Financial Institution Study

APAC

Future-proofing Fraud Prevention in Digital Channels

GBG

Survey conducted by

THE ASIAN BANKER

STRATEGIC BUSINESS INTELLIGENCE FOR THE FINANCIAL SERVICES COMMUNITY

GBG and The Asian Banker surveyed 324 respondents from financial institutions (FIs) in six key Asia-Pacific markets including Australia, China, Indonesia, Malaysia, Thailand, and Vietnam to better understand emerging and future fraud trends in an increasingly digital world specifically for financial institutions. This study aims to gauge the digitalisation priorities of financial institutions based in the Asia Pacific and also assess their key fraud challenges and gaps in fraud control and mitigation.

Contents

Key findings

Instant gratification

for bank account application, loan, and credit card application see greater demand and rollout by financial institutions in APAC.

End to end fraud management platform readiness

is a key differentiation to driving digital product preference for 66% of APAC financial institutions. Vertical silos are still seen in 43% of APAC financial institutions, and most prevalent in digital banks.

The unbanked segment

has pivoted to be a mainstream focus as fraud technology advances.

Social engineering crimes

in particular to scams continue to be the top challenge in 2020-21.

Device integrated financial products

like e-wallet are becoming hygiene offerings for financial institutions keen in expanding to digital channels.

Upgrading to fraud management platform solutions

is a work in progress for 57% of the respondents.

Thailand, China, and Indonesia

have estimated fraud prevention budgets higher than the APAC average budget baseline.

Budgeted investment in digital fraud management platforms

by at least 52% of respondents, and are a key priority in 2020-21.

01. Trends and priorities of APAC Financial Institutions in the digital age

Key features of digital offerings

FIs maintain a strong digital proposition for their customers predicated on a robust e-banking solution and mobile banking application. A significant majority of FIs have already introduced these facilities for their customers to enable a smooth, convenient, and safe customer journey. The next-gen digital offerings have not caught up with FIs in APAC yet, with relatively few FIs offering features such as fraud alerts and instant payment stop (21%), voice-activated fund transfers (22%), and mobile phone voice assistant (25%) services.

Device integrated financial services like mobile banking (57%) and e-wallet / mobile wallet (52%) form the core of existing FI online products.

Figure 1: Current online product offerings

Priorities in digitalisation

From the research, FIs are going beyond creating a digital presence, but are ramping up the availability of digital instant gratification series of financial products. Products to help customers transact instantly are the second highest in planned online products; instant bank account application and instant loan each are in the plans for 31% of the respondents. Instant credit cards are also coming up fast on planned rollouts (29%).

In Figure 1, on-the-go banking (mobile banking app and e-wallet / mobile wallet) has already been implemented by over 52% of the respondents. Device integrated financial service like e-wallet is becoming a hygiene factor for financial institutions to compete for consumer share of voice, focused by 90% of respondents (57% currently implemented and 33% planned adoption). Respondents are considering new ways to augment mobile banking, one of the offerings which would be rolled out include P2P payment and fund transfer using mobile number (29%).

Ensuring a superior customer experience has always been an integral priority for FIs seeking to simplify the customer journey. FIs are looking to smoothen online engagement and are continuously identifying new opportunities in addressing potential gaps with their customer's digital experiences. Close to one-third of respondents are already looking at voice enabled financial services like user voice-activated fund transfer and bill payment to create even more seamless digital customer experience.

31%

are planning to offer instant bank account and instant loan

29%

are planning to offer instant credit cards

52%

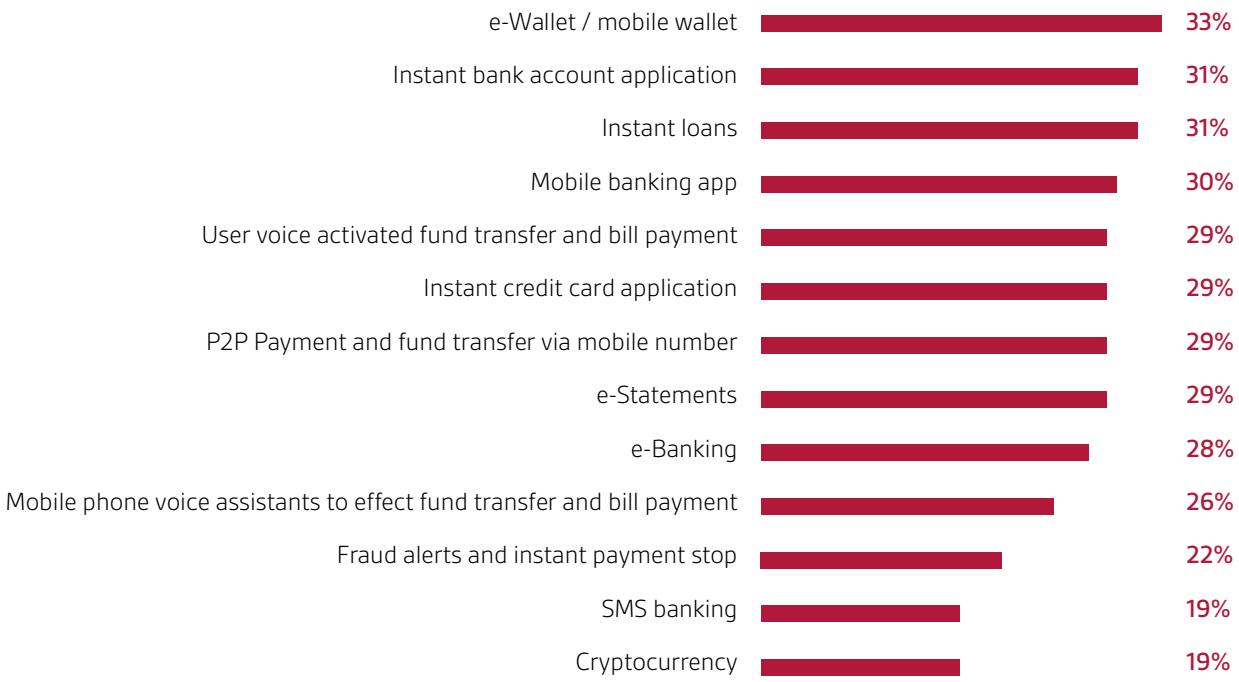
have implemented on-the-go banking (mobile banking app and e-wallet / mobile wallet)

90%

of total respondents in APAC would offer e-wallet by 2020-21

In 2020-21, FIs are looking to introduce more instant online financial products.

Figure 2: Planned online product offerings

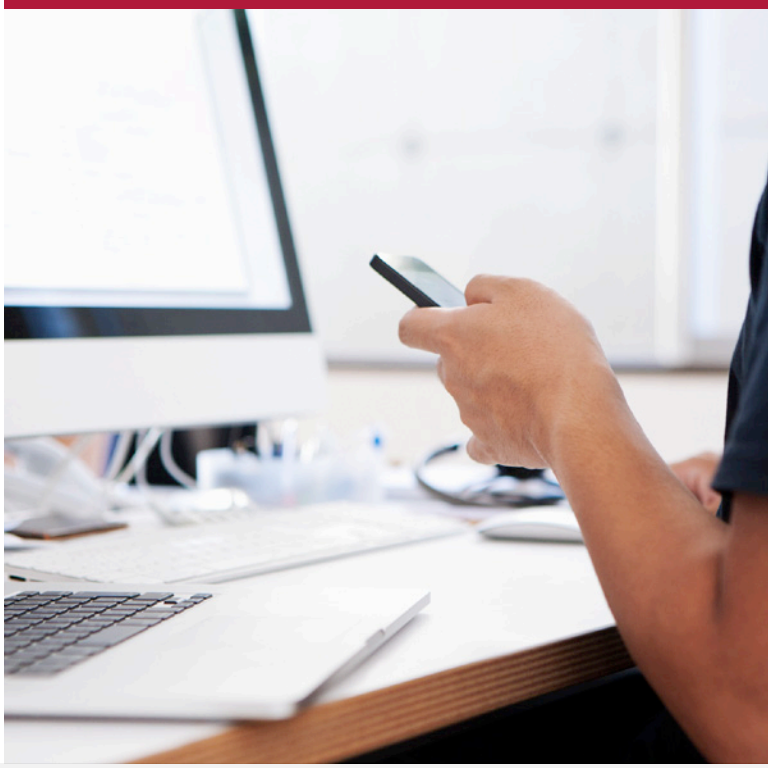


Breakdown across channels

FIs continue to maintain an omnichannel strategy to keep customers engaged while addressing pain points in a seamless and frictionless manner. On an aggregate across APAC, mobile banking and app banking are of equal importance to support retail banking transactions, while banking in branch has become the least preferred channel.

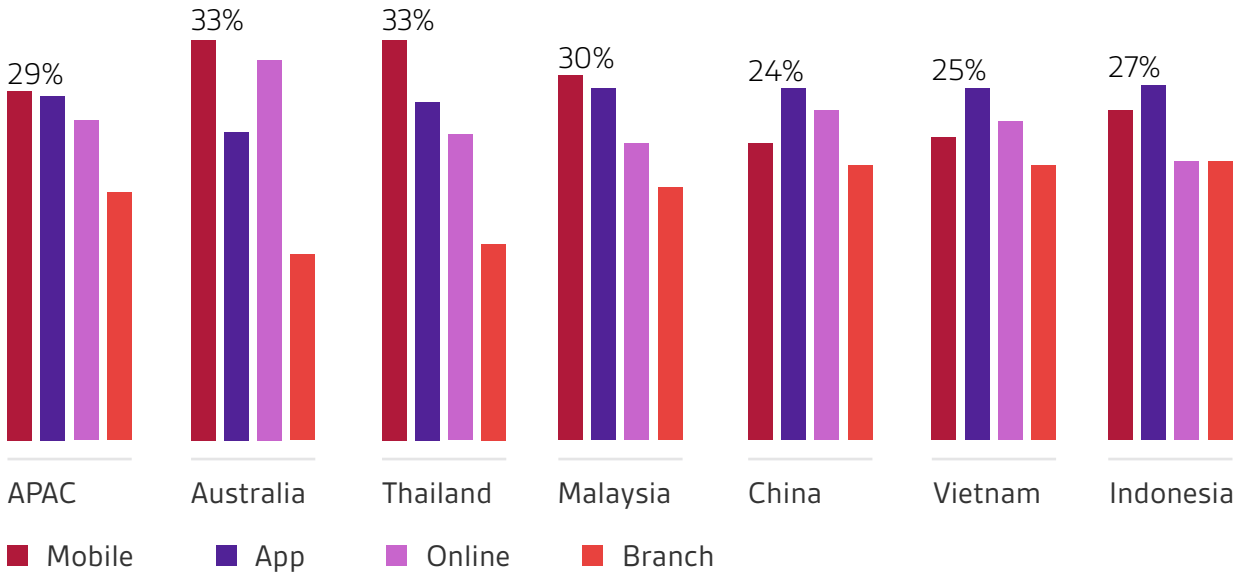
APAC sports one of the highest growth rates in finance apps. Banking via finance apps continues to rise steadily across both mature and developing countries in APAC, with a 106%[1] growth in finance apps installed from 2018 to 2019. Consumers in Indonesia, China, and Vietnam, in particular, are seen to prefer app banking over other channels today.

Digital transactions led by mobile **29%** and app **28%** dominate engagement across various countries in APAC



[1] The State of Finance App Marketing in APAC, 2020 Edition, Appsflyer

Figure 3: Channel preference in APAC

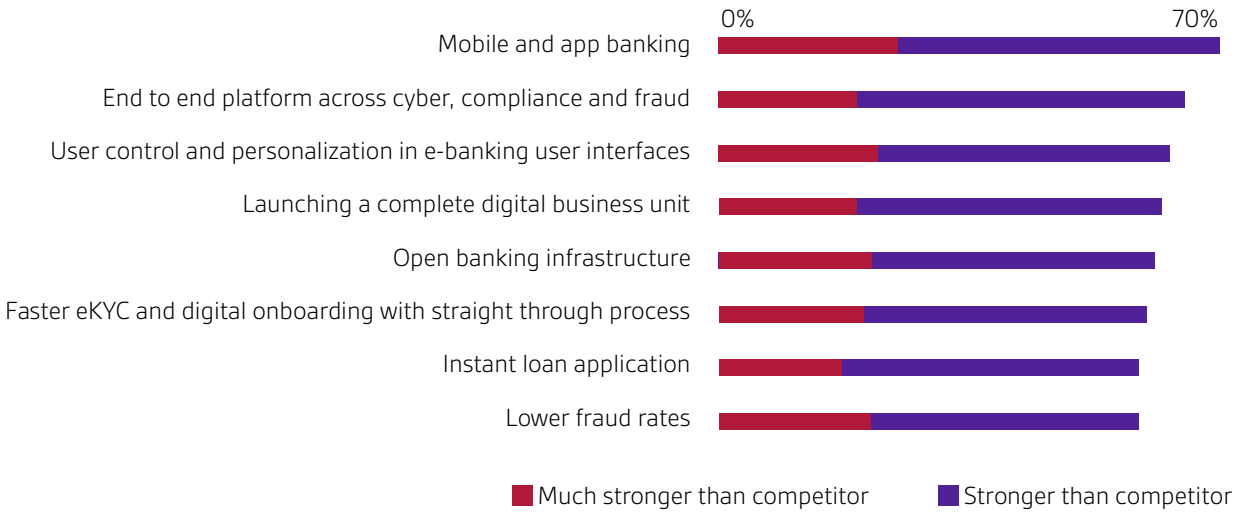


End to end fraud and compliance risk management is a key differentiation to drive digital product preference.

Differentiating digital offerings

Having the right digital product mix and infrastructure to support the desired experience differentiate one financial service provider from another. On the front end, FIs hone and create respectively unique mobile and app banking experiences (71%) as their key differentiator. On the backend, the most significant differentiation in driving digital product preference is the readiness of an end to end fraud and compliance risk management platform (66%). FIs clearly recognise and acknowledge the importance of creating digital trust and digital safety with an integrated fraud management approach.

Figure 4: Competitive differentiators in digital offerings



Key customer segments

Today, most FIs in APAC are eyeing beyond more traditional and accessible segments like white and blue-collar working professionals to new segments, in particular, the unbanked population in APAC. According to GBG's press release on extending digital fraud risk management for Southeast Asia's unbanked, new-to-credit and gig economy workers to onboard and transact easily, in Southeast Asia, about 25% of the 400 million[2] adults are fully "Banked" and enjoy full access to financial services. Almost 50% of adults in Southeast Asia remain "Unbanked" and do not own a bank account.

Accessing the financially excluded segments has always been a massive challenge for FIs; only 24% of the respondents had been targeting the unbanked. The complexities in onboarding the unbanked population arises from insufficient and fragmented data, and a huge contribution to high non-performing loans, low approval rates, and a high level of fraud.

Progressively, fraud technology has become more sophisticated to leverage on mobile data, device ID, and location intelligence to help FIs identify and onboard good actors and authentic customers more confidently. This year onwards, 32% of respondents are planning to access the unbanked and 31% underbanked. The incremental attention to these segments is set to bring the unbanked and underbanked into the mainstream segment focus from this year onwards.

The unbanked segment would become a key customer segment by 2020-21

[2] Asiaone, GBG and CredoLab partner to extend digital fraud risk management for Southeast Asia's unbanked, new-to-credit and gig economy workers to onboard and transact easily, June 2020

Figure 5: Key customer segment

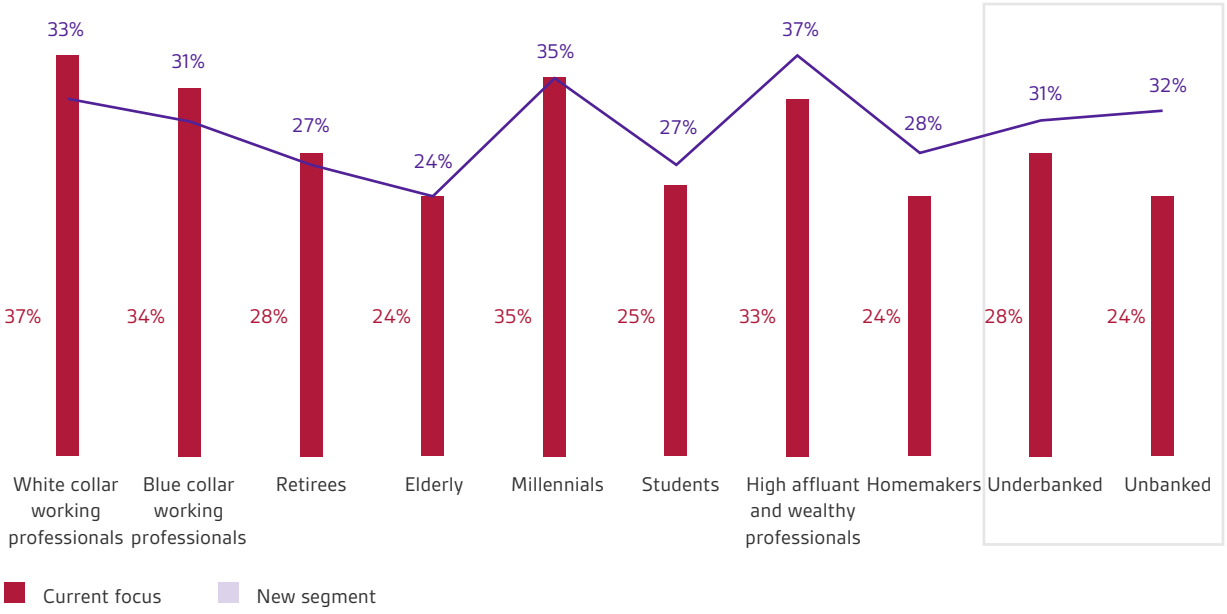
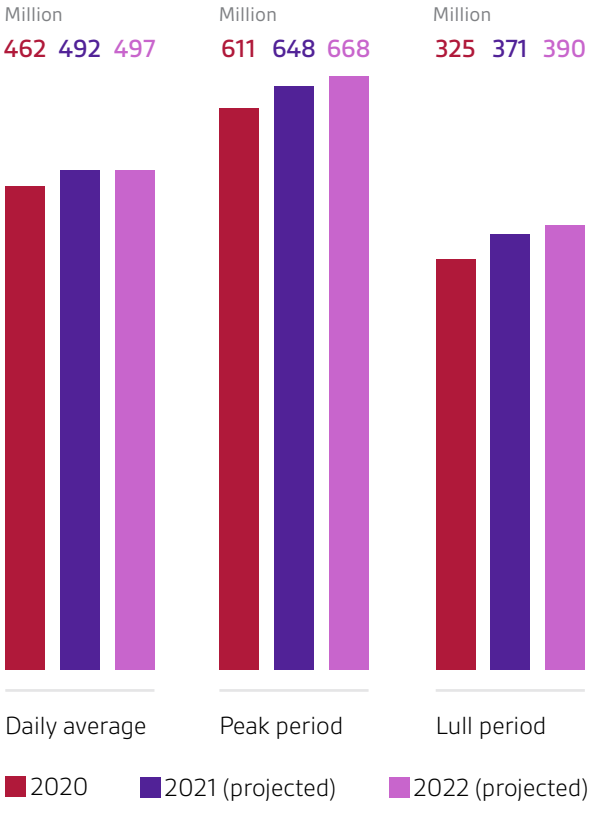


Figure 6: Volume of digital transactions in APAC, 2020 - 2022



Key drivers for peak digital volume

As the number of digital channels grows, inevitably this brings a forward momentum in the volume of digital transactions during the 2020-22 period. The average daily volume of transactions is pegged at 462 million this year with a forecasted 6% growth. Peak daily volume of transactions is 32% higher than the average daily volume and is forecasted to grow at 6% as well.

FIs expect a sustained increase in the volume of digital transactions for 2020-22

02. Key fraud and risk management challenges in digitalisation

Key challenges in increasing growing digital channels

Financial crimes 4.0, a term coined by GBG, is a mega risk trend and emerging financial crime patterns arising from the state of hyper-connectivity in today's Industry 4.0. The unfolding of digitally connected devices and greater availability of data through the sharing of personal data as a result of massive utilisation of social media, internet of things (IoT), eCommerce, cyber-physical world to achieve immediacy of transactions. With continuous streams of PII data exchanged online, fraudsters are able to easily tap into this information and use them to administer cyber fraud attacks.

The COVID-19 pandemic has also escalated the volume of cyber fraud attacks with increased online dependency. In the US, cyber-attacks rose by 238%2 between February and April 2020; in APAC, Standard Chartered Bank in Malaysia saw an increase of 90%[2] in cybercrime complaints during their Movement Control Order (MCO) lockdown

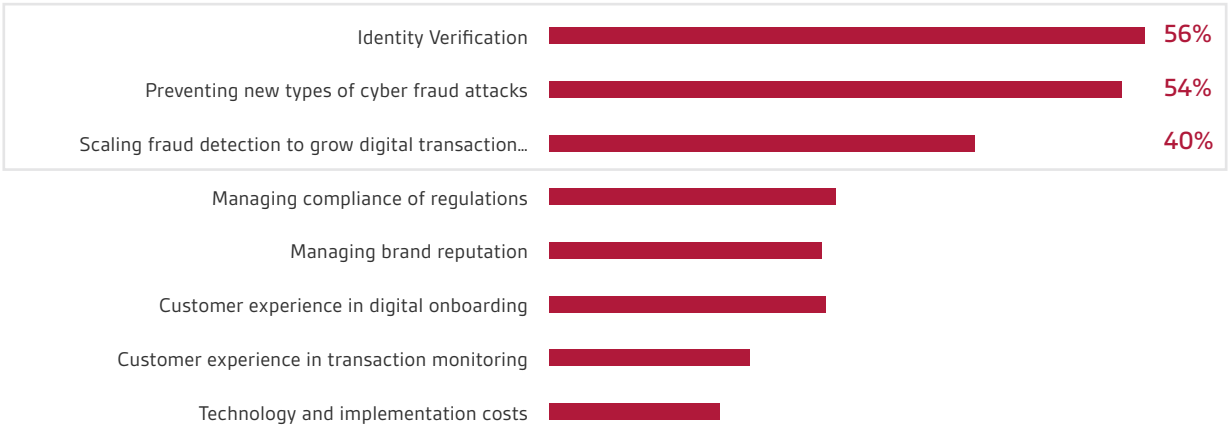
54% of respondents see preventing new types of cyber fraud attacks as the second most important challenge to grow digital transactions, with scalability in fraud detection as the next highest (40%). Identity crime which impacts both the KYC phase and digital onboarding fraud detection, is seen as the top challenge by 56% of the respondents.

Some of the other factors surveyed which were not rated as challenges by the majority of FIs are technology and implementation costs, fraud expertise within internal teams, and legacy systems.

[2] Source: The Edge Markets, Aug 2020

Top 3 boxes – The biggest challenges preventing the growth of digital transactions are identity verification, prevention of emerging cyber fraud attacks, and scalability of fraud management

Figure 7: Most challenging factors in growing digital transactions in APAC

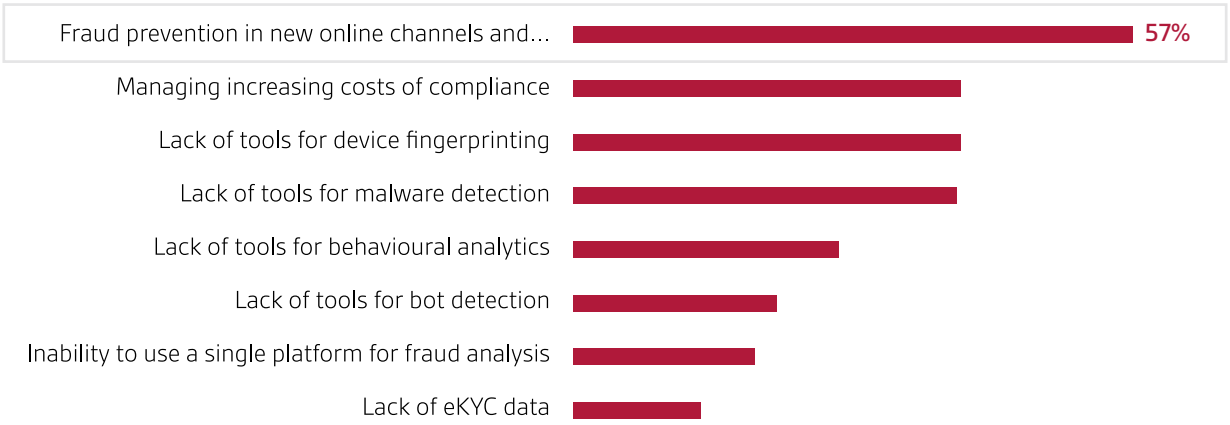


FIs are also facing challenges in mitigating unknown and new fraud patterns (57%) when launching new digital products, propelled by cyber endpoint threats like device fingerprinting (40%), malware detection (40%) and bot detection (21%).

As a whole, the costs of technology and implementation are not seen as a concern. Most FIs also cite high level of confidence with the fraud expertise in their internal teams.

Top 3 boxes – The biggest challenge inhibiting the introduction of new digital offerings for 57% of FIs is to prevent fraud in new online channels and products

Figure 8: Most challenging factors in expanding new digital products in APAC

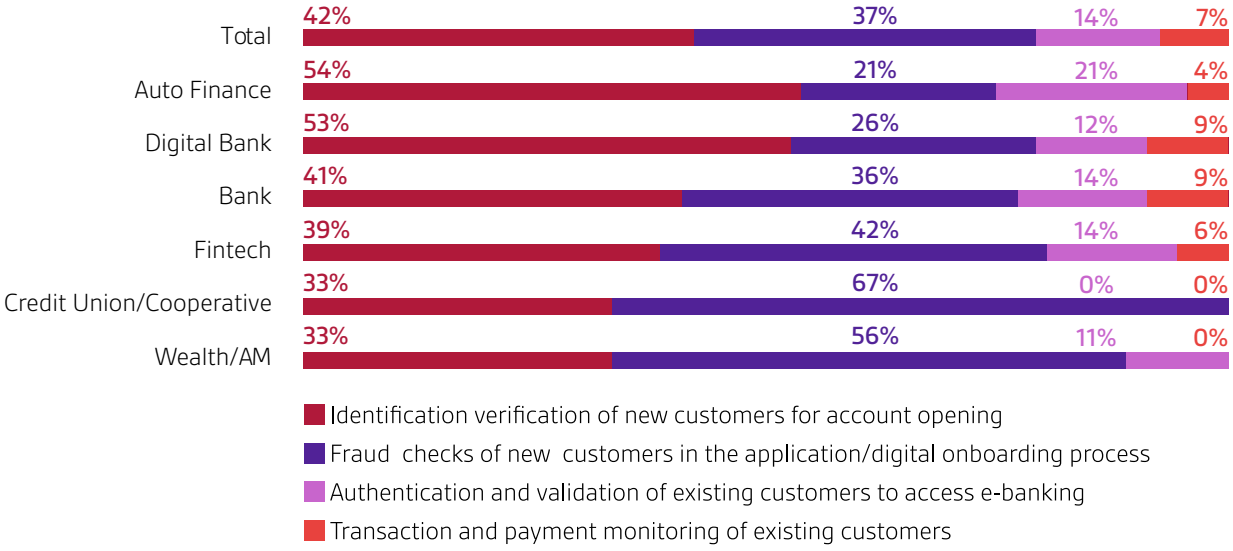


Key challenges in the fraud management customer journey

Across the fraud management customer journey, identity verification is further reinforced as a key challenge for APAC FIs, especially for auto finance providers (54%) and digital banks (53%). For fintechs, credit unions and cooperatives, and wealth and asset management organisations, the bigger challenge comes from the digital onboarding phase.

Both identity verification and fraud detection in the digital onboarding phase are the biggest challenges for FIs in APAC

Figure 9: Key challenges in the digital fraud management customer journey



Organisation Fragmentation

An additional impediment in fraud management and effective digitalisation is centred on existing organisational frameworks that limit the ability to respond to emerging digital threats with timeliness. Data is key to building and future-proofing a successful enterprise fraud management solution. A good data strategy requires consistent and holistic stream of data sharing across internal banking arms responsible for AML & compliance, fraud and cyber risks, and can help to negate repeat fraud attacks on the bank by the same crime ring.

Today, more and more FIs are working hard to stitch together at least two of the functions, with cyber security and fraud functions making the most progress in sharing data. Yet, a distinct 43% of FIs indicated that cyber security, fraud control and compliance functions are still operating in silo.

Vertical silos are prevalent in APAC FIs - limited integration of key fraud preventive functions

Figure 10: The organisational structure of cyber security, fraud control and compliance functions

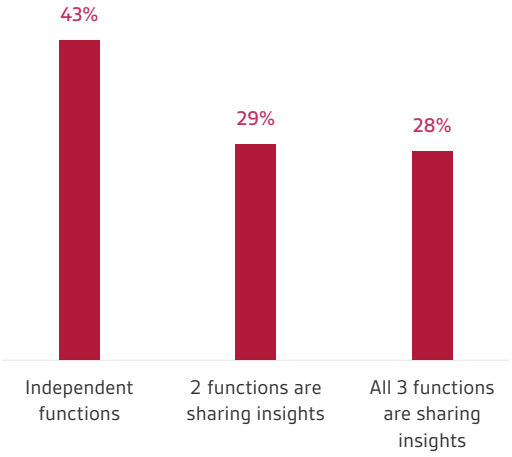
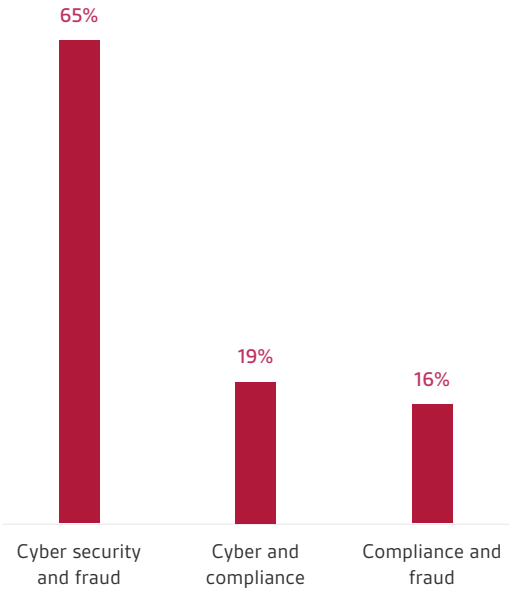


Figure 11: Functions responsible for fraud & compliance operating collaboratively today



03 – Fraud Challenges and Threats in APAC

Growth in Fraud in 2019

Pilfering, deception, fraud, extortion, bribery, falsification, money-laundering – there are endless creative and tech savvy ways which fraudsters siphon money from financial institutions and consumers illicitly. Financial crime 4.0 can be committed by a single fraudster, like a one to one money scam or theft of identity, to large-scale operations run by international organised crime rings; they are more complex to detect and prevent with rapid digitalisation and the use of advanced technology.

Across the board, more respondents are seeing an increase in fraud attacks from first party, social engineering, cyber and AM, with the frequency in social engineering type fraud the highest. Social engineering attacks are one of the most difficult types of crimes to detect, as they start with the manipulation of consumers to disclose their private data, and often involve the victims themselves in the act of committing the crime. Scams are an ongoing challenge with 60% of respondents observing an increase in frequency last year while first party identity fraud generally marked a downward trend.

Singapore

Scam cases made up 27%[3] of overall crime in 2019, and has grown 54% YoY. Amount of money lost through scams were up 16% to S$168million as compared to 2018. eCommerce and loan scams are 2 of the top 10 scams executed in 2019.

Australia

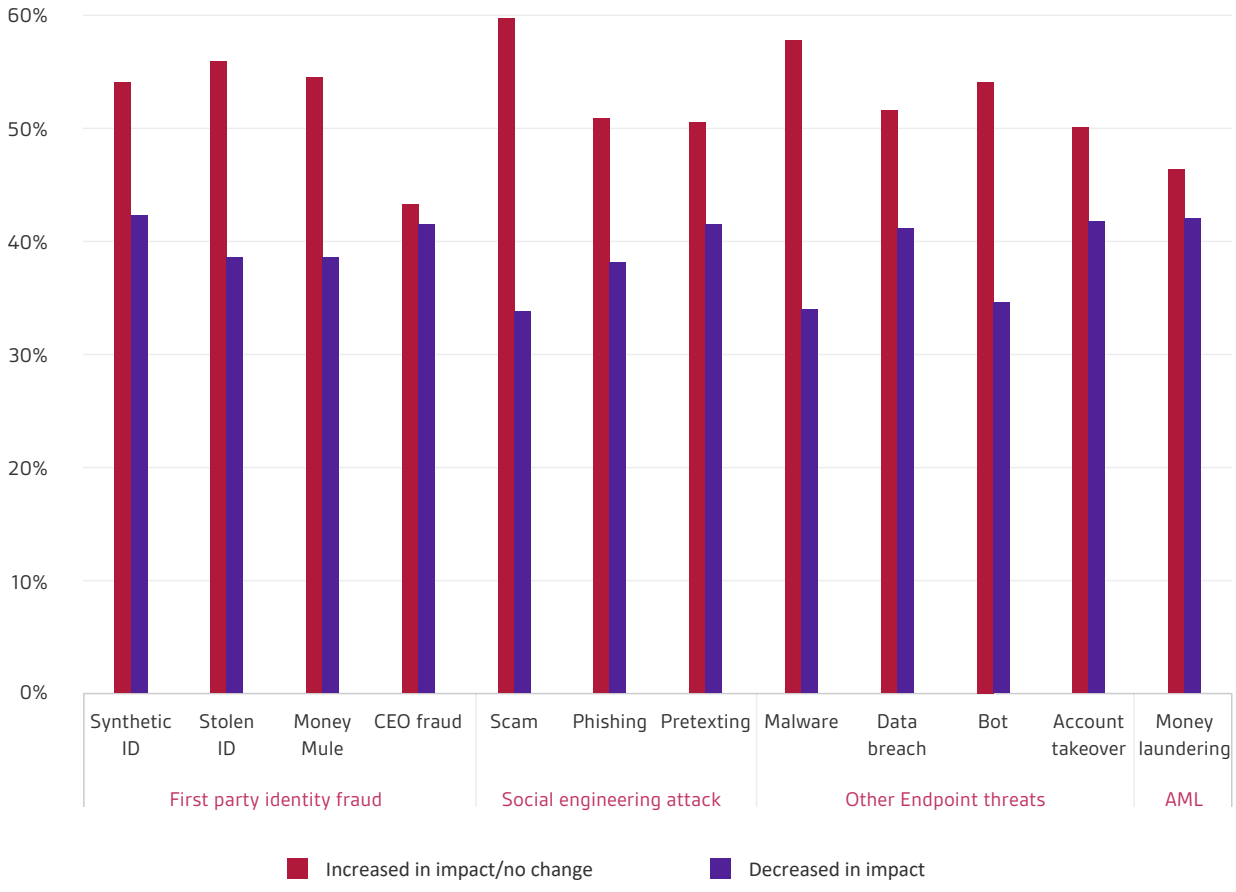
AU$142.898 million[4] were lost to scams in 2019 as compared to AU$107 million in 2018, an increase of 33% YoY, with the majority in investment scams.

[3] channelnewsasia, Feb2020

[4] Australian Competition & Consumer Commission

All fraud typologies are on the rise, in particular social engineering crimes.

Figure 12: Impact of fraud typologies on FIs in 2019

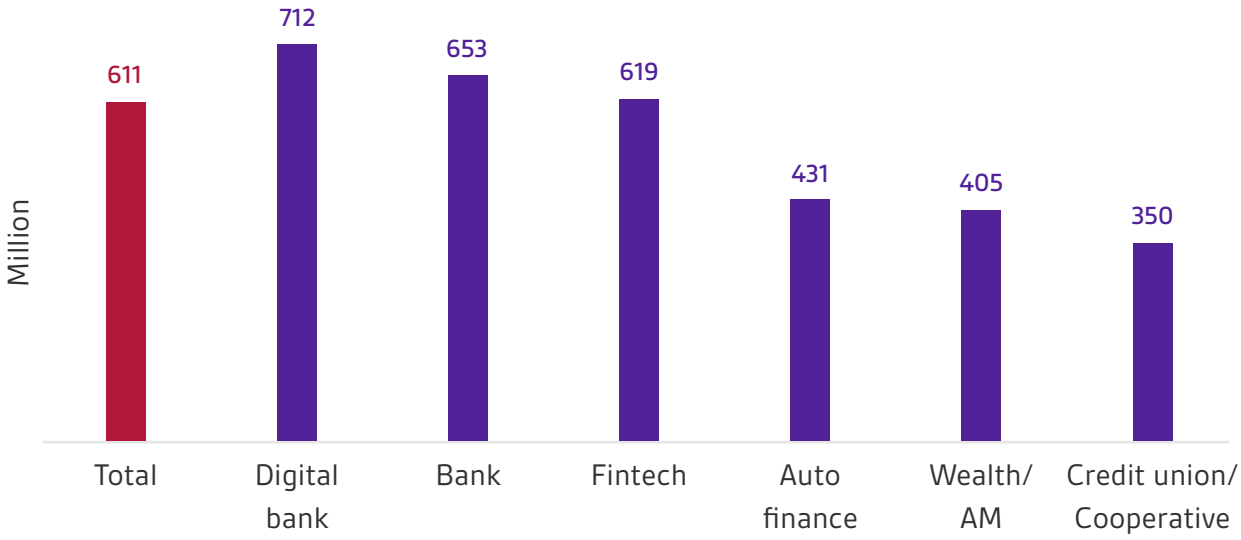


Fraud escalation

Fraudsters are opportunists seeking to take advantage of when organisations go into uncharted areas. Almost one quarter of the respondents see new digital product launches and new app launches (20%) contributing to a spike in transactions. The other contributing factors include promotional activities that motivate consumers to transact more, and many FIs may find scaling fraud prevention to meet spiked volumes in real time difficult.

Seasonal periods in themselves create the environment for fraud activities to take place more easily. Shopping festivals, holiday seasons are when FIs see spikes in phishing and fraud activities. 10% of respondents also attributed transaction spikes to direct attacks by fraudster or malware.

Figure 13: Volume of digital transactions during peak period in 2020

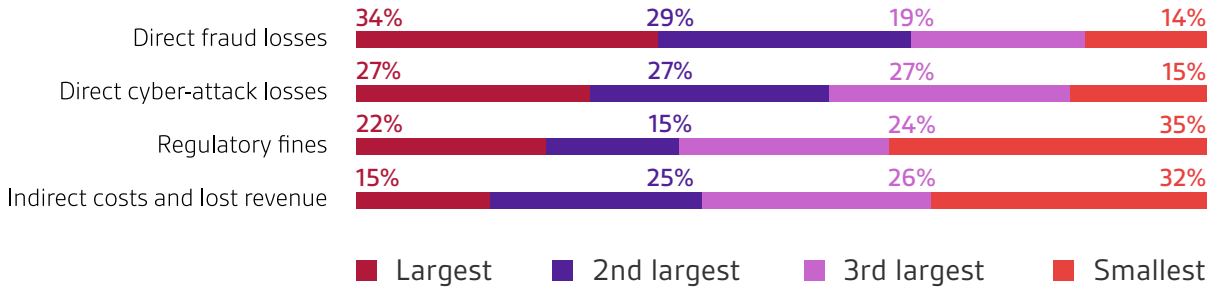


Key type of fraud loss

FIs seek to minimise damages across various vectors especially fraud and cyber-attacks. FIs have flagged both direct fraud (34%) and cyber-attack losses (27%) as the highest ranked losses experienced in 2019. In the Asia-Pacific region, cybercrime is estimated to be around US$171 billion by the Center for Strategic and International Studies and recent cyberattacks demonstrate that these have become organised and coordinated.

FIs experienced direct losses stemming from fraud **(34%)** and cyber-attacks **(27%)**

Figure 14: Volume of digital transactions during peak period in 2020



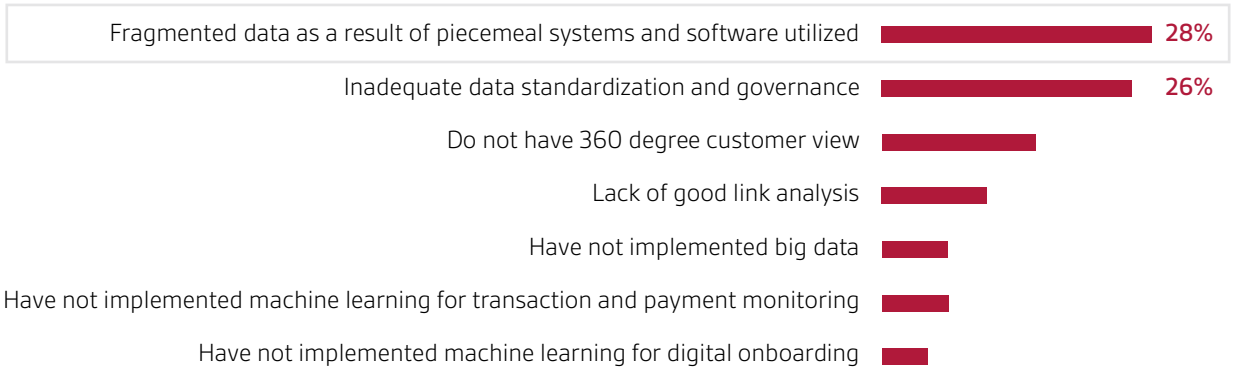
Note: The ranking is for the 4 largest losses resulting from fraud attacks

Gaps in fraud control and risk investigation

Leading FIs are increasingly focused on a utilising a centralised enterprise fraud management platform, with effective 'prevention, detection, response and recovery' capabilities to fend against more evolved and digitally enabled threats. The biggest limitation resulting in ineffective fraud risk investigations is the fragmentation of data as a result of piecemeal systems and software, which 28% of respondents are facing today. The lack of data standardisation and governance presents yet another cause for ineffective fraud risk investigation experienced by 26% of respondents.

28% of FIs consider fragmented data as the most critical limitation in their fraud risk investigation

Figure 15: Top box score - most critical gap in fraud risk investigation

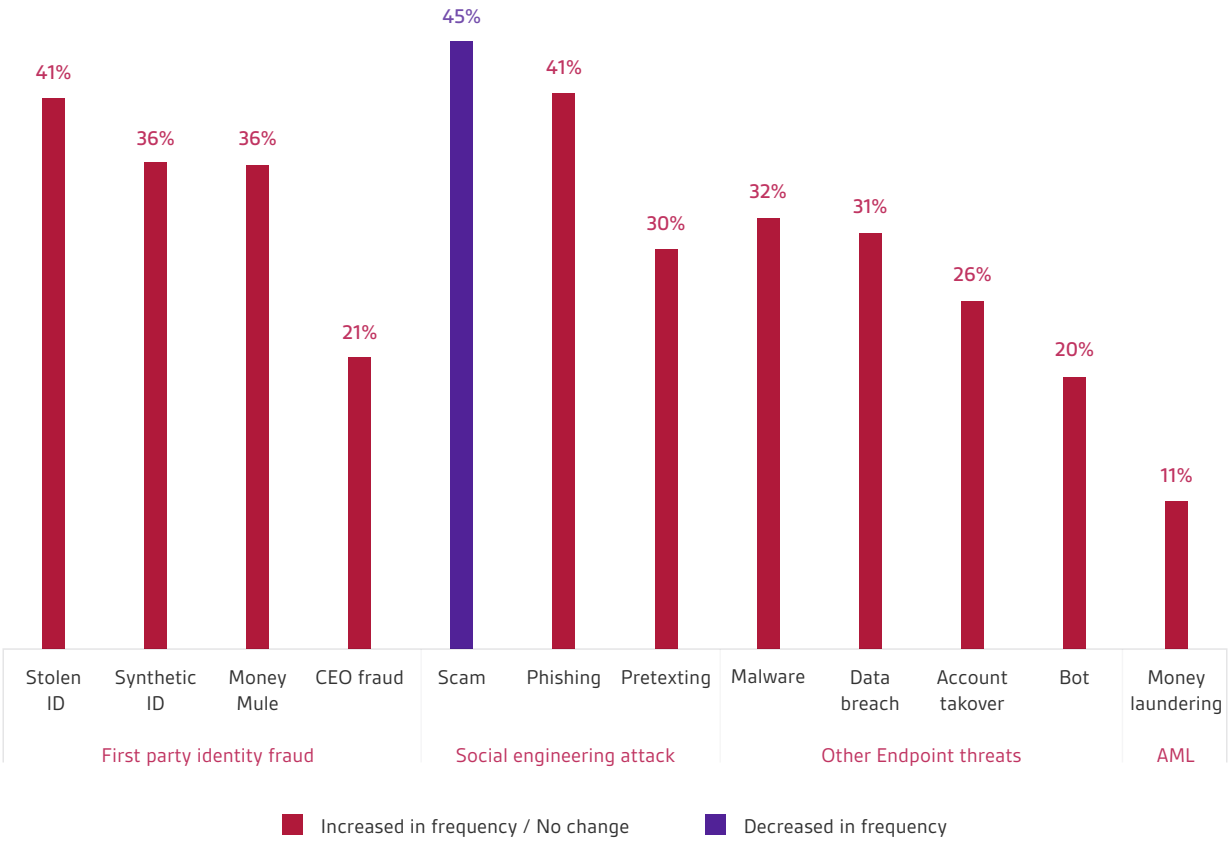


Expectations of social engineering attacks led by Scams **(45%)** and Phishing **(41%)** will dominate fraud prevention priorities of FIs

Expected evolution of frauds in 2020

Understanding the dynamic and fluid nature of digital frauds will help FIs better prepare for the emerging threats of the future. FIs expect social engineering attacks to continue to form the primary thrust of new sources of fraud likely to impact FIs. In particular, scams (45%) are still expected to register an uptick in 2020-21 on fraud attacks, followed closely by phishing (41%) and stolen ID (41%) activities. These are particularly acute in Malaysia, Thailand and Vietnam, where respondents expect a greater growth and focus in social engineering fraud typologies, which harness more innovative and complex psychological manipulation methods.

Figure 16: Expectations of fraud increase in 2020



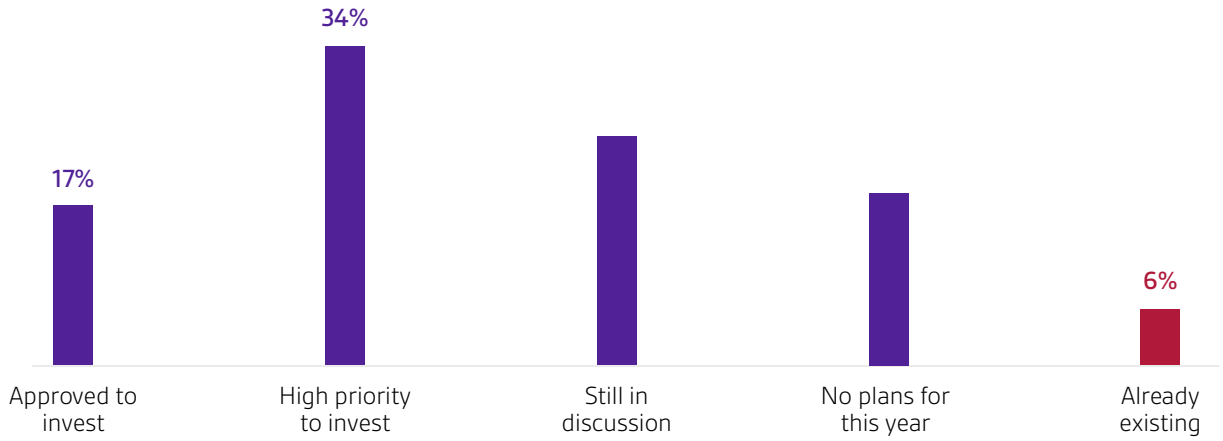
04. Future-proofing fraud prevention through fraud technology and investment

Investing into fraud management platforms in 2020

FIs are maturing in digital transformation and are looking at technological investments more strategically. It is clear from the research that FIs acknowledge the gaps in effective fraud management without an integrated end to end fraud and compliance platform solution, though early adoption is still low, with existing implementation by 6% of the respondents. The adoption of an end to end platform is likely to pick up pace; one-third of the FIs rate investing in end to end fraud management platform solutions as a high priority, while 17% have already set aside a budget to implement in 2020-21.

57% of FIs already are on or are in the process of upgrading to fraud management platform solution in 2020-21

Figure 17: Planned investment for end to end fraud management platform solution by 2020-21



Onboarding vs Transaction Monitoring

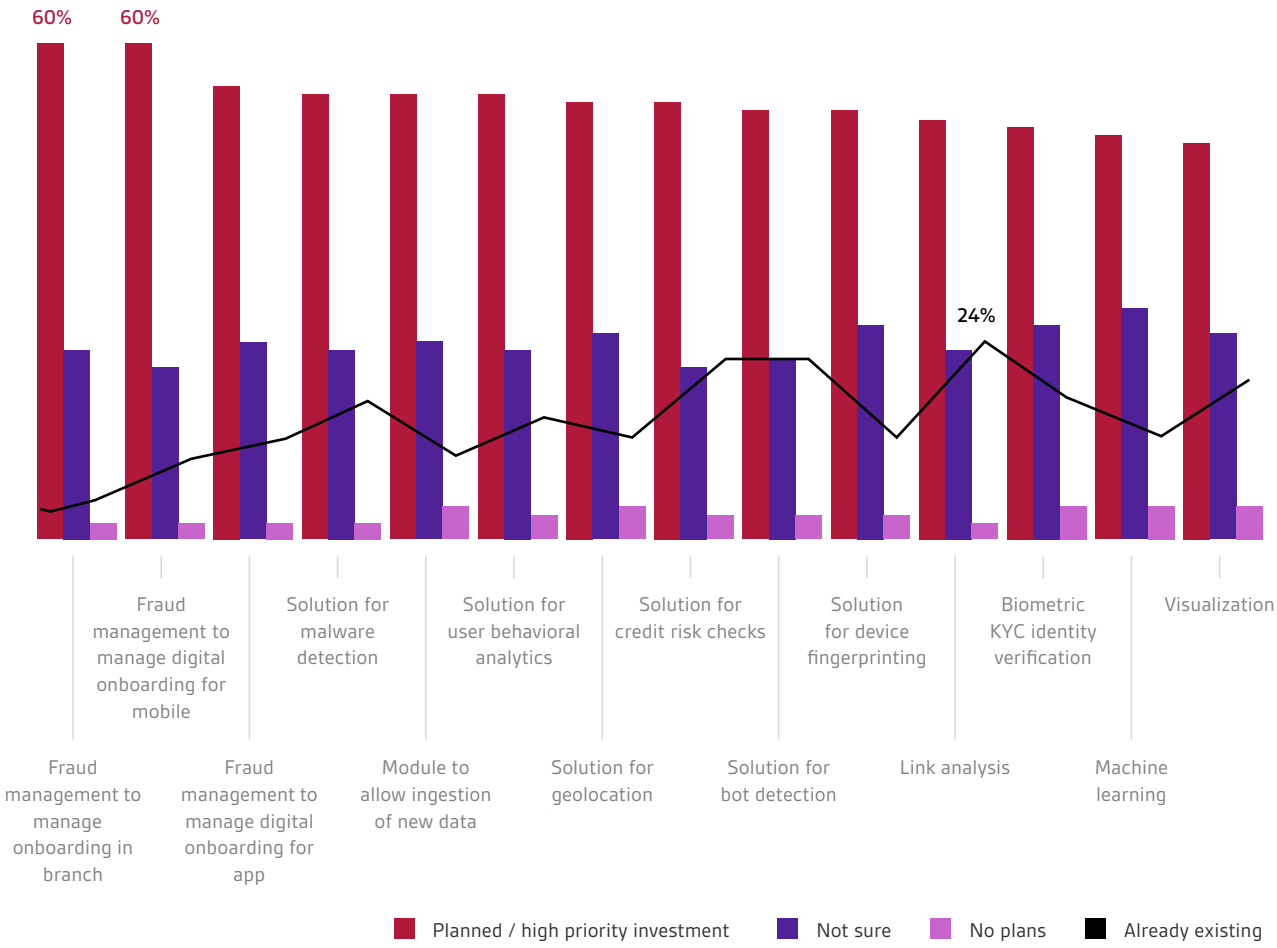
To digitally onboard customers better, the solutions that FIs have prioritised to invest in are fraud management across branch and mobile, (60% of respondents respectively). 55% of respondents are prioritising fraud management for app. There is a mixed interest in different types of solutions to fight fraud across APAC, including solutions for endpoint threat detection, ingest external data, predictive analytics and fraud data analysis.

More than **50%** of the respondents have planned investment to upgrade their digital onboarding fraud solutions

Some of the newer approaches that FIs are exploring to manage fraud prevention include the use of a centralised module to ingest new data into the core platform. At present, additional data sources can be shared via a direct API with the fraud risk scoring or fraud modelling engine. Having separate APIs generally take a longer time for FIs to onboard new solutions, as opposed to having a centralised platform to support the ingestion of external data. 54% of respondents are planning to invest in this type of solution this year onwards.

Link analysis appears to be the solution which almost one-quarter of the respondents already have installed. A number of FIs also have some types of cyber endpoint threat solution installed, with malware detection and bot detection as two of the highest in this category.

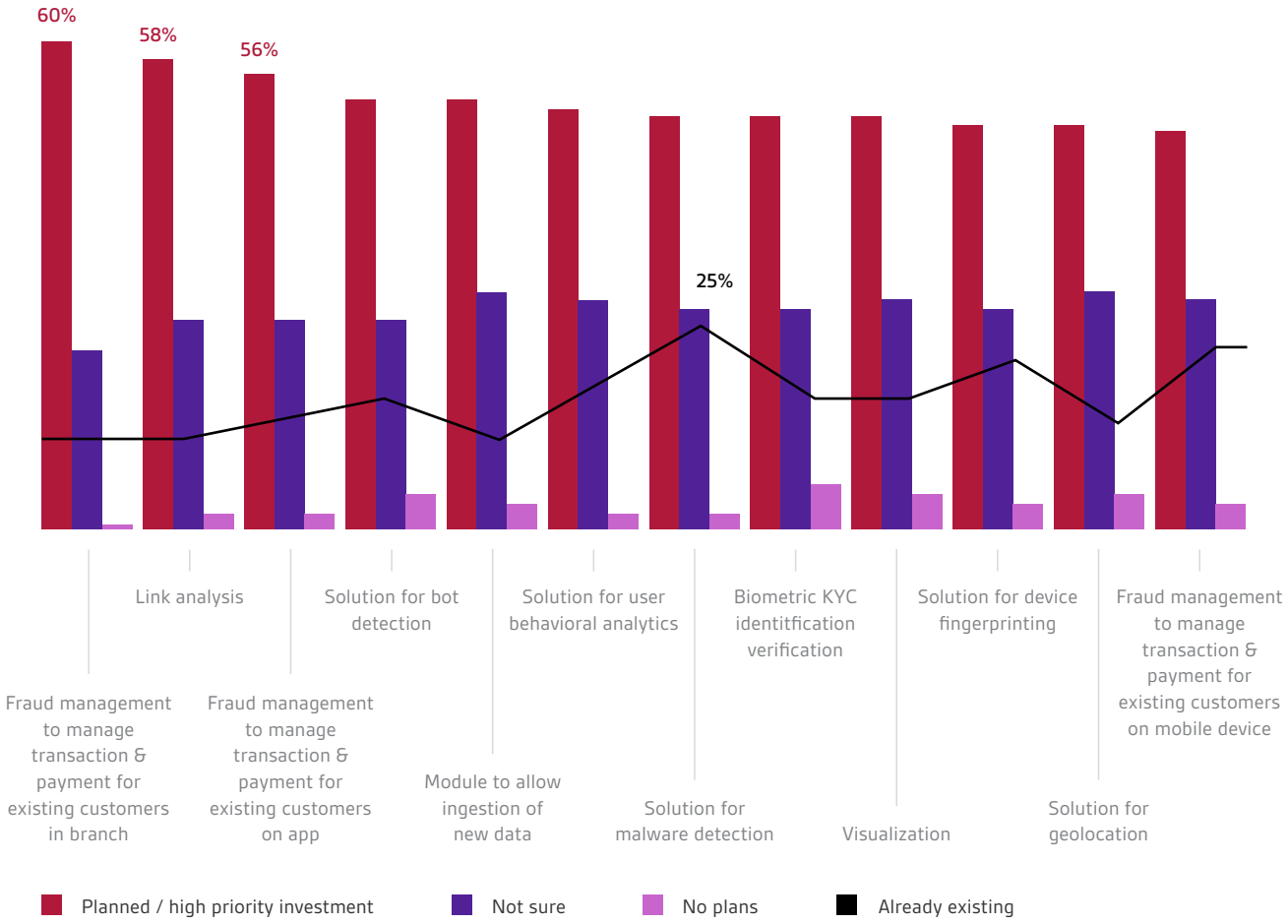
Figure 18: Planned investment in fraud management technology for digital onboarding



In the transaction monitoring and payments phase, FIs are looking to invest in transaction and payments fraud management in branch (60%), app (56%) and link analysis (58%). The expectation of high volumes of social engineering crimes could be one of the reasons for the heavy focus in link analysis. Similar to fraud management during digital onboarding, it is a mix bag to approved technology investment. A couple of fraud management solutions appear to be of high importance to more than 50% of the respondents whether they are for digital onboarding or transaction monitoring, these include a module to ingest new data and bot protection, with planned budget by more than half of the FIs.

Transaction and payment fraud management readiness is highest for malware detection, with implementation done by one-quarter of the respondents. The other cyber endpoint threat prevention higher on the list of readiness is device fingerprinting (23%). Across the different channels, more respondents have prioritised fraud management on mobile channels.

Figure 19: Planned investment in fraud management technology for transaction and payments monitoring



Investment budget for fraud management

The average estimated budget to purchase new fraud prevention technology in 2020, per FI in APAC, is USD83.3million. Three of the APAC countries are coming in above the average estimated fraud budget with Thailand leading at USD95.4 million, China USD91.4 million and Indonesia USD88.9 million. Australia has the smallest estimated fraud budget of USD76.1 million.

An average of US$83.3 million fraud prevention budget planned for 2020

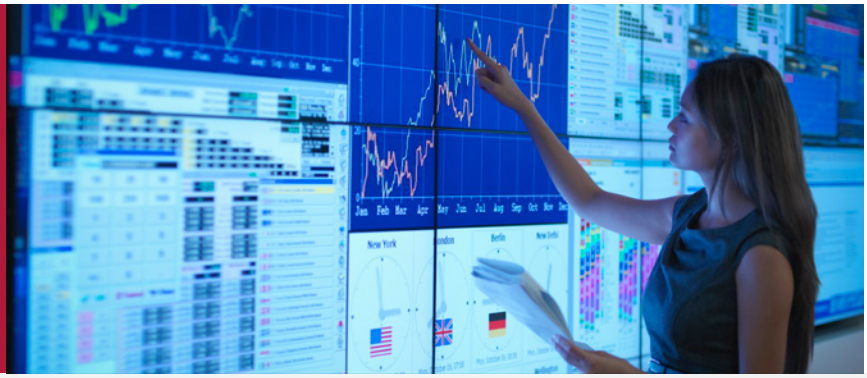
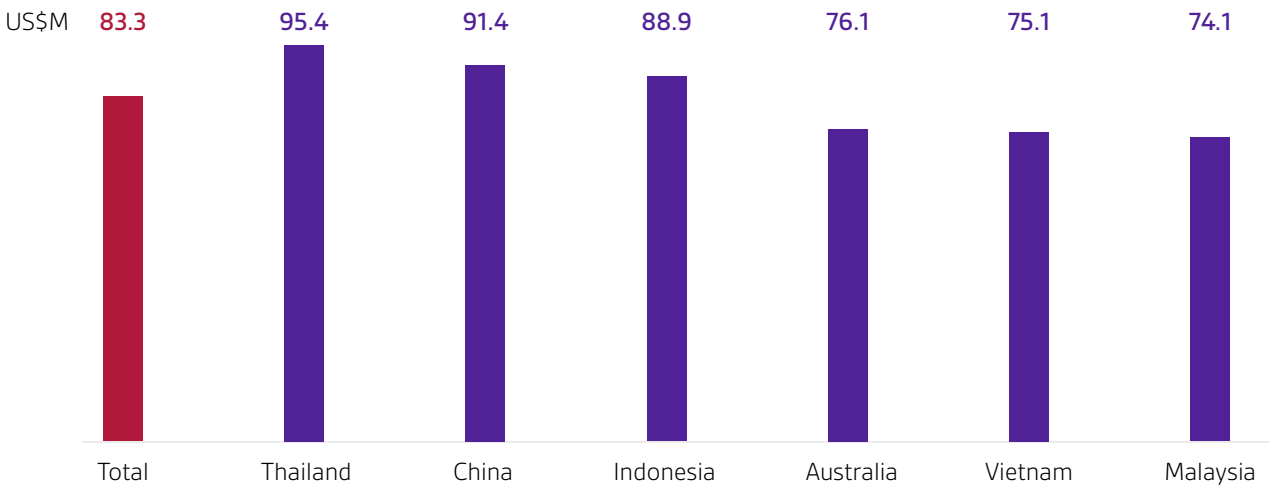


Figure 20: Estimated new fraud technology investment budget in 2020-21



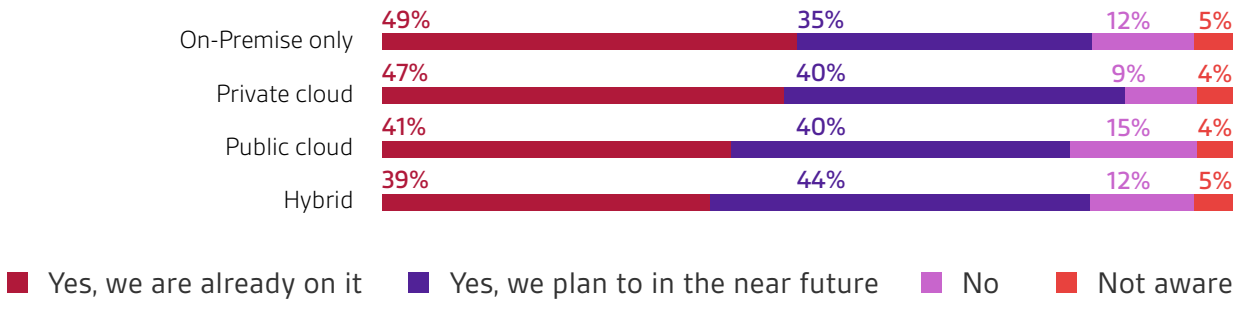
Cloud hosted solutions

There is an apparent inclination towards using cloud-hosted fraud detection solutions. On-premise only is the preferred option by almost half of the organisations, with more on-premise fraud detection applications planned for by 35% of the respondents. FIs (44%) are weighing the possibility of opting for a hybrid cloud architecture system.

However, private cloud solution looks to overtake the preference for on-premise solution in the long term, with 47% of respondents already on it and 40% planning for it in the near future.

Private cloud deployment would be the preferred in the near term

Figure 22: Cloud hosted fraud detection solution



Conclusion and Recommendations

Digital fraudsters are becoming increasingly innovative and the intensity of their attacks far more overwhelming. Given the range of technologies available to fraudsters, their ability to escalate and impact FIs through digitally led fraud poses significant concerns. While many FIs are moving in the right direction in scoping out and trialling new fraud management technology, it remains to be seen how quickly FIs can get ahead in meeting the challenges posed by these fast-escalating sources of risks. However, it is clear that those organisations, which lack the ability to respond quickly and strategically will fail in countering these rising threats.

Further compounding the situation, the global outbreak of the novel coronavirus has forced FIs in the APAC region to ramp up and embrace a fuller spectrum of digitalisation in a short time. This strategic transformation carries additional sources of risk that have the potential to fundamentally undermine the long-term sustainability of any organisation. FIs, who are able to harness and integrate new technologies holistically to power their fraud management to more proactively, predictively and agilely, will succeed in mitigating complex fraud typologies in the new normal.

New-Gen Sustainability

Financial crimes 4.0 typologies require a new generation of fraud management technology. FIs are progressively and decisively moving towards an end to end fraud management platform, where cyber endpoint threat integration is no longer an option.

Centralised module to ingest new data

is a newer approach that FIs are progressively exploring to manage fraud prevention. At present, additional data sources can be shared via a direct API with the fraud risk scoring or fraud modelling engine. For accelerated onboarding and ingestion of external data, instead of opting for separate APIs, a centralised platform has the advantage of amassing best of breed solutions which FIs could opt to turn on with a license key as long as they have access to the platform.

Cyber fraud management

is essential to protect against escalating fraud typologies, especially prevalent in uncertain times like the COVID pandemic. New approaches to endpoint threat protection includes using mobile and app metadata to determine the risk propensity of individuals, and correlating and analyzing data points within devices of individuals to detect anomalies, in addition to the standard solutions to track down malware, bots and emulators

Real time scalability

As FIs develop and bring to market an increased number of digital products across a mix of mobile, app, and web channels, fraud and risk departments need solutions to manage surges in activities that create spikes in the number of transactions. Multi-tenanted cloud solutions are proven to manage and replicate growth across multiple locations. With improved security measures built into cloud solutions, highly regulated industries like the finance and banking sector are already planning on cloud deployment moving forward.

About GBG

GBG (AIM: GBG) is a global technology specialist in fraud, location and identity data intelligence with offices in 18 locations worldwide. For over 30 years, GBG has been accessing and verifying identities, to the standards set by financial regulators, of more than 4.4 billion people worldwide or 57% of the world's population. GBG has a network of over 270+ global partnerships and access to 510+ datasets to provide data with accuracy and integrity.

In the fraud category, GBG manages end-to-end fraud and compliance needs across a range of industries including financial services (international, regional and local banks, auto finance, P2P lending, mutual companies, and credit unions), insurance, government services, retail, betting and wagering. Some of our customers include 90% of top tier banks in Malaysia, 4 top tier banks out of Indonesia's BUKU 4, BNP Paribas Personal Finance in Spain, regional banks like HSBC, and major wagering players like Tabcorp.

For more information

gbgplc.com/apac
contact@gbgplc.com

GBG locations:

APAC
Beijing, Canberra, Jakarta, Kuala Lumpur, Melbourne, Shanghai, Shenzhen, Singapore, Sydney

EMEA
Barcelona, Chester (UK HQ), Dubai, Edinburgh, Germany, Liverpool, London, Nottingham, Turkey, Worcester

USA
Atlanta, New York, San Francisco

GBG