TRUSTING IN THE BANKING EXPERIENCE

A BANKING INSIGHTS REPORT BY UNISYS

UNISYS | Securing Your Tomorrow®

TABLE OF CONTENTS

Research Methodology

The online survey was conducted by Omnipoll and fielded during November 2018 to a nationally representative sample of over 1,000 people aged 18+ in each of Australia, Hong Kong, New Zealand, the Philippines and Taiwan – 5,291 respondents in total.

Executive Overview

The findings of the 2019 *Unisys APAC Banking Insights* survey suggest that while banks have been busy focusing on adapting or developing products and services for particular areas of the customer experience, e.g. mobile, they have neglected to innovate other systems and processes at the same rate. The end result is a variety of technologies and experiences that don't align and make it difficult for the customer.

The report reveals that perfecting the end-to-end customer journey is now absolutely critical to attracting new, and retaining existing, customers. For banks, this involves delivering services in new ways, streamlining interactions to save customers time and effort, and using methods that boost security and compliance without compromising the customer experience.

Banks can get ahead of the competition by creating an actionable roadmap that rolls out improvements for a more convenient and personalised experience.

Omnichannel banking uses data analytics to transform the customer experience, allowing banks to unify all platforms and deliver a single view of the customer. This ensures customers receive a personal and connected experience at any point in their interaction, regardless of the service or platform.

Banks have an opportunity to focus on empowering customers by providing them with a banking experience that fits with their lifestyle. Having a secure, integrated digital banking platform will increase customer satisfaction and brand loyalty.

"Banks have made significant headway as they evolve their products and services to keep up with customer expectations of digitalised services. However, banks must be careful they don't mistake the use of digital technologies for digital transformation.

Digital transformation is the idea of using technology not just to replicate an existing service in a digital form, but to use technology to transform that service into something significantly better."

Ian Selbie, Industry Director, Financial Services, Unisys Asia Pacific

UNISYS | Securing Your Tomorrow®

Asia Pacific 2019 Banking Insights

Trusting in the Banking Experience:
What matters to Asia and Pacfic bank customers

View the full report www.unisys.com/BankingInsightsAPAC

Trust

Which organisations do consumers trust most to share their data with?

New Zealanders and Filipinos **trust banks twice as much as government**

Hong Kongers and Taiwanese **trust government more than banks**

Australians **trust no-one**

Security

What matters most to bank customers?

6 in 10 want safety and security of their data

Half want easy to understand, transparency in products, processes and services

Biometrics for bank security?

Face and fingerprint

7/10 of APAC bank customers comfortable using face and fingerprint biometrics to access mobile banking and ATMs

Behavioural

Only **3/10** are comfortable with banks monitoring and using behavioural biometrics such as how you typically hold and use your smart phone

Customer Experience

#1 **Reason for not supporting biometrics:**
Data security concerns

What annoys bank customers most?

Aussies, Kiwis and Taiwanese:
Having to repeat themselves across different touchpoints

Hong Kongers and Filipinos:
Long queues in the branch

A Time of Great Change

Organisations all over the world know that the key to attracting and retaining customers comes down to the experience they deliver.

Digital technology has, and will continue to, transform customer expectations when interacting with organisations – and banks are no different. Across the financial services sector, digital innovation is seen as a critical pathway to engage customers, increase loyalty and drive value to the business.

Banks have been distracted by developing smart new products that deliver to the demands for improved technology and greater convenience, while simultaneously trying to juggle the rapid evolution of regulation and legislation. While the sector has been preoccupied creating new revenue streams in silos, they've often forgotten what the end goal should be: developing a customer experience where all products and services are linked seamlessly to each other.

As a result, banks are yet to deliver a five-star service that offers a holistic end-to-end approach that spans products, service and channels of delivery.

Along with growing expectations of customer experience, there is also increasing pressure for banks to deliver a safe, secure and ethical service to their customers.

The Australian Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry has put a spotlight in bank security and the outcomes are being closely watched by the rest of the region.

In many countries across Asia, governments and financial regulation bodies are driving the security agenda in financial institutions by setting formal standards and requirements for banks to be accountable for, and take appropriate steps to protect, customer data. Many include appointing a Chief Information Security Officer (CISO).

For example, Bank Negara Malaysia (BNM) – the central bank in Malaysia – has set standards detailing the level to which a Malaysian financial institution's board is responsible for the organisation's IT and cybersecurity, including that all financial institutions must designate a CISO[1].

Similarly, in the Philippines the Monetary Board enhanced guidelines on information security management of Bangko Sentral Supervised Financial Institutions (BSFIs) including that they appoint a CISO[2]. The Monetary Authority of Singapore (MAS) moved to tighten the rules on cybersecurity for financial institutions by proposing a set of six essential cybersecurity measures to protect their IT systems – the measures already exist as guidelines, but the financial regulator is proposing to make them legally binding requirements[3].

Furthermore, the Hong Kong Monetary Authority (HKMA) launched the "Cybersecurity Fortification Initiative" (CFI) in 2016 aimed to raise the level of cybersecurity of banks in Hong Kong including a common Cyber Resilience Assessment Framework, professional development program to increase the supply of security professionals to the industry and a cyber intelligence sharing platform[4].

The APAC Banking Insights study explores how customers engage with their banks to uncover their expectations, preference and frustrations with processes and services.

Central to this is determining how customers feel about all the elements of their banking experience and where in the journey banks are failing to create those unified, efficient and personal touchpoints.

In addition, building on the high consumer concern around identity theft, bank card fraud and virus and hacking in Asia Pacific and globally (2018 Unisys Security Index[1]), the 2019 APAC Banking Insights report examines bank customer willingness to use new technology, particularly biometrics, as part of a bank's security measures.

At a glance, the 2019 *Unisys APAC Banking Insights* report reveals three key themes:

- **An Institution Customers Can Trust**: Banks across Asia Pacific have yet to win the hearts of customers, who want to know organisations can be trusted to safeguard their most personal information.
- **Banking on Customer Experience:** As customers remain frustrated by the lack of insight into their customer journey, banks are yet to deliver a true omnichannel approach. Those that don't will struggle to build meaningful and lasting relationships with customers.
- **The Evolution of Digital Identities:** As digital identities and biometrics become more prevalent in commercial engagement, banks must provide customers with the confidence that they will protect this highly personal information.

[1] Bank Negara Malaysia (BNM) "Risk Management in Technology" – September 2018

[2] Bangko Sentral Ng Pilipinas - *Enhanced Guidelines on information Security Management* – September 2017

[3] Monetary Authority of Singapore media release

[4] Hong Kong Monetary Authority media release

The Trust Factor

Trust has become a critical element for building and fostering sustainable relationships with customers. Consumers expect a tailored and highly personal experience and banks have the opportunity to create a significant competitive advantage by establishing a trusted relationship that puts the interest of the customer first.

As more digital services require personal information for engagement, customers are feeling increasingly pressured to provide highly unique data, from names, ages, addresses, passport numbers, phone numbers to next of kin and even their biometrics.

However, without trust, customers are reluctant to provide this information.

Unisys research shows that customers are more likely to share their personal data if they have a clear understanding of the purpose, who it will have access to it and how it will be secured[5].

In fact, concerns about security and trust are often cited as the main reasons that consumers do not use digital channels to their fullest potential.

This is likely to be linked to an increase in high profile data breaches across all types of organisations, from banks and government to telecommunications and healthcare providers.

For example, in mid-2018 it was revealed classified material from the NZ Security Intelligence Service (NZSIS), New Zealand's domestic intelligence agency, was left in a Wellington café bathroom. Meanwhile, between August 2018 and January 2019, more than 900,000 clients of Philippine-based Cebuana Lhuillier were affected by a data breach that exposed addresses, source of income and dates of birth.

Building Trust in Banking

For the first time in the *Unisys APAC Banking Insights* survey, we asked customers which type of organisations they trusted the most with their personal data. The purpose was not only to determine customer sentiment for banks against other commonly used institutions, but to determine how customers felt about giving banks their personal information, and whether they were trusted to protect it.

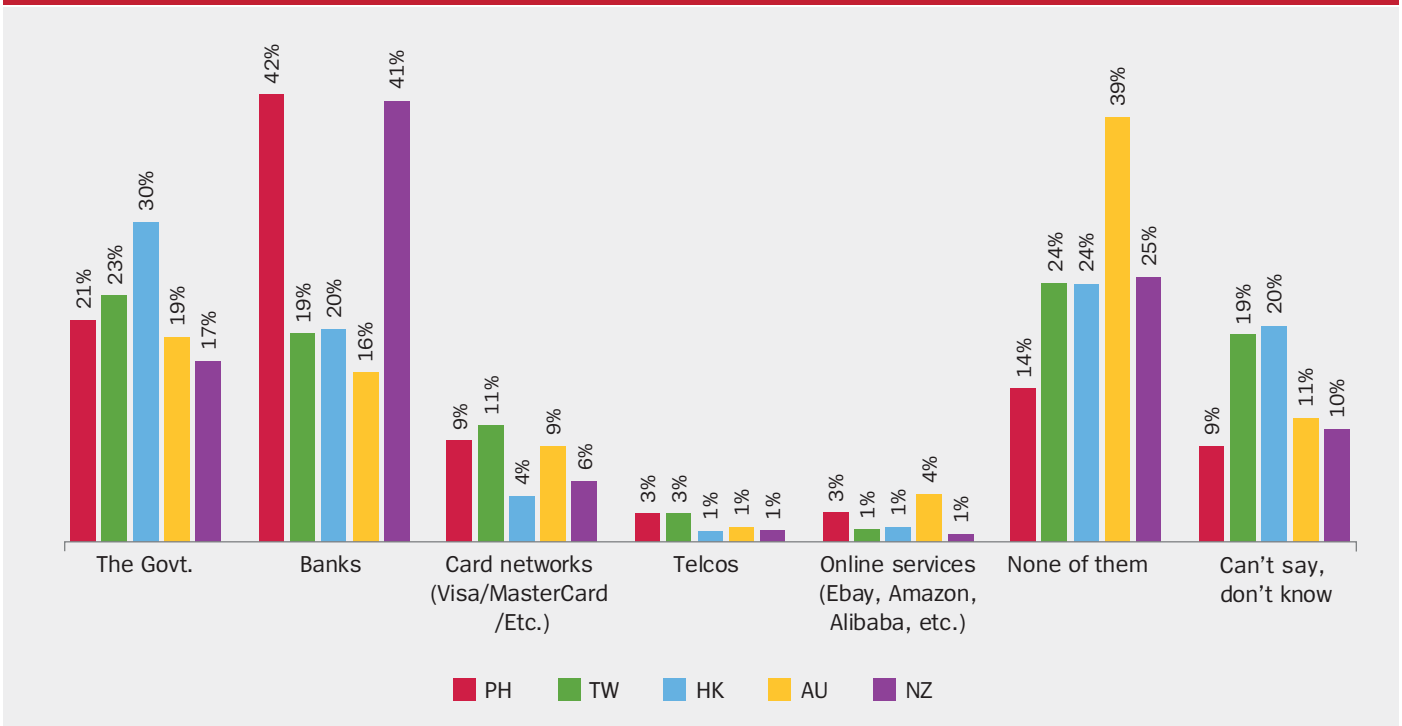
For those in New Zealand (41 per cent) and the Philippines (42 per cent), there was a significant show of trust in banks compared to other organisations, particularly government entities where trust is very low.

In Australia, customers were unable to place trust in *any* of the organisations listed in the survey, with 39 per cent stating, 'none of the above'. According to the Office of the Australian Information Commissioner, in 2018 alone Australian organisations reported over 800 data breaches across a variety of industries including financial services, government, retail and healthcare. This low trust would have been exacerbated by the widely reported investigation and findings of the Australian Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry which dominated media headlines.

One in four of Hong Kong, New Zealand and Taiwanese respondents were also unable to place their trust in any of the organisations listed. Taiwan has been a high-profile target for hackers for over a decade, where government and the automotive industry are often falling victim to the loss of personal information for malicious purposes.

The findings demonstrate that banks across Asia Pacific have a duty of care to their customers to reinforce their commitment to the security and safety standards by which they safeguard their data.

Regional Comparison: Who Do You Trust Most to Share Your Personal Data With?



[5] Unisys Security Index 2018 global report

How to Win with Trust

Open Banking frameworks have been introduced across the financial services industry globally in a bid to give customers more control of their banking data and stimulate competition within the industry.

Traditional banks are looking to use Open Banking as a mechanism to differentiate in an overcrowded market. Open Banking also presents financial service institutions with the opportunity to evolve the way they currently operate. Not only will it encourage innovation and competition within the industry, but it will also enable opportunities to diversify, bring in new revenue streams and also be seen to support the customer and their experience with the bank.

Governments will also play a role in the success of this new banking ecosystem. The introduction of a government framework will ensure consistency and equality across the banking landscape; creating a common playing field when it comes to compliance, the rise of new products and services and better serving the customer.

However, given that the 2019 *Unisys APAC Banking Insights* report finds that data security is the top thing that matters to bank customers in all countries surveyed, it is critical that banks ensure that the entire supply chain of their financial services ecosystem is adequately secured against malicious and accidental breaches.

In the last year, there has been growing momentum for Open Banking across Asia Pacific. Those who do not trust corporate or public institutions to manage or protect their personal data are acutely aware of the benefits open banking gives them as the customer, including:

- **Greater Visibility and Transparency into Use of Data**: Unless customers provide consent, banks can no longer share customer data with third party organisations.
- **Convenience**: The move to Open Banking has the potential to create an entirely frictionless experience for customers, particularly those looking to switch banks, and possibly even get a better deal out of it.

While banks have no control over how customers feel about using other services, how they are seen to manage personal information is integral to gaining trust and support from customers.

A Definition of Open Banking

A system that provides a user with a network of financial institutions' data through the use of application programming interfaces, better known as APIs.

The Open Banking Standard defines how financial data should be created, shared and accessed. By relying on networks instead of centralisation, open banking helps financial services customers to securely share their financial data with other financial institutions. Benefits include more easily transferring funds and comparing product offerings to create a banking experience that best meets each user's needs in the most cost-effective way[6].

[6] Investopedia

What Customers Want: A Seamless Experience

Since its inception, the *Unisys APAC Banking Insights* report has focused on understanding what's important to the customer. This helps identify flaws and areas for improvements in the transactional moments customers have with their financial service institutions.

The reality is that current systems rarely capture or unite every touch point or interaction in end-to-end customer journeys. However, this clarity is essential to creating a true omnichannel experience.

The Unisys report explored how customers felt about the following issues:

- Long queues in branches
- The bank not knowing all the relationships or products customers have with that provider
- The customer having to repeat themselves to different service consultants or channels such as phone/branch/internet
- Online services that require customers to print a form and mail it, or go to the branch
- Customer credit cards being frozen or cancelled due suspected fraudulent activity

Previously, many bank customers across Asia Pacific were annoyed by long queues in branches and inconvenience when credit cards have been frozen due to suspected fraudulent activity.

However, the 2019 *Unisys APAC Banking Insights* report reveals a change: customers in Australia (29 per cent), New Zealand (32 per cent) and Taiwan (30 per cent) have grown increasingly tired of having to repeat themselves to a different service consultant or channel, such as phone, branch or internet.

Not only is repetition a key concern cited by residents in these countries, but in all countries surveyed, their frustration with this has steadily increased over time.

This is the greatest annoyance for all age groups, except those aged 50+.

These findings reinforce that banks are yet to achieve the seamless omnichannel experience they are striving for and customers expect.

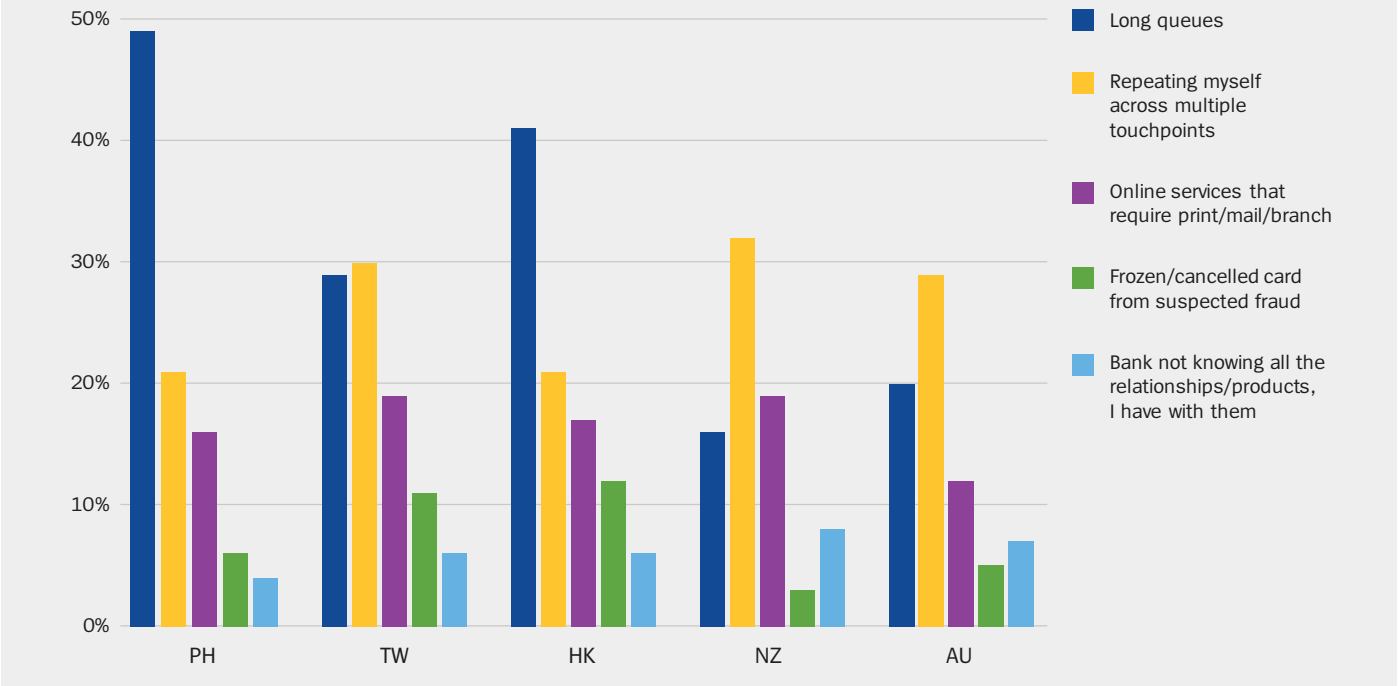
Growth in percentage of bank customers who rank having to repeat themselves to different service consultants or channels such as phone branch or internet as their top annoyance over the last three years:

	AU	NZ	HK	TW	PH
2016	24%	24%	13%	20%	14%
2017	20%	N/A	15%	21%	13%
2018	29%	32%	21%	30%	21%

Yet in Hong Kong and the Philippines, long queues in branches remain the top annoyance of customers. While both countries offer a lot of bank branches for customers to use, the frustration might be driven by the increased use of digital products and services within the physical branch involving greater automation and less human contact.

Customers in Australia and New Zealand are less annoyed by long queues in branches which is likely to be directly linked to ongoing growth in mobile and online banking requiring less visits to the branch.

Regional Comparison: What Annoys Bank Customers Most?



Accessing and Controlling Digital Identities

Across Asia Pacific the use of digital identities and biometrics has infiltrated the everyday lives of customers who use it to access their mobile phones, talk to digital assistants, move through buildings and travel freely across country borders.

The evolution of biometrics, including face, voice and fingerprint within banking has been well received by customers, particularly by those who enjoy the convenience it offers.

The *Unisys APAC Banking Insights* survey sought to determine to which degree customers felt comfortable with their bank using biometrics to verify their identity to authorise access to transactions.

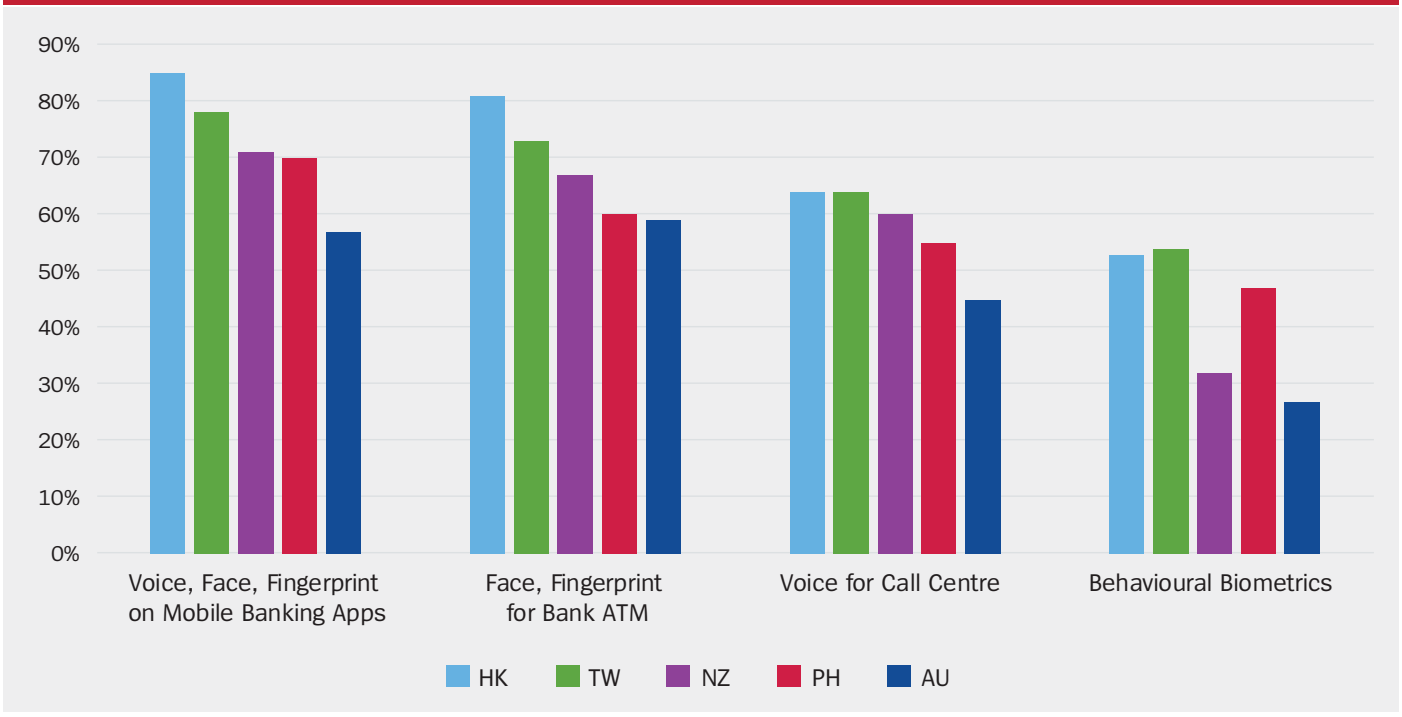
The findings show there is a willingness among all respondents in all countries to use biometrics, including voice, face and fingerprint across mobile banking apps and at bank ATMs in all countries.

What is Behavioural Biometrics?

Behavioural biometrics provides a new generation of user security solutions that identify individuals based on the unique way they interact with computer devices like smartphones, tablets or mouse-screen-and-keyboard.

By measuring everything from how the user holds the phone or how they swipe the screen, to which keyboard or gestural shortcuts they use, software algorithms build a unique user profile, which can then be used to confirm the user's identity on subsequent interactions[7].

Regional Comparison: Comfort Using BiometricsIdentity Verification For Transactions



The commercial sector has made significant headway into the adoption of biometrics across industries from banking and retail to healthcare and insurance.

However, while voice, face and fingerprint are all widely accepted and already used in many of the banks' processes, consumers are less comfortable with a bank using behaviour biometrics, such as tracking the unique way a person scrolls through websites, types on a phone or presses buttons, to verify identity.

This is likely driven by a combination of less familiarity with this type of security measure and an unwillingness to be monitored on an ongoing basis. If banks want their customers to embrace behaviour-based identity authentication, they will need to convince them that the benefit of security is worth forgoing some level of privacy.

Those aged 25-35 years are most likely (57 per cent) to support the use of behavioural biometrics, closely followed by 18-24 and 35-49 year olds, where over half are comfortable with banking using this type of technology.

Interestingly, in all countries except Taiwan, support for behavioural biometrics is the lowest among aged 50+ (25 per cent in New Zealand, 18 per cent in Australia, 38 per cent in the Philippines and 40 per cent in Hong Kong). In Taiwan, 55 per cent of those aged 50+ support the use of behavioural biometrics, above all other ages.

The findings provide us with the reminder that a one-size fits all approach to the adoption or delivery of biometrics won't work.

Today's access to data enables banks to operate in a customer-obsessed environment; making it easier than ever to understand the needs, desires and preferences of audiences in order to tailor their experiences with the bank.

[7] International Biometrics and Identity Association

The Next Generation of Banking Security

Use of behavioural biometrics in financial service institutions has advanced across the world, led by the UK in particular. Most notably, The Royal Bank of Scotland introduced behaviour biometrics to monitor visitors to their websites and determine access to applications and products.

With behaviour biometrics set to be the next generation of authentication and security for banks, gaining buy-in to passively monitor behaviours may take some time.

Reasons Given by Those Not Comfortable Using Biometrics for Banking	AU	NZ	HK	TW	PH
I don't want the bank to have access to my identity data	46%	31%	47%	60%	34%
Biometrics are not safe, my biometrics data can be stolen and it is not like a pin, which can be changed or replaced	37%	31%	49%	58%	55%
I am uncertain about the safety of my data once collected	46%	35%	52%	55%	42%
I am concerned banks will be required to share my biometric information with the government	31%	20%	25%	38%	22%
Biometrics technology is not reliable	29%	15%	33%	32%	24%
I am just not comfortable	57%	40%	25%	30%	39%
Other reasons	6%	7%	8%	5%	5%

When asked why they are not comfortable with banks using biometrics, responses varied from country-to-country.

In mature banking markets such as Australia and New Zealand customers were 'just not comfortable' with banks using their biometric information. While these countries typically have a higher adoption of advanced technologies, it appears that culturally their citizens fiercely guard their privacy.

In Hong Kong, citizens were most concerned about what would happen to their data once collected (52 per cent) while in the Philippines (55 per cent) customers were concerned that their biometric data was not safe and that it could not be replaced. This demonstrates the need for banks to regularly communicate to their customer about not only the way in which they safeguard their biometrics but the added security level they offer.

Biometrics are a part of a person's digital identity. It's therefore not surprising that there is also a sense of attachment to identity markers that could be accessed without consent.

Data from the *Unisys Security Index* reveals citizens across Asia Pacific are very concerned about identity theft, and banks need to ensure they are regularly demonstrating the value of advanced authentication and biometrics as part of their customer experience.

As customers continue to embrace digital services, banks need gain trust and build consumer confidence in the digital services they provide by not only showing how data is protected, but providing control over when, where and how that personal biometric information is used.

About Unisys

Unisys is a global information technology company that builds high-performance, security-centric solutions for the most digitally demanding businesses and governments on earth.

Unisys offerings include security software and services; digital transformation and workplace services; industry applications and services; and innovative software operating environments for high-intensity enterprise computing.

More than 500 financial institutions worldwide rely on Unisys solutions. Elevate™ is an end-to-end, digital banking software platform and suite of applications designed to help financial institutions deliver an instantly secure, omnichannel banking experience to their customers. Elevate is secured with Unisys' Stealth®, an identity-based microsegmentation security software that allows banks to microsegment and conceal critical assets and establish encrypted channels for secure user, application and system communication. For more information on Unisys' financial services capabilities, please visit http://www.unisys.com/industries/financial-services

For more information, visit: www.unisys.com

or email UnisysAPAC@unisys.com.

More valuable industry research can be found at www.unisys.com/bankinginsightsapac.

05/19

19-0122