Both countries fare highest in terms of consumer attitudes towards advanced authentication methods among all other survey countries. 80 percent of Chinese consumers, furthermore, regard biometrics within the top ten features that increase their online banking experience. Across, APAC three quarters of consumers find high confidence in their bank's security measures if they encounter biometrics – whether physical or behavioural – during an online banking activity.

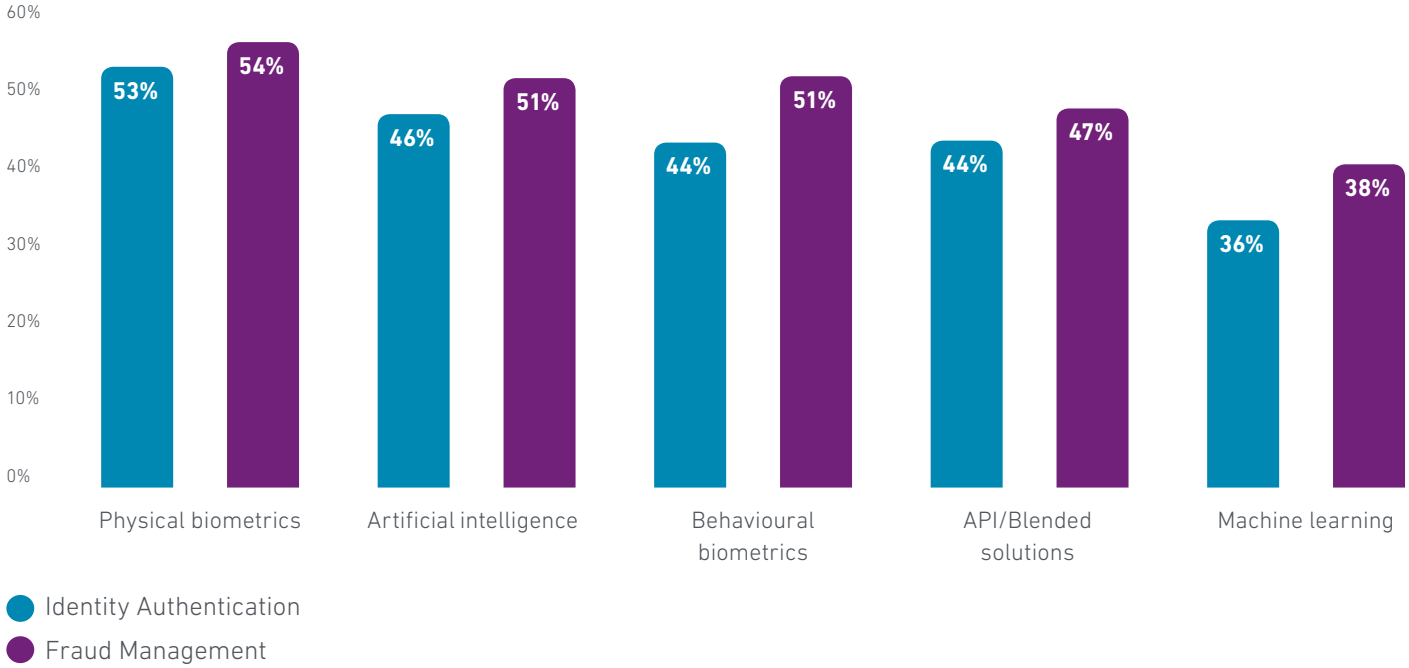
Behavioural biometrics authenticate consumers, for example, through speech patterns, keystroke dynamics, signature analysis.

Businesses in Asia-Pacific have started to embrace biometrics or other advanced methods to recognise their customers better or prevent fraud. This includes the roll-out of facial recognition for account openings or voice recognition that identifies the customers while they state the nature of their call (Spotlight 4). Around half of businesses currently consider or are actively implementing biometrics or artificial intelligence solutions for fraud management and identity authentication (Figure 3). At the same time, they continue to invest in the more traditional authentication methods with passcodes and PIN codes topping the list.

80% of Chinese consumers regard biometrics within the top ten features that increase their online banking experience

Figure 3: Around half of businesses in Asia-Pacific are actively implementing advanced authentication or fraud management solutions or have them under consideration.

Q: Which of the following does your organisation currently have under consideration or is actively implementing for fraud management/identity authentication?



Spotlight 4: **Banks in Asia-Pacific launch facial recognition**

Facial recognition and voice biometrics are gaining popularity for identity verification in both emerging and advanced economies in Asia-Pacific as businesses are investing in advanced analytics, machine learning and artificial intelligence. The premise of these methods is to offer a safe and convenient experience that reduces risks and errors in the proofing process and prevents identity theft and fraudulent transactions. A major bank in Japan is set to equip its ATMs with facial recognition technology by the end of 2019, allowing customers to open accounts. This will replace the need to submit a copy of an ID, such as a driver's license. Another example is from Thailand, where a leading bank launched facial recognition in account opening in March 2019 and intends to use the technology also for passbook account openings via a mobile app.

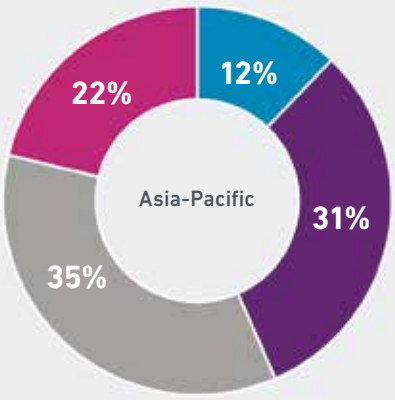
Banks in Asia-Pacific have also embraced the roll-out of voice biometrics. Since 2016, an increasing number of consumers in multiple countries, including Australia, Hong Kong, India, Malaysia, the Philippines, Singapore, Taiwan, Thailand and Vietnam, have benefited from having their identity verified while explaining their reason for calling. As consumers become used to operating their device with verbal commands, voice recognition can act as a "natural extension", offer greater security than, for example, fingerprint biometrics and remove the need for PINs, passwords or security questions.

Consumers are willing to share their personal data – if they perceive a benefit in doing so

Most consumers are willing to share personal data, such as financial, commercial or biometric data or contact information, with organisations, albeit with different degrees of confidence (Figure 4). 57 percent express concern (are not willing at all or only a little willing), while only 12 percent are very willing to share their data. Among the most confident are consumers in Vietnam, Thailand, Indonesia and India, while consumers in Japan, Hong Kong and China are significantly more hesitant.

Figure 4: The majority of consumers is willing to share their personal data with organisations, although only a small share does so very willingly

Q: How willing are you to share your personal data with the organisation you currently deal with for online?



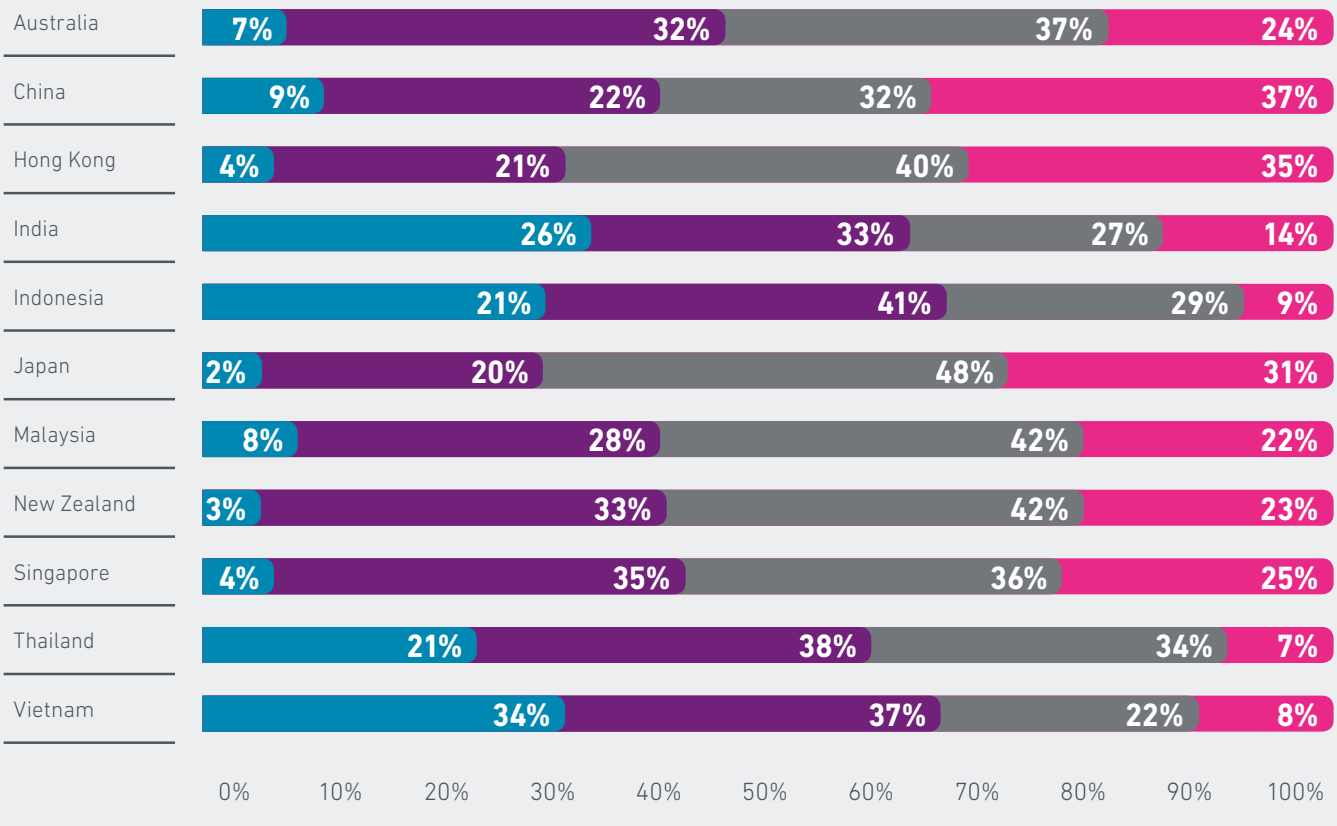
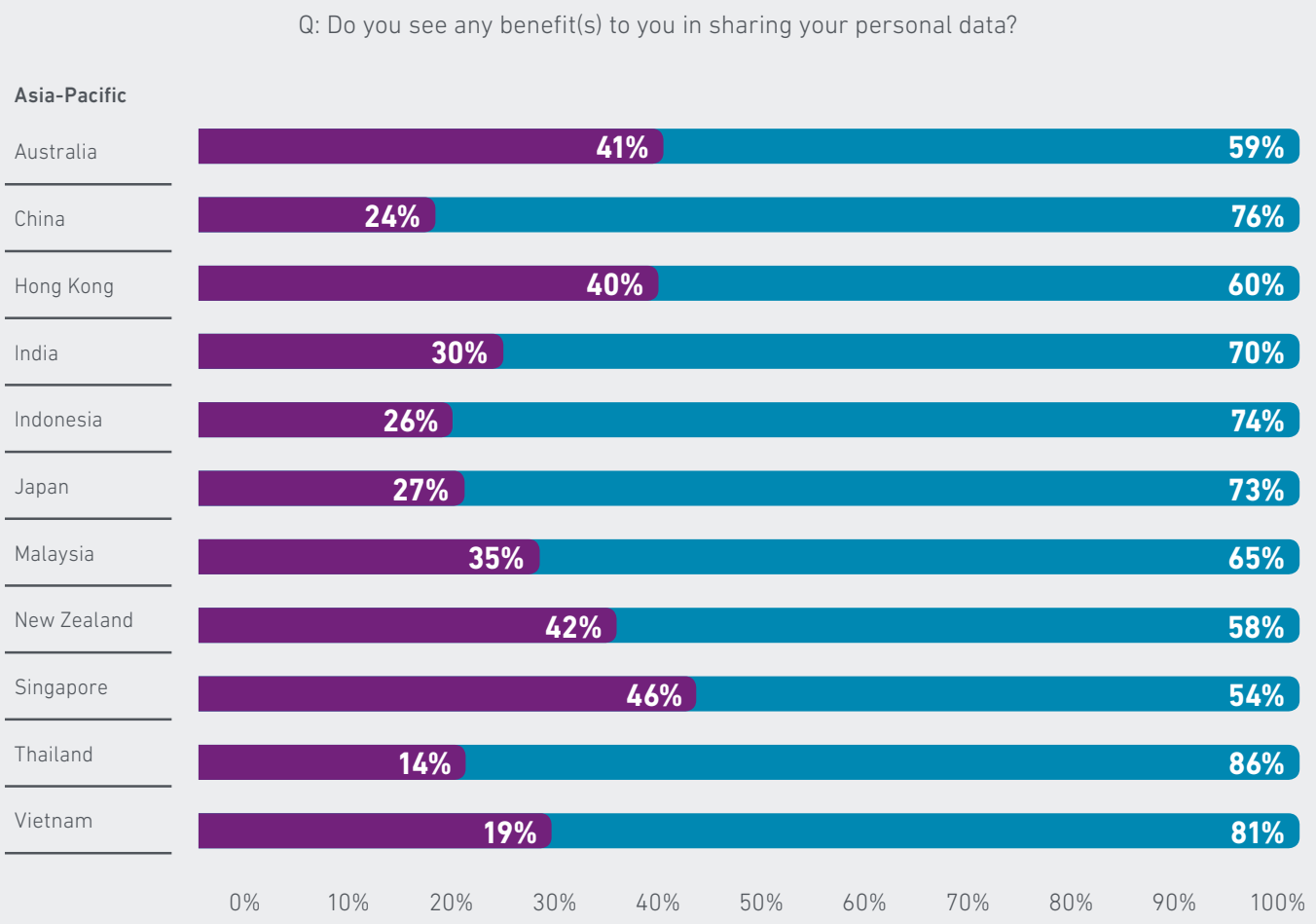
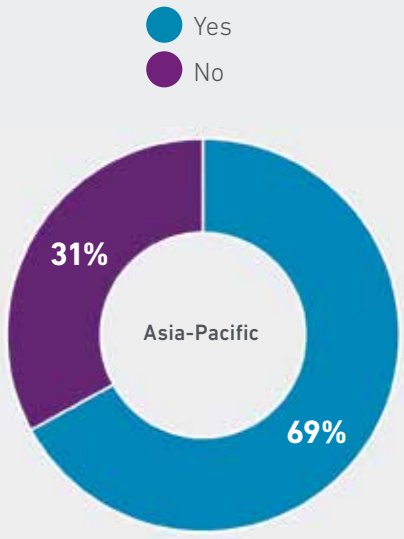


Figure 5: Most of the consumers that are willing to share their personal data perceive a benefit in doing so





Those consumers that are willing to share their personal data, do so largely with a benefit as a result in mind (69 percent) (Figure 5). For example, 73 percent are willing to go through a more thorough onboarding process when opening an online account if this enables a more convenient experience later.

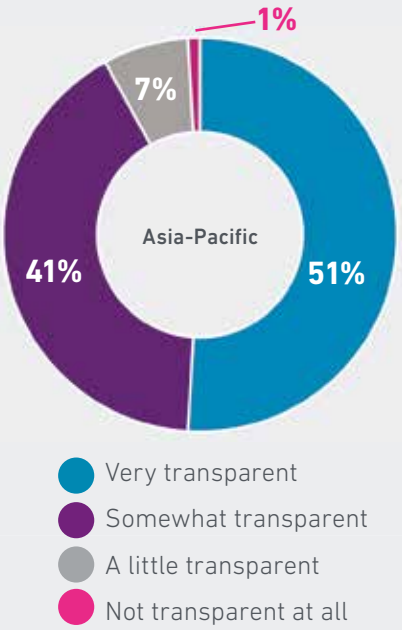
73% of consumers are willing to go through a more thorough process when opening an account if this enables a more convenient experience later

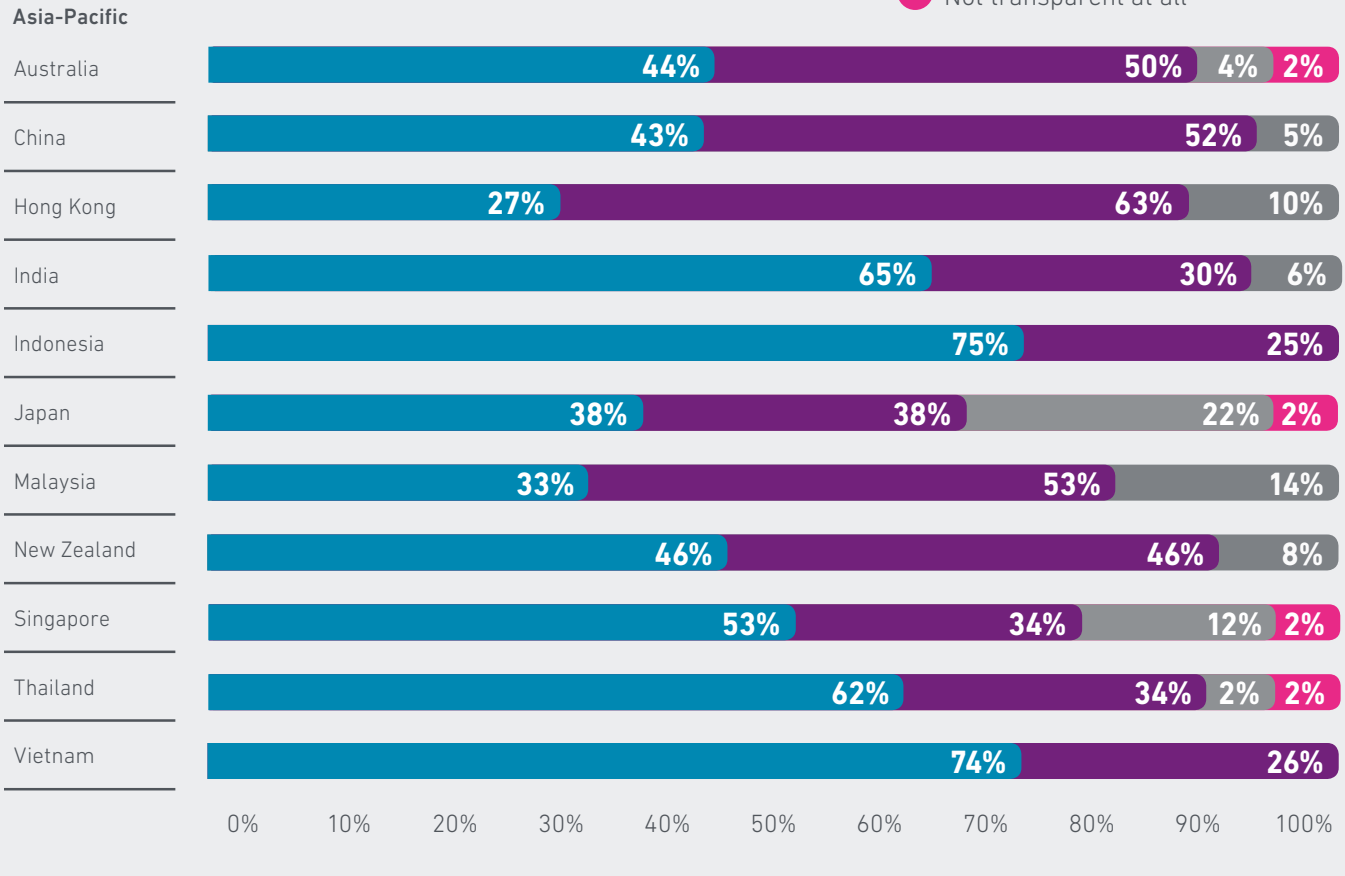
Transparency is a strong enabler for consumer trust

89 percent of consumers are aware that businesses are collecting and using their personal information. But do customers know what it is used for? Nine out of ten businesses believe they are open and transparent about the use of customer information, with most of them having active initiatives to educate consumers on what it means to "accept" terms and conditions, make it clearer how information is being used and giving consumers more control over the use of their data (Figure 6). This corresponds with a strong consumer sentiment. 81 percent of consumers feel strongly that it is important for businesses to be fully transparent about how their information is used.

Figure 6: Nine out of ten businesses believe they are open and transparent about the use of personal data

Q: How transparent are you with your customers when explaining how you use their personal data?





Triggered by the desire to increase trust, 58 percent of businesses plan to invest more in the next 6 months to proactively create greater transparency. Particularly businesses in India, Indonesia, Thailand and Vietnam, where consumers feel the strongest about knowing how their personal data is used, treat transparency initiatives as a priority.

Among consumers, regulations like Open Banking, that warrant consumer consent for the exchange, storage and use of their personal data, are viewed very favourably and can contribute to raising trust between consumers and businesses (Spotlight 5). Open Banking has led other businesses to take notice and proactively create more transparency-inspired initiatives such as communicating terms more clearly and providing the consumer with a sense of control over the use of their information. In India, regulatory bodies have reprimanded several large industry players for the unauthorised use of personal data, sending a strong message to consumers that the protection of their personal data matters.

Spotlight 5:

Open Banking is now being rolled out in Australia with the implication that banks must allow customers to share their current account information through APIs with authorised third-parties such as fintechs, account aggregators or start-ups, to name a few. As a result, customer data can be used to the advantage of the customer, for example, for income or expense verification or budgeting. This not only increases convenience for consumers but can also reduce risks associated with repeated submission of data and reuse of passwords. Crucial for the success of open banking, though, will be effective control systems for the exchange of data and storage of data by third-party providers.

81% of consumers feel strongly that it is important for businesses to be fully transparent about how their information is used

Top 3 transparency-inspired initiatives

Communicating service terms more concisely

Helping consumers feel in control of their information

Educating consumers about the use of their information

The banking, financial services and insurance (BFSI) industry and government agencies are the most trusted

Sixty percent of consumers place a high level of trust in banks and insurance companies in handling their personal data, followed by government agencies (57 percent) and payment service providers (56 percent) (Figure 7). Trust in banks and insurance companies is highest in India and lowest in Japan. Despite falling last in the region, consumers in Japan still trust banks more than any other industry.

By comparison, trust in government agencies is highest in Vietnam (69 percent of consumers have indicated a high level of trust), China (66 percent) and Singapore (61 percent). In Singapore, both the government and its regulatory arm, the Monetary Authority of Singapore (MAS), have spearheaded multiple initiatives to promote e-KYC, cyber security and data privacy. The Singapore government is taking an active role in shaping the ePayments ecosystem to advance the country to a cashless society. In 2018, the MAS announced new ePayments guidelines for financial institutions to standardise consumer protection. In addition, it announced plans to open the Fast and Secure Transfers (FAST) payments system, which has enabled real-time funds transfers between consumers and businesses across banks since its introduction in 2014, to non-bank firms. The goal is to enable non-bank firms to integrate their products and services with FAST and thus offer more convenient choices for consumers.

Rounding out the top three, payment system providers, enjoy the highest trust in Thailand (76 percent), followed by 73 percent of consumers in Indonesia and 68 percent in India placing high trust in them. As payment system providers are becoming increasingly integrated into the world of mobile banking and electronic/mobile commerce, this is likely changing the perception of consumers. Payment system providers have enjoyed the highest increase in trust in the past year, with more than a quarter of consumers indicating a positive change.

For global and Asia-Pacific consumers alike, social media sites lag considerably behind other industries with only 24 percent of consumers trusting them. Surprisingly, 47 percent of consumers within the Asia-Pacific region are still more likely to open a new online account using their social media account. (e.g. 'would you like to set-up/login using your Facebook account').

Spotlight 6: Thailand is accelerating access to digital services:

The Thai government launched Thailand 4.0 in 2016 to drive digital innovation and adoption and ultimately put Thailand at the forefront of the global digital economy. As part of the initiative, the government is creating a nationwide broadband network connecting rural villages to towns and cities and encouraging businesses in rural areas to use e-payments and e-marketplaces to sell local products and services. The initiative fuelled an increase in the launch of digital banking services, such as the installation of 550.000 electronic data capture (EDC) terminals nationwide to enable credit and debit card payments. In addition, consumers in Thailand have benefitted from the availability of mobile banking, QR code payment and PromptPay, an ID that acts as a proxy for a consumer's bank account and eliminates the need to include bank account number and name for each transaction.

Top 3 trusted industries:

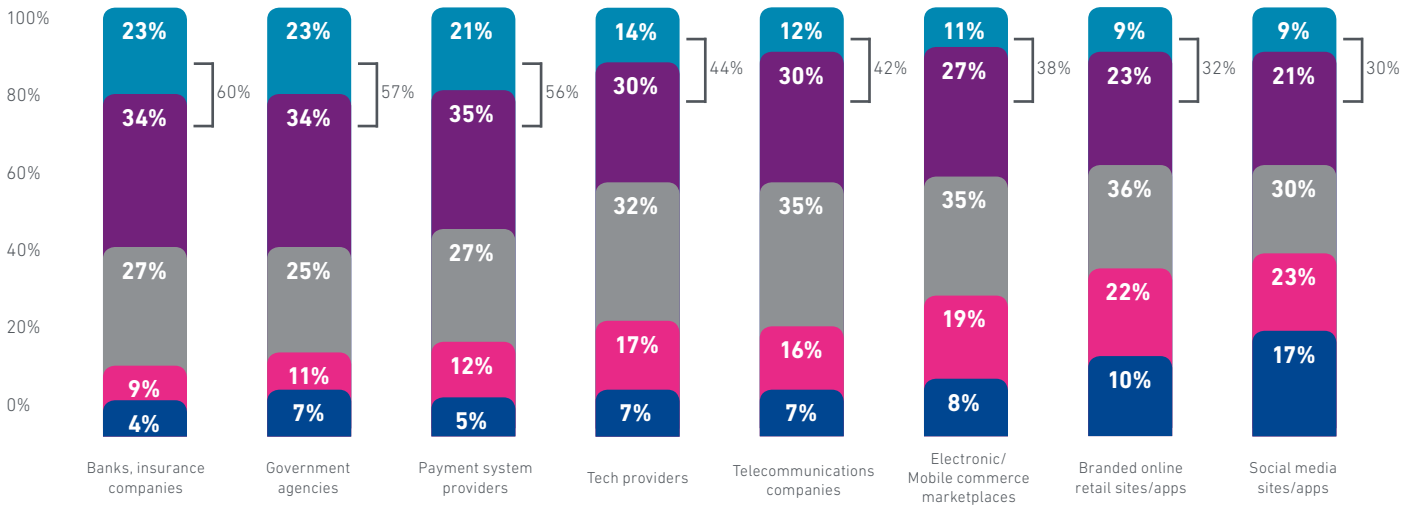
60% Banks and insurance companies

57% Government agencies

56% Payment service providers

Figure 7: The BFSI industry leads on consumer trust in Asia-Pacific

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



"Australia is very forward thinking in terms of consumer protection and regulation of the use of personal information is a good thing. It gives consumers piece of mind that their data is protected and confidence in our organisation. Trust in financial institutions has definitely gone up as a result."

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

Conclusion

Digital adoption and with it a fast-growing digital ecosystem are changing the relationship between businesses and consumers in Asia-Pacific. While businesses are striving to drive and unlock the benefits from increasingly digital lifestyles, they must tackle many challenges. Customers like to be recognised and expect to be met with a personalised experience at every interaction. At the same time, the growing sophistication of cyber-attacks including online fraud requires a matching response to guarantee the safety of personal data and safeguard businesses' reputation.

Faced with these challenges, what can businesses do to deliver both the security and convenience consumers expect? 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. Digital identity programmes that create a "single source of truth" and provide businesses and government agencies with verified customer digital identities are key in balancing security and convenience for online transactions. But building trust between consumers and businesses online is difficult. Creating transparency regarding how businesses use their customers' information and investing in the right technology for fraud management and safe customer authentication can go a long way toward creating more trust. As consumers feel strongly about how businesses use their personal data, businesses that are transparent and use the data to increase customer security and convenience can be particularly successful in establishing customer trust. In return, consumers are willing to share data and go through a more thorough account set-up process, if they benefit from it such as a more convenient log-in later. By the same token, as businesses have started to embrace advanced customer authentication methods, for example, those, that leverage biometric data, they fare well once consumers start to gain experience with them.

In general, consumer trust in businesses and government agencies is moderate to low in Asia-Pacific, with variation driven by geographical and vertical markets. Leading in consumer trust are banks, insurance providers, government agencies and payment service providers. Consumers in 5 out of 11 countries trust banks and insurance providers more than any other industry, with government agencies and payment service providers following behind. What does it take to build consumer trust, and how are businesses measuring up? We further explore different dimensions of trust between consumers and businesses in the upcoming Asia-Pacific Consumer Trust Index 2019.

India Findings

Experian India Fraud Report 2018 - 19

Introduction

In the last few years, the Indian credit landscape has seen a remarkable upsurge with strong and steady growth in the economy.

Financial inclusion, one of the key growth drivers, has led to an exceptional increase in consumers' credit appetite. And while this growth has been the harbinger of tremendous opportunities – for both businesses and consumers – it has also been the bearer of new and unseen challenges; one of these being fraud.

Let's take a look at the fraud trends and how they are changing India's credit system.

Overall Trends in Frauds

In step with the current fraud trends in the country, identity frauds and market alert frauds were the leading contributors to the overall fraud distribution.

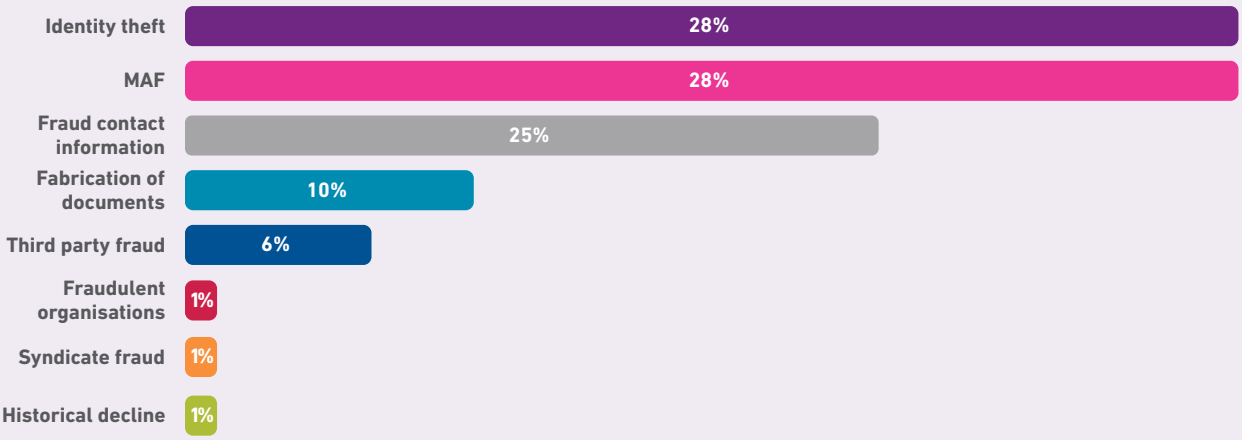


Figure 1: Distribution of different types of Frauds.

*MAF: Market alert frauds.

On the other hand, factors like identity theft and frauds by fabrication of documents saw a downhill quest.

We see a decline of 13% in the cases of identity theft.

Fabrication of documents have gone down by almost 10 percent.

Fraudulent contact information has gone up from 10% to more than 25% in the last year.

Distribution of Frauds by Product

The fraud rates are highest for credit cards whereas two-wheelers have the lowest fraud rates.

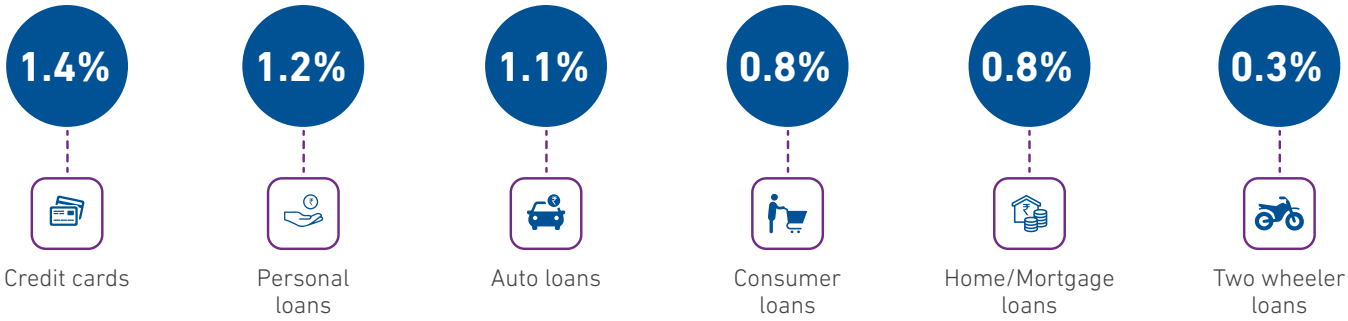


Figure 2: Product-wise Monthly Fraud Rates.

Distribution of Frauds by Geography

Delhi and West Bengal have the highest fraud rates followed by Punjab, Uttar Pradesh and Haryana.

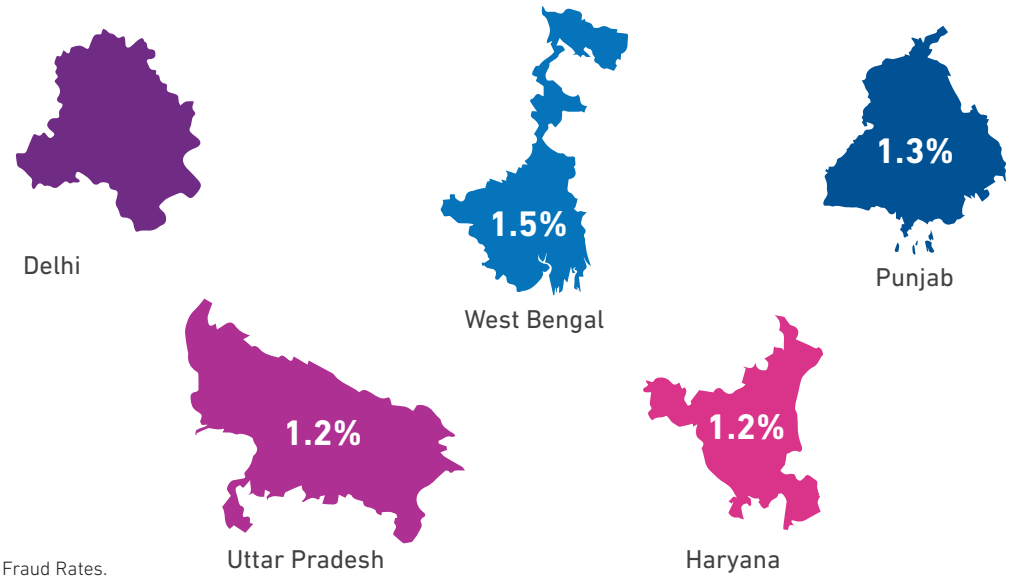


Figure 3: State-wise Monthly Fraud Rates.

Tier-Wise Distribution of Frauds

Tier 2 cities marked the highest fraud rate followed by Tier 1 cities. Though the overall volume of applications from Tier 4 cities is large the fraud rate is very low at 0.4%.

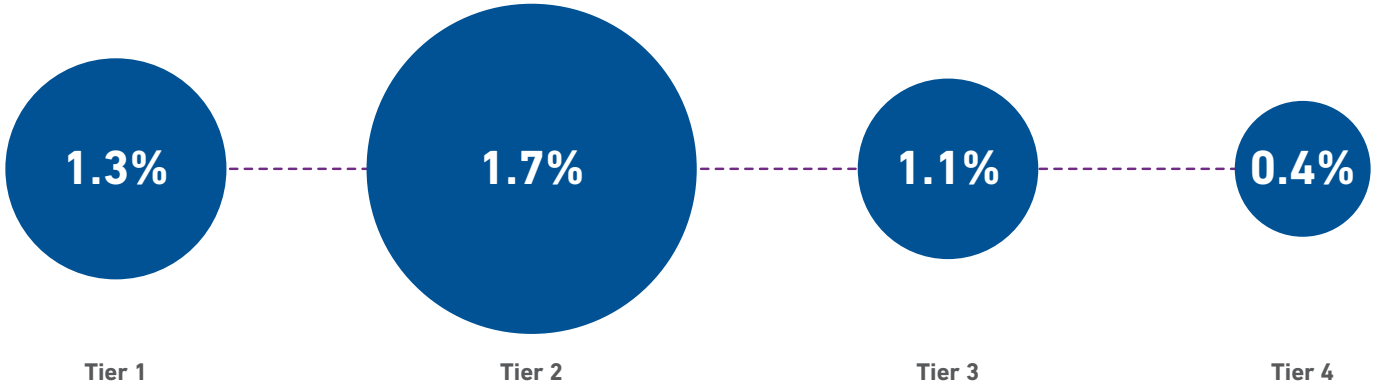


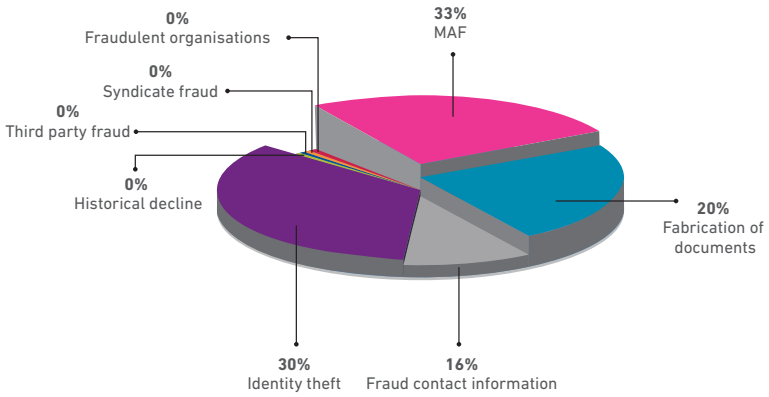
Figure 4: Tier-wise Monthly Fraud Rates.

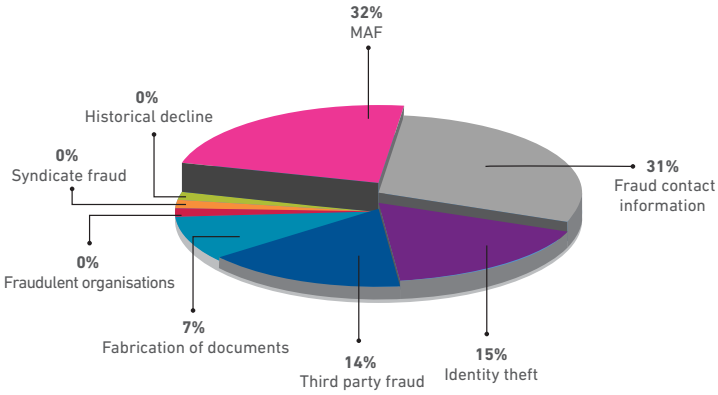
Product-wise Fraud Trends

The analysis below is based on applications that have been declined for fraudulent intent.

Home Loans/Mortgages

- The top reasons for declining applications for fraudulent intent were:
  - Market alert frauds (33%)
  - Identity theft (30%)
  - Fabrication of documents (20%)



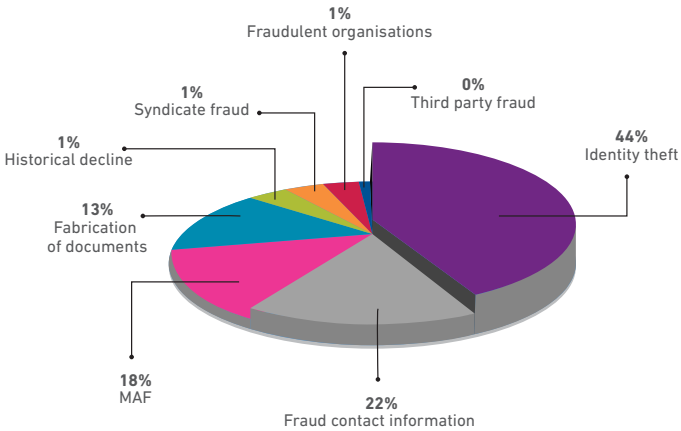


Credit Cards

- The top reasons for declining applications for fraudulent intent were:
  - Market alert frauds has seen a rise of 18% in the last year apart from being the top reason for declining applications (32%)
  - Fraud contact information was the second contributor for declining applications at 31%

Personal Loans

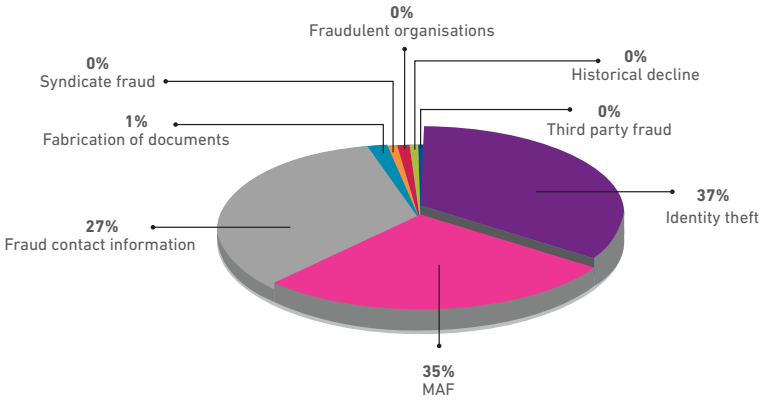
- Even though identity theft frauds saw a 24% decline in the last one year, it still remained the top reason for declining applications (44%)
- A steep rise by 25% in fraudulent contact information cases was seen in the last one year

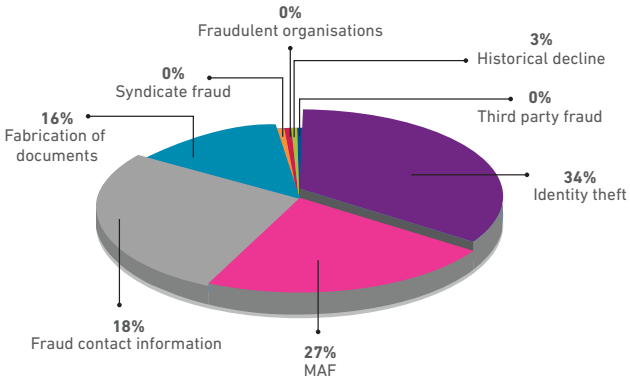


*MAF: Market alert frauds.

Consumer Loans

- Fabrication of documents as a reason for declining applications fell from 4.9% to 1.4% in the last one year while identity theft has increased from 24.4% to 27.5% in the same period



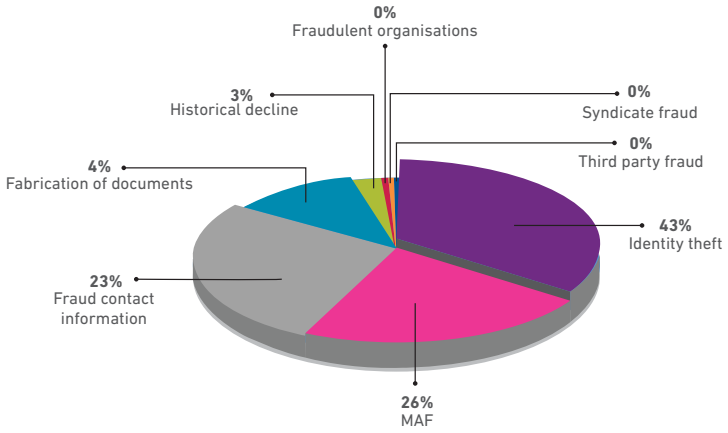


Auto Loans

- At 34%, identity theft was the main reason for decline in auto loan applications as well as increasing the percentage of frauds from 19% to 32% over the last one year
- The other contributor to decline in auto loan applications was market alert frauds (27%)

Two-Wheeler Loans

- Identity theft saw a decline of 13% in frauds last year while being the top reason for decline in applications (43%)



*MAF: Market alert frauds.

All the data in this report is from the application fraud prevention platform called Hunter used across the banking and financial services industry.

For more insights on the fraud trends in India and APac, get the 2019 Experian Identity and Fraud Report: Asia Pacific Edition.

Write to us at experian.indiainfo@experian.com

Experian Services India Pvt. Ltd.
5th Floor, East Wing, Tower 3, Equinox Business Park, LBS Marg, Kurla (West), Mumbai - 400070, India.

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 programme 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.

Learn more at **www.experian.in**

Related Research

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

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

Contact

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

Experian Services India Pvt. Ltd.

5th Floor, East Wing,
Tower 3, Equinox Business Park,
LBS Marg, Kurla (West),
Mumbai - 400070, India

experian.indiainfo@experian.com

www.experian.in

19/04/23_DA_BR