



MOBILE IDENTITY:
THE FUSION OF FINANCIAL SERVICES,
MOBILITY AND IDENTITY



CONTENTS

FOREWORD	4
1.0 MOBILE IDENTITY	6
2.0 FINANCIALLY MOBILISED OMNIPRESENT CONSUMERS	27
2.1 The ‘Omnipresent’ Mobile Consumer	27
2.2 The Confluence of Identity, Privacy and Security – this is now one conversation, not three	30
2.3 “Identity of Things”, “Privacy”, “Internet of Trust”	32
3.0 MOBILE IDENTITY RESEARCH	34
3.1 Methodology	34
3.2 Financial Services Executive Study	35
3.2.1 Drivers of Existing Identity Systems and Processes	35
3.2.2 Changes to Investments in Identity Systems and Processes	36
3.2.3 Institution Identity Strategies and Responsibilities	36
3.2.4 Trust and Third-Party Identity Providers	38
3.3 Mobile Identity Consumer Study	39
3.3.1 Authentication Method Descriptions	39
3.4 Federated Identity	40
3.5 Second Factor Authentication	41
3.6 Mobile Digital Signature	43
3.7 Incremental Appeal of Authentication Methods	44
4.0 MOBILE IDENTITY TECHNOLOGY FOR THE INTERCONNECTED FINANCIAL SERVICES INSTITUTION	46
4.1 Identity Technology Key Developments and Roadmap	46
4.2 Authentication in a Interconnected Financial Services World	49
4.3 Federated Identity in a Interconnected Financial Services World	54
4.4 Mobile Digital Signature in an Interconnected Financial Services World	56
4.5 Mobile ID = Mobile Number + Device + Behaviour	58
4.6 Mobile Threat Defence	60
4.7 Secure Omni-Present Intelligent Identity	62
5.0 CONCLUSIONS	65
6.0 ABOUT THE AUTHOR	66
7.0 ACKNOWLEDGEMENTS	67
8.0 NOTES & REFERENCES	68

FOREWORD



Welcome

It's my pleasure to present the tenth in my series of financial services industry thought leadership reports: **Mobile Identity – The Fusion of Financial Services, Mobility and Identity**. For this report, we developed some unique research methodologies that allowed us to discover some fascinating new information about how financial institutions can unlock the trust needed to digitally engage the 'no-finapp-phobic'¹ Gen X and Ys.

This report is a look into generational change – particularly as it affects Gen X and Y, who together make up half of the global population². Their adoption of mobile digital technology will both expose institutions to risk and create opportunity. My central argument is that mobile digital technologies have changed how these generations prefer to be identified. The trust paradigm has shifted from having to prove who we are, to being recognised for who we are. Both our identities and our consumption of financial services are now inextricably fused with our mobile device, which is why mobile identity is a critical issue and why this research is so timely.

In just seven years, since the advent of the smartphone, these devices have become the primary means for consumers to access financial services. This inflection point has forever changed the industry. We are now transitioning to an 'omnipresent' customer engagement model, characterised by expectations of predictive, personalised and presence-based financial application experiences that are part of the fabric of our increasingly interconnected lives.

But just as the mobile device has become our gateway to the financial services world, it has also become the source of new risks for both individuals and institutions. Cybercrime has become the domain of industrial-strength perpetrators who are often highly organised, highly skilled, abundantly resourced and keen to exploit any points of weakness in the internet and the devices and systems connected to it. This seismic shift in the nature of cybercrime requires us to reimagine identity and its role in securing our personal lives, our information, our institutions and the services they offer.

In my last report 'Analyse This, Predict That – how institutions compete and win on analytics', I emphasised that data analytics brings new risks to financial institutions, particularly around the appropriate use of personal information. Critically, I argued that a new customer engagement model is required – one that ensures that analytics enhances value, whilst also reinforcing the trust that consumers place in their financial institutions. Since then, growing numbers of major security breaches have been reported – unfortunately, the insufficient protection and monitoring of customers' personal information has been behind many of these.

This study across seven countries within the Asia Pacific region, Europe and America explores our changing attitudes towards the identity of individuals and mobile devices. We begin by introducing a 'Generational Acquisition/Digital Engagement Matrix' that illustrates how an institution's future growth prospects can be determined by its ability to firstly acquire and then digitally engage Gen X and Y, and the wallets they control. Against this strategic backdrop, we then consider the technological impact of mobility and identity. We then present the results of research into financial services executives and consumer attitudes towards a range of identity topics and interactions that can be enabled by mobile devices, and analyse the impact these would have on consumers' relationships with their financial services institutions.

Lastly, we present a vision for secure, intelligent omnipresent identity in the interconnected financial services world. Here, we both explain some world-leading technological developments, including those that Telstra has directly invested into, and discuss the role that next-generation identity, access management and security technologies can play in helping your institution map out its trust journey.

We show that mobile identity is a fundamental enabler for innovation, and – just as importantly – that mobile identity is critical to the trust relationships that will unlock access to many wonderful new experiences that will be created as mobile financial services continue to evolve.

The insights presented in this report were only made possible by the generous participation of industry and research partners, to whom I am sincerely grateful.

We welcome the opportunity to provide you and your management team with an in-depth briefing on what these insights mean to your institution. At the back of this document, we've provided a list of contact numbers. Please also visit www.telstraglobal.com/mobile-identity for further information.

Rocky Scopelliti

Global Industry Executive – Banking, Finance & Insurance

Telstra Global Enterprise Services

1.0 MOBILE IDENTITY

KEY INSIGHTS



The financial services industry is moving from an age of digital disruption to one of digital survival. For example, in markets such as the US, Accenture predicts that full-service banks could lose approximately 35 per cent of their market share by 2020 to “Pure Plays” – whether online or mobile – and up to 25 per cent of US banks could disappear completely during that same period³. Neo-banks (e.g. Simple, Moven, GoBank, and Bluebird) were reported to have secured nine per cent of the US market in 2013. McKinsey & Company analysis suggests that banks that are digital laggards could see up to 35 per cent of their net profit eroded, while winners may increase profits by 40 per cent or more. They predict that

within five years, digital sales may account for 40 per cent or more⁴ of new inflow revenue to institutions in the most progressive geographies and customer segments. (This is predicted to be highest in Europe, reaching 50 per cent by 2018.) The battle is about relevance – digital relevance – and the people who will decide the winners are Gen X and Y, who today account for approximately half of the world’s population and are the custodians of existing wealth and wealth creation into the future.

We analysed information from 318 financial services executives across the Asia Pacific region, Europe and the US and 4,272 consumers across seven countries (Australia, Singapore, Indonesia, Malaysia, Hong Kong, UK

and the US) on the topics of identity and security. What we learned is that for the financial services industry to transition into this new mobile digital era, significant developments in the trust paradigm are required to attract and engage Gen X and Y and provide them with the security they desire.

Here are the top ten insights that we believe financial institutions need to know and consider to succeed in their identity transformations.

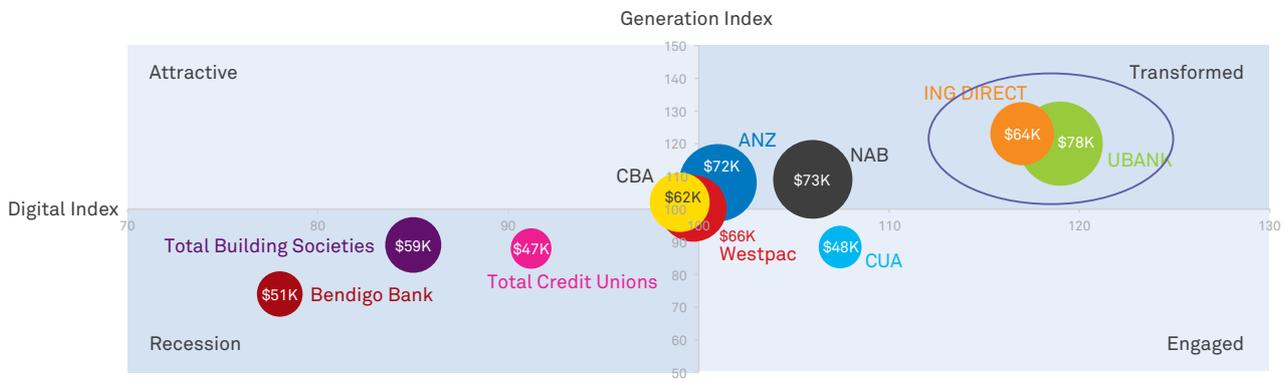
1. The battle to acquire and digitally engage Gen X and Y is on. The Online Pure Plays' are 'winning wallet' but is it now the Mobile Pure Plays' turn

“Up to half of the world’s banks will disappear through the cracks opened up by digital disruption of the industry.”
- Francisco Gonzalez Rodriguez, Chairman and CEO BBVA, 2015

In my report last year, we presented the Competitive Growth Model that featured two major trends: firstly, the inter-generational wealth transfer from the ageing baby boomer and pre-boomer generations to Gen X and Y and secondly, technology proliferation as Gen Z – the digital natives – are introduced to financial services. These trends have created a disruption zone for new entrants to squarely focus their propositions on Gen X and Y. We have now further developed this model to create a Generational Acquisition/Digital Engagement Matrix. This enables us now to assess the relative performance of institutions and how they are transforming their businesses in response to these trends.

In order to understand how exposed an institution is to ‘Generational Recession’ or how well it is performing on ‘Generational Transformation’, we rate the institution based on the dynamics of its generational profile (Generational Index) and digital channel adoption (Digital Index) compared with the industry average (with an index of 100 being the industry average). We also consider a third factor measuring what is at risk – in other words, the net worth of the customers concerned. In this case, we use Average Footings (\$AUD) or dollars held in traditional banking products at the institution⁵. Using the Australian banking market, we analyse how some institutions are performing (see Figure 1).

Figure 1: Generational Acquisition/Digital Engagement Quadrant - Australian Market



Sources: Roy Morgan Single Source, July – December 2014; Telstra Research 2015

1.0 MOBILE IDENTITY

KEY INSIGHTS (CONT.)

Transformed Quadrant – *the institution attracts Gen X and Gen Y customers as well as engaging with them via digital channels.*

Based on this index, the Online Pure Plays – UBank (an online division of NAB) and ING Direct – are relatively outperforming the other Australian banks listed and considered ‘Transformed’ in our quadrant classifications. All the major banks (NAB, ANZ, CBA, Westpac) fall within the standard deviation and are close to the average; however, NAB and ANZ are clearly attracting a greater size of wallet (average 14 per cent) compared with CBA and Westpac.

Recession Quadrant – *the institution struggles to attract Gen X and Gen Y consumers or engage with them via digital channels.*

At the opposite end, in the ‘Recession’ quadrant, are Bendigo Bank and the community institutions displayed collectively as Total Credit Unions and Total Building Societies. Attracting the younger demographic is a well-known challenge for this part of the industry. The average age of a Credit Union customer in Australia is 51.5 years, compared with 42.5 years for banks⁶. By comparison, the community-based institutions have the lowest average size of wallet, ranging between 24 per cent and 40 per cent lower than the best performer, UBank. The results indicate that players in this quadrant are most exposed to inter-generational wealth transfer.



Engaged Quadrant – *the institution engages customers via its digital channels but it struggles to attract Gen-X and Gen-Y consumers.*

Credit Union Australia (CUA) has made good progress with digitally engaging its customers and is positioned in the ‘Engaged’ quadrant. However, like the other community-based institutions, CUA hasn’t attracted Gen X and Y and has the second-lowest size of wallet.

Attractive Quadrant – *the institution attracts Gen-X and Gen-Y consumers but struggles to engage with them via digital channels.*

Of interest is the absence of any player in this quadrant in the Australian market, perhaps suggesting that digital is a necessary precondition to attract Gen X and Y.

*UBank and ING Direct are relatively new entrants in the Australian market. UBank was established in 2006 and ING Direct in 1999 – both use eVerification processes for on-boarding new customers online. In that short period of time, they have acquired approximately two million customers and penetrated 6 per cent of Australia’s Gen X and Y population. This demonstrates, firstly, how quickly digital can move a market, and secondly, how digital relevance translates into customer acquisition. The question now is: what will happen now that we have moved into a **mobile first** financial services world? If the developments in the US market referred to earlier, together with the global FinTech phenomenon, are anything to go by, then we can anticipate the ‘Mobile only Pure Plays’ will change the game once more.*

2. The basis of identity and security is trust. Establishing trust is paramount – despite customers trusting financial institutions more than other organisation types, few are very satisfied with their current institution’s security performance

“Trust is ours to lose, though it is (also) ours to protect. If we mess up that trust through this transition and find our way to not having guided them to think that we are always going to be there to protect them, we are going to lose them. If we don’t protect that trust, it’s game over.”

- Richard Davis, President and CEO US Bancorp, 2015

When it comes to financial institutions, trust is critical for consumers and is the most important driver of choice when it comes to choosing an institution. Trust comes in multiple

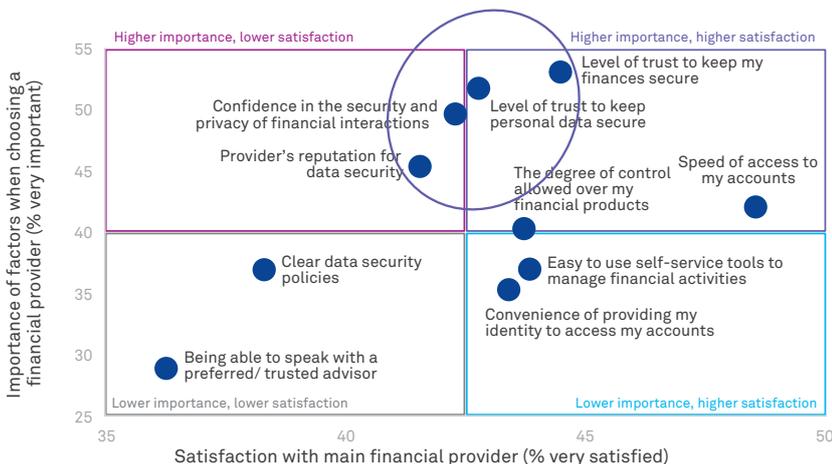
forms – paramount is the trust that finances are secure (critical for 53 per cent), but almost as important is security of personal information (52 per cent). Trust is also reflected in the need for confidence in the institution to provide security and privacy (50 per cent), and the institution’s overall reputation for data security (48 per cent). These factors are important to consumers irrespective of the country in which they live.

Yet when we compare to how satisfied consumers are with these same important factors, fewer than half of all consumers state that they are ‘very satisfied’ with their main financial institution. This indicates a disconnect between what consumers want from their institutions when it comes to security and what they are currently getting (see Figure 2).

The basis for identity and security is trust – trust that the holder of the personal information will keep it safe and secure and not disclose details without authorisation. In a positive result for financial institutions, they are viewed as the type of organisation most trusted to manage personal information – even ahead of the Government (except in Singapore, where the Government is most trusted).

Mobile operators rank high in the list in Table 1, just ahead of internet retailers (who are particularly positively perceived in the UK). Social networks and Google are the least trusted, despite the plethora of personal information already held by such organisations.

Figure 2: Drivers of Satisfaction/Choice of Financial Institution (Global)



Source: Telstra Research 2015

Table 1: Most Trusted Identity Institutions (Global)

Most trusted organisations with personal information – average rank	
1	Your bank or financial institution
2	Government or semi-government body
3	Mobile operator/communication services provider
4	Internet retailers, e.g. eBay, Amazon
5	Specialist identity provider
6	Your mobile handset manufacturer
7	Postal service
8	Mobile App stores
9	Google
10	Social networks

1.0 MOBILE IDENTITY

KEY INSIGHTS (CONT.)

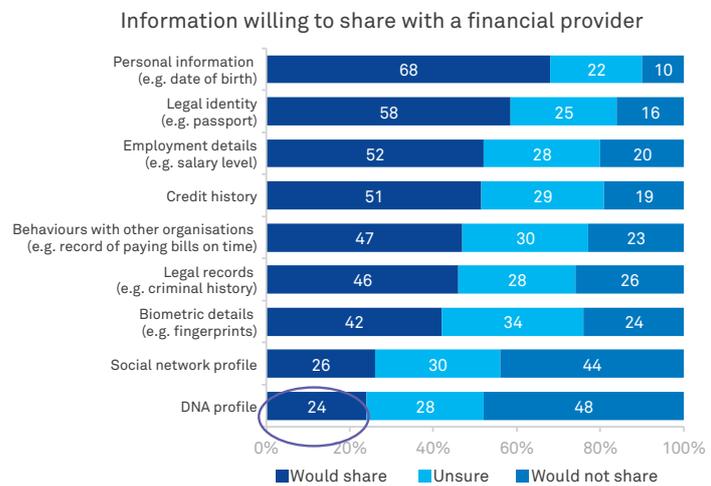
3. Consumers are more willing to share personal information with financial institutions than other types of institutions – even their DNA, particularly as their wealth increases

“Confidence in the banking industry is on the rise, and trust in customers’ own financial services providers is high. But customers are on the move, with unprecedented access to competing banks and new types of financial service providers. Banks must earn the highest levels of trust in order to retain customers, win more business and create genuine loyalty.”

EY Global Consumer Banking Survey, 2014

The fact that consumers are willing to trust their financial institution with personal information (above all others) places institutions in a place of privilege. In fact, one in five consumers would be happy to go as far as sharing their DNA if it would help secure their financial and personal information (see Figure 3).

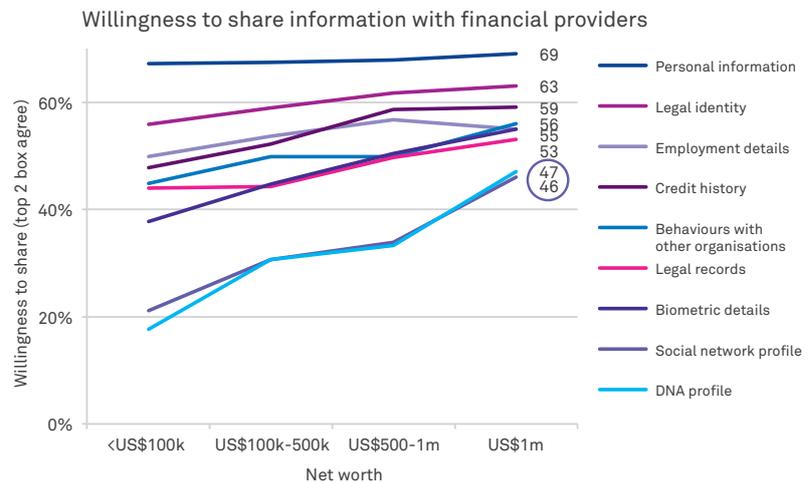
Figure 3: Willingness to Share Personal Information with Financial Services Institution



Source: Telstra Research 2015

We found those with more to invest are more willing to ‘do what it takes’ to ensure security. A staggering 47 per cent of those with a net worth of more than US \$1 million would share their DNA profile with a financial provider (see Figure 4).

Figure 4: Willingness to Share Personal Information with Financial Services Institution (by Net Worth \$ (Total Investments & Assets – Debt))



Source: Telstra Research 2015

4. Robust authentication methods improve customer satisfaction, but institutional performance varies significantly – this gives the leaders a distinct competitive advantage



“Since launching in Australia ING Direct has gained the advocacy of our customers by delivering customer-focused products and services. We are now looking to leverage the trust they have in us to become their primary bank.”

**- Simon Andrews,
Chief Operating Officer,
ING Direct, 2015**

When asked how happy they are with their main financial institution's authentication methods overall, only 42 per cent of consumers are 'very satisfied', but this does vary by country. Hong Kong consumers are the least satisfied with their institutions, with just 14 per cent being 'very satisfied'. Singapore and Malaysia fare only slightly better, with 22 per cent and 30 per cent respectively happy with their institution's authentication methods.

This is important not only because it is a key driver of institution choice, but also because it strongly influences advocacy. Taking consumer ratings of financial institutions across all seven countries, and directly comparing customer satisfaction with the institution's identity and authentication methods and the Net Promoter Score (NPS) for the institution as a whole, yields a very strong correlation coefficient.

1.0 MOBILE IDENTITY

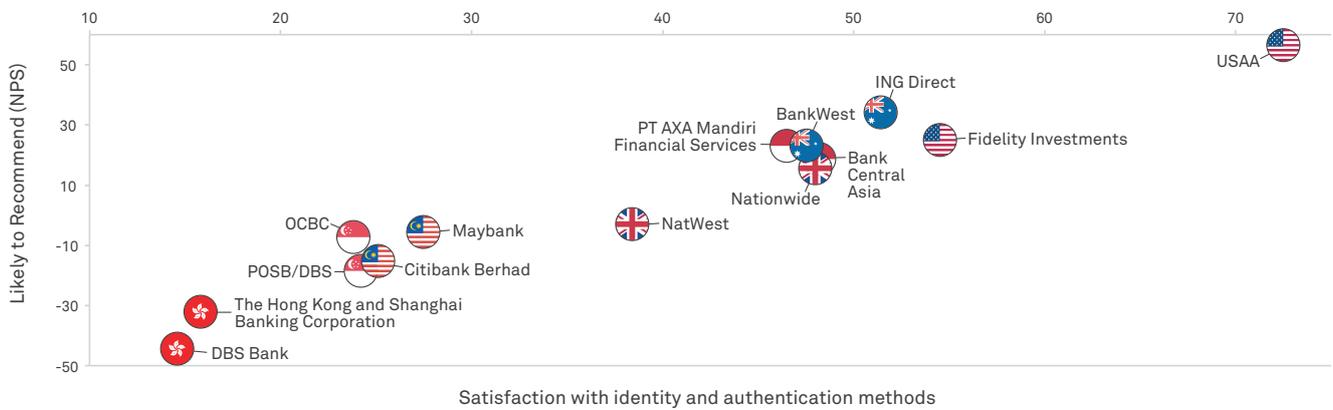
KEY INSIGHTS (CONT.)

Figure 5 below shows the top two financial services institutions in each country, based on customer satisfaction with identity and

authentication methods. While direct comparison between the countries is difficult due to cultural tendencies for survey ratings (the US is well-known

for 'easier grading'⁷), the correlation between the data sets is almost perfect for these institutions (see Figure 5).

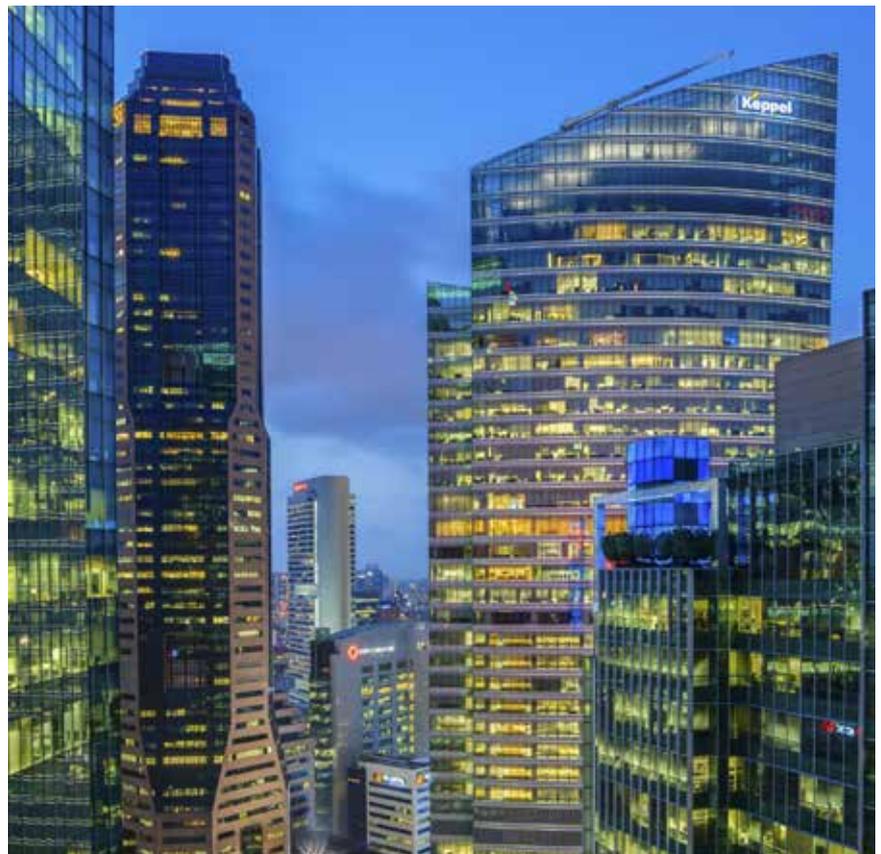
Figure 5: Advocacy/Satisfaction with Authentication Methods (Global Top 2 Per Country)



Source: Telstra Research 2015

The US is a clear leader on both dimensions and USAA's recent biometrics developments (see Case Study 3) may explain the very high satisfaction levels. Of interest also is ING Direct in Australia, who not only lead the Transformation Index (see Figure 1), but have a clear advantage in their NPS/ Authentication Satisfaction performance.

The significant variation in performance by institutions within each country studied leads us to conclude that the opportunity exists for institutions to differentiate using identity and authentication methods that provide high levels of security for personal information.

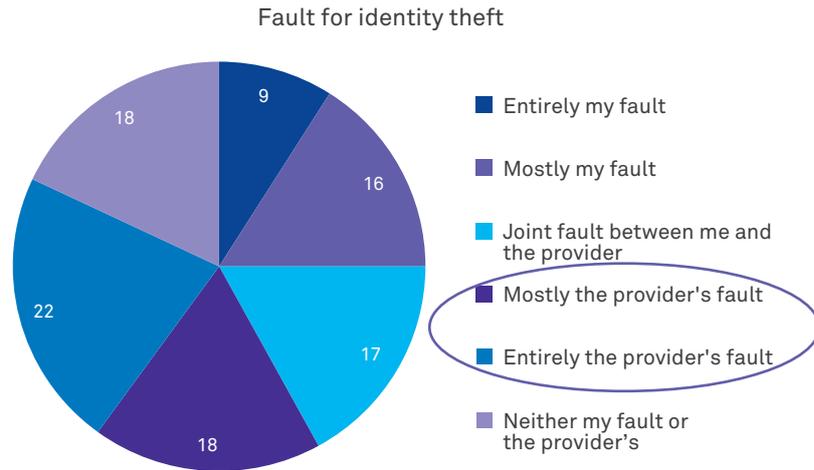
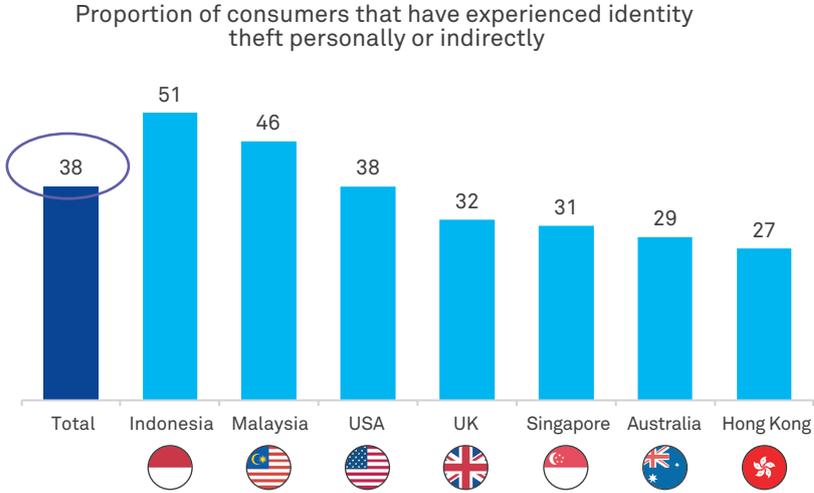


5. Identity theft is impacting Gen X and Y, particularly as their wealth increases, and many think it's the institution's fault – this will inevitably lead to customers defecting

“Good cybersecurity practices are not a minority sport for technologists only.” – **Andrew Gracie, Executive Director, Bank of England, 2015**

Security of finances and personal information is not just a key acquisition driver; it is also essential for retaining customers. Specifically referring to digital interactions with financial institutions, almost one in five consumers (19 per cent) claim to have personally experienced identity theft or to feel their identity has been compromised, and (23 per cent) know someone to whom this has happened. Critically, 40 per cent of them believe it was the institution's fault. The net impact is that around two out of every five consumers (38 per cent) have experienced digital security failings, either personally or indirectly. In Malaysia and Indonesia this rises to half of all consumers – 51 and 46 per cent respectively (see Figure 6).

Figure 6: Identity Theft (Global)



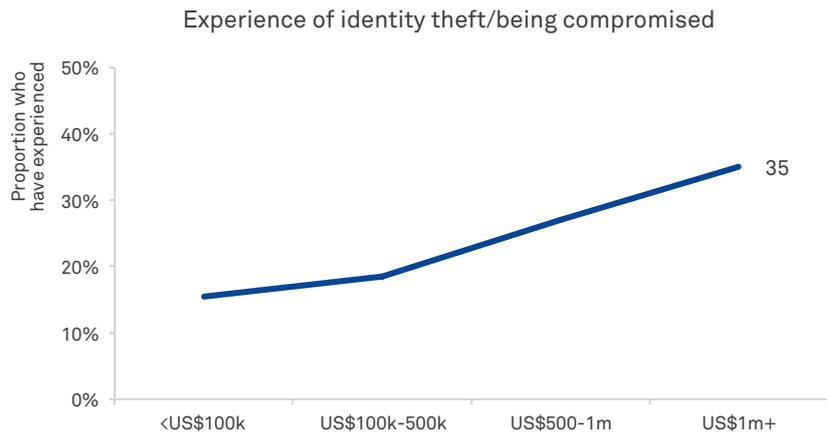
Source: Telstra Research 2015

1.0 MOBILE IDENTITY

KEY INSIGHTS (CONT.)

Of further concern, it seems that those with the most to invest are the most likely to experience security failings with digital financial transactions – over a third (35 per cent) of consumers with a net worth of more than US \$1 million have personally experienced such a situation (see Figure 7).

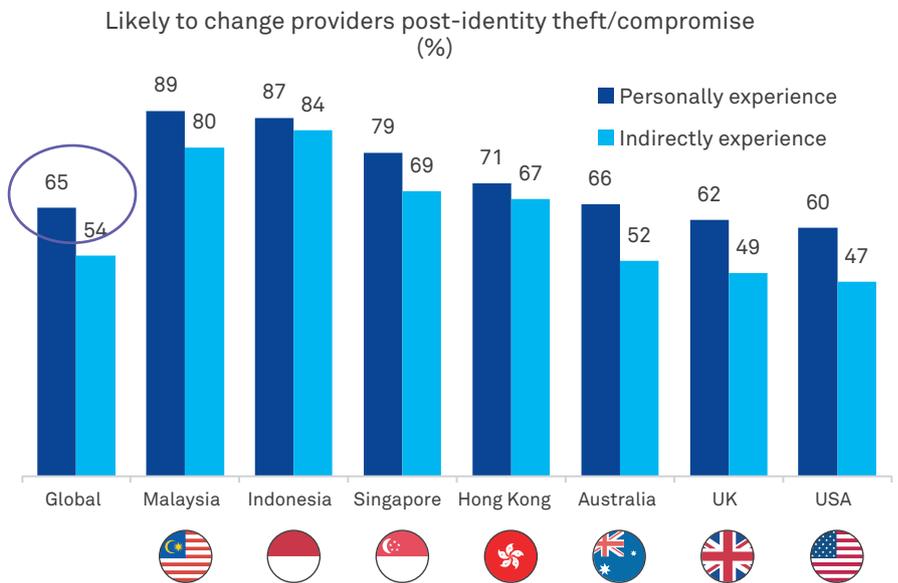
Figure 7: Identity Theft High Net Worth (Global)



Source: Telstra Research 2015

The impact of identity theft on consumers does not just involve financial loss (although 58 per cent have experienced some kind of financial loss and 22 per cent a major loss), but also inconvenience, insecurity around future transactions and, for some, a feeling of personal violation. These factors add up to a high likelihood of switching institutions – two thirds (65 per cent) of consumers state that having their identity stolen or compromised would make them very likely to switch institutions, and almost as many (54 per cent) said the same if they knew someone who had experienced identity theft. In Malaysia, Indonesia and Singapore, those numbers jump significantly with eight to nine out of every ten consumers stating that they would be likely to switch institutions should their identity be compromised. That is a huge risk for financial institutions and will have an impact on business well beyond recompensing customers for financial losses (see Figure 8).

Figure 8: Identity Theft & Likelihood to Switch Institution

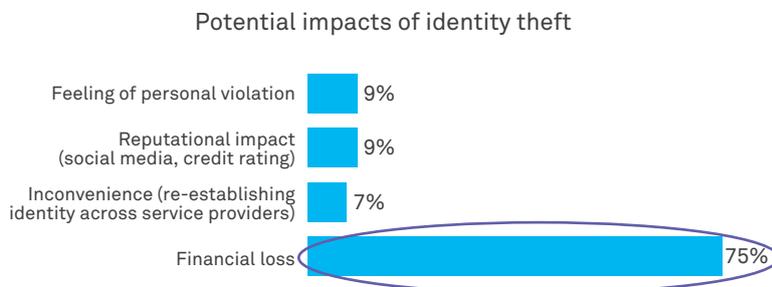


Source: Telstra Research 2015

The financial services industry is well aligned on matters concerning customers and identity theft. Institutions across all regions and business types ranked financial

loss (75 per cent) as being the most significant impact for customers. Sixty three per cent of consumers agree and ranked it as their number 1 concern (see Figure 9).

Figure 9: Perceived Consumer Concerns with Identity Theft by Institutions



Consumer Concerns with Identity Theft (Global)

Concern on impact from identity theft – ranked

1	Financial loss	63%
2	Inconvenience of resolving	11%
3	Feeling insecure about other/future personal information stored	10%
4	Feeling personally violated	10%
5	Reputation impact	7%

Source: Telstra Research 2015

1.0 MOBILE IDENTITY

KEY INSIGHTS (CONT.)

6. Passwords are a flawed authentication method – and everyone knows it



“The whole notion of passwords is based on an oxymoron. The idea is to have a random string that is easy to remember. Unfortunately, if it’s easy to remember, it’s something non-random. And if it’s random, then it’s not easy to remember.”

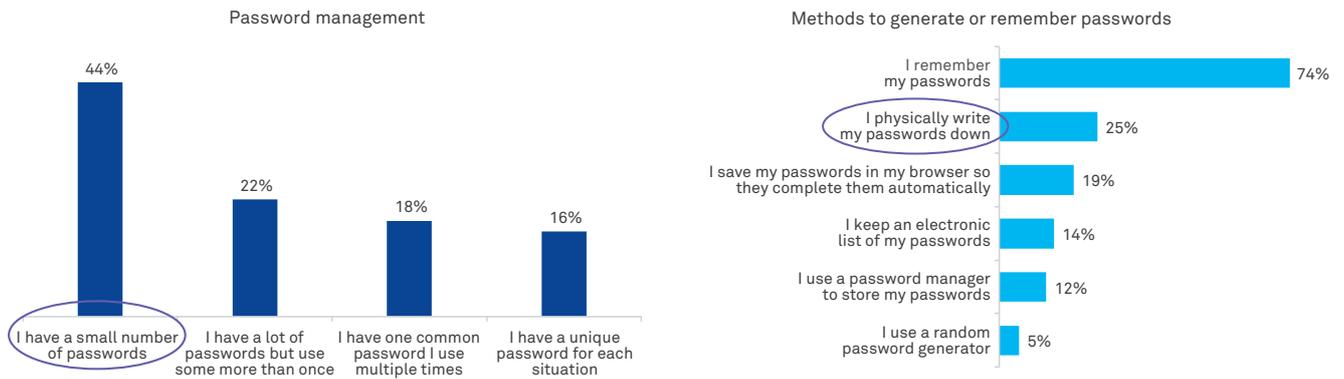
**- Bruce Schneier,
Author, 2008**

Consumer concerns about security, coupled with common usage of passwords across financial and other digital accounts, would suggest that consumers carefully manage their passwords to ensure they are as secure as possible. As is very well-known, this is definitely not the case.

Almost half (44 per cent) of consumers have a small number of passwords that they use multiple times across their digital identities, and one in five (18 per cent) use just one common password across all digital accounts (see Figure 10).

If that were not concern enough, we see that a quarter of consumers (25 per cent) physically write their passwords down, presenting an even greater risk to security. Only one in ten (12 per cent) uses a password manager and one in 20 (5 per cent) use a random password generator (see Figure 10).

Figure 10: Managing Passwords

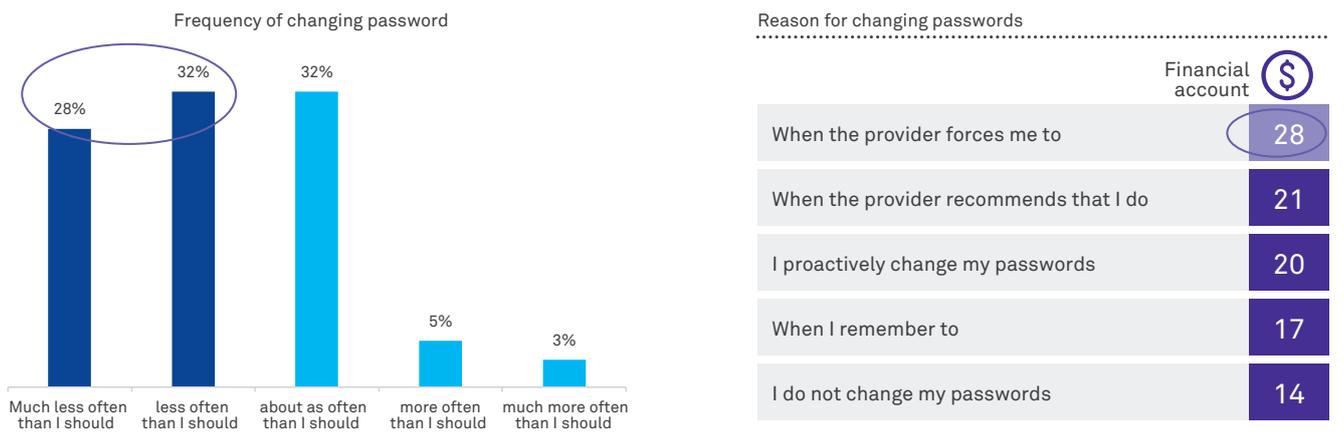


Source: Telstra Research 2015

Alongside this, most consumers (60 per cent) also admit that they do not change their password as often as they should; when they do, it is usually because they are prompted by their

financial services institution. 14 per cent don't even change passwords, while only one in five (20 per cent) report proactively changing their passwords (see Figure 11).

Figure 11: Changing Passwords



Source: Telstra Research 2015

1.0 MOBILE IDENTITY

KEY INSIGHTS (CONT.)

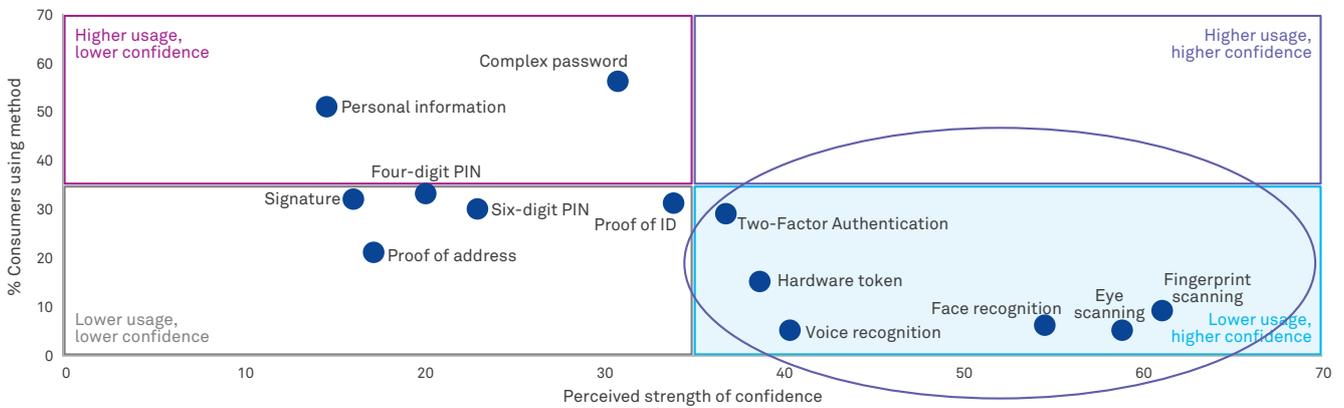
7. There is a disconnect between usage of authentication methods and their perceived security strength. The industry still thinks customers prefer passwords – it’s time to look to authentication methods that garner greater trust

“We want to identify people for who they are, not what they remember.”
- Ajay Bhalla,
CEO, MasterCard, 2015

When we ask consumers how strong they perceive each authentication method’s security to be in terms of protecting their personal and financial information, it is clear that there is a significant disconnect between the methods commonly used and consumer confidence in their security.

Complex passwords and the provision of personal information, the most commonly used methods, are both viewed as having significantly lower security than biometric options – particularly fingerprint scanning, eye scanning, facial recognition and two-factor authentication options (see Figure 12).

Figure 12: Authentication Methods – Usage & Perceived Strength (Global)



Source: Telstra Research 2015

Fingerprint scanning is perceived to be the strongest method of authentication in Australia, Malaysia and Singapore, while the US and Hong Kong rate eye scanning as the most secure method; Indonesia and the UK believe strongly in facial recognition. These three biometric methods achieve at least two of the top three security ratings across all markets. Use of a hardware token appears in the top three for Hong Kong and Singapore, while two-factor authentication rates highly in Australia, Malaysia and Singapore (see Table 2).

Table 2: Authentication Methods – Usage & Perceived Strength (by Country)

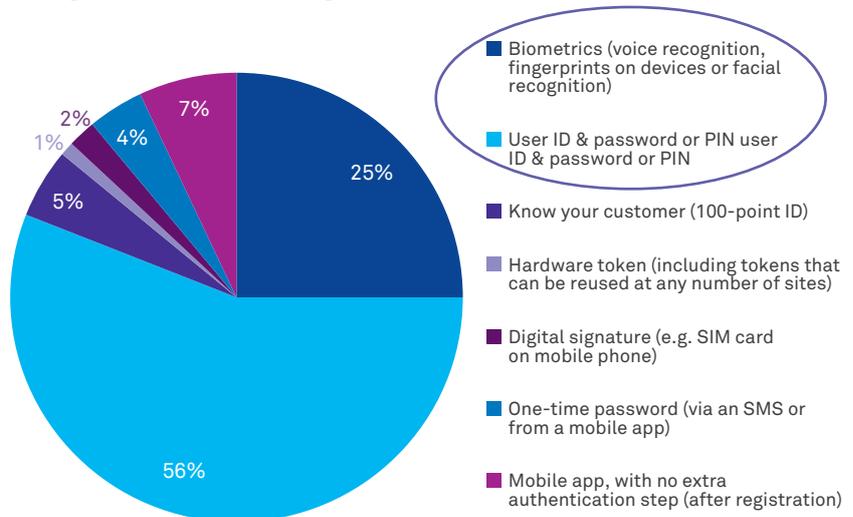
							
Fingerprint scanning	55	30	69	51	41	39	67
Eye scanning	32	31	58	32	32	39	73
Face recognition	41	23	77	22	24	57	52
Voice recognition	30	10	38	22	26	34	48
Hardware token	39	26	45	27	30	39	35
Two-Factor Authentication	45	25	50	28	34	32	35
Proof of ID	34	14	26	13	16	24	42
Complex password	28	14	49	23	15	32	29
Six-digit PIN	21	6	24	15	9	24	26
Four-digit PIN	10	3	22	13	9	16	23
Proof of address	16	9	20	9	9	13	19
Signature	14	7	19	9	11	8	18
Personal information	12	4	20	10	6	13	15

Source: Telstra Research 2015

Despite the shortcomings of password or PIN schemes outlined in point six, most of the financial services industry executives (56 per cent) still predict that their customers will want to use these methods to access financial services or applications through mobile devices (see Figure 13). These findings were consistent across all regions. Interestingly, Pure Play Online/Mobile Banks, Neo-banks and FinTechs were the only class of provider who believed customers would prefer another method (specifically biometrics) over passwords or PINs. Offsetting this finding, however, is the fact that one in four (25 per cent) predict biometrics becoming the preferred access method.

Figure 13: Customer Identity Methods via Mobile Devices (Total Institutions)

Which of the following methods do you predict your customers will expect to be able to access via mobile device to establish identity with your organisation when accessing online financial services or mobile applications



Source: Telstra Research 2015

If financial institutions are to provide the level of security that consumers are looking for, and for customers to trust that their financial and personal information will be kept safe, it is time to look to authentication methods that will aid this.

1.0 MOBILE IDENTITY

KEY INSIGHTS (CONT.)

8. The financial services industry recognises that it has underinvested in identity and security-related capabilities – but this about to change

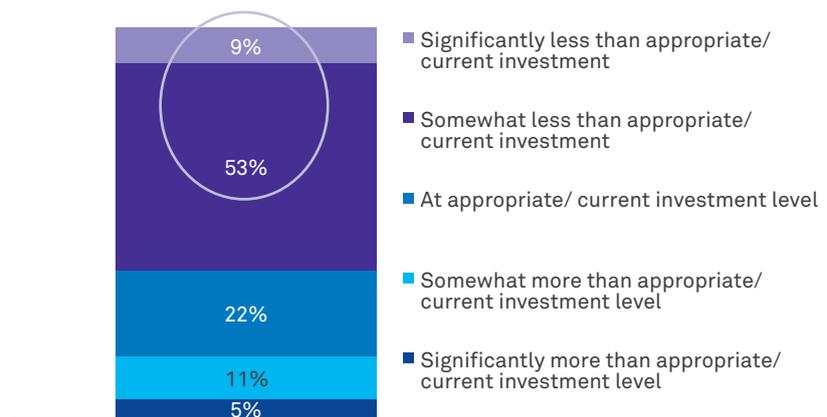
“The attackers didn’t even need to get into the bank’s services; once they got into the network, they learned how to hide the money transaction activities behind particular actions.”
- **Sergey Golovanov, Kaspersky, 2015**

The dominant view in the industry is that the current investment in identity systems is less than appropriate (62 per cent), with 9 per cent of respondents seeing significant underinvestment (see Figure 14). This finding is consistent with a global PwC study⁸ that found a lack of investment over the past two years means that many financial services institutions are falling behind the market in implementing up-to-date processes and tools to detect and

respond to today’s evolving security threats (see Figure 16). PwC reported that investment in security by financial services institutions has been stalled at four per cent of total IT budgets for the past seven years. However, our research suggests this is about to change – 87 per cent of respondents anticipate that their institution’s level of planned activity and investment in customer identity will increase, with 27 per cent of those predicting a significant increase (see Figure 15).

Figure 14: Current Activity & Investment Level (Total Institutions)

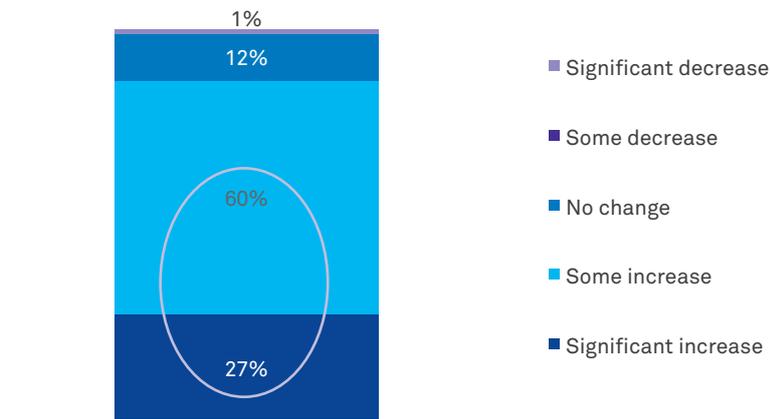
Which of the following best describes your company’s level of activity and investment related to customer identity?



Source: Telstra Research 2015

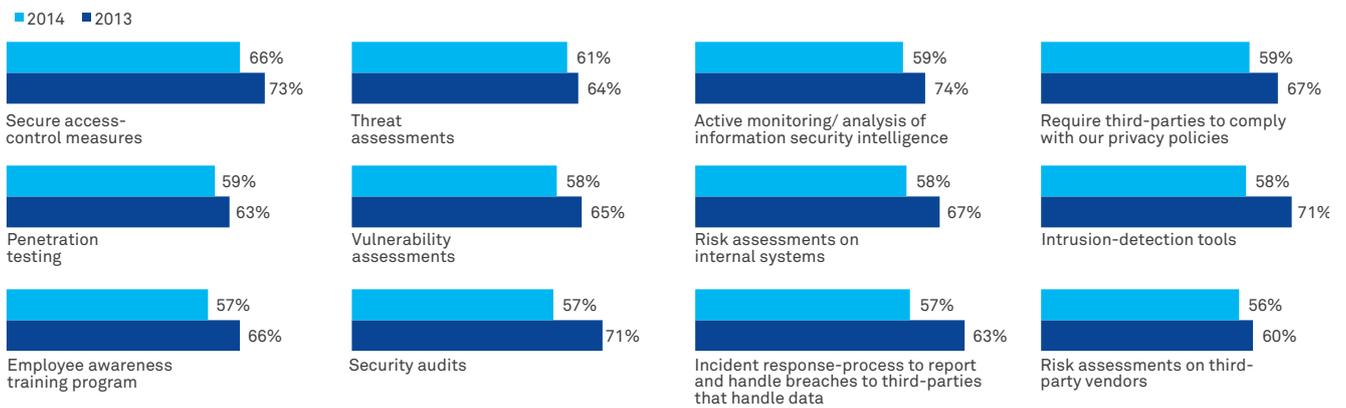
Figure 15: Planned Activity & Investment Level (Total Institutions)

Which of the following best describes your company's level of planned activity and investment related to customer identity?



Source: Telstra Research 2015

Figure 16: Falling Behind in Security Safeguards 2013- 2014



Source: PwC 2015

1.0 MOBILE IDENTITY

KEY INSIGHTS (CONT.)

9. To the 'no-finapp-phobic' Gen X and Ys, the mobile has now become the primary access device for financial services – more secure, mobile-based identity is a key part of the solution

“Enhanced customer engagement, data analytics and a mobile-first approach are the three key trends that will dominate retail banking. My first touchpoint when I look to engage with a bank is with the app.”

- Andrew Milroy, Vice President ICT Research Frost & Sullivan, 2014

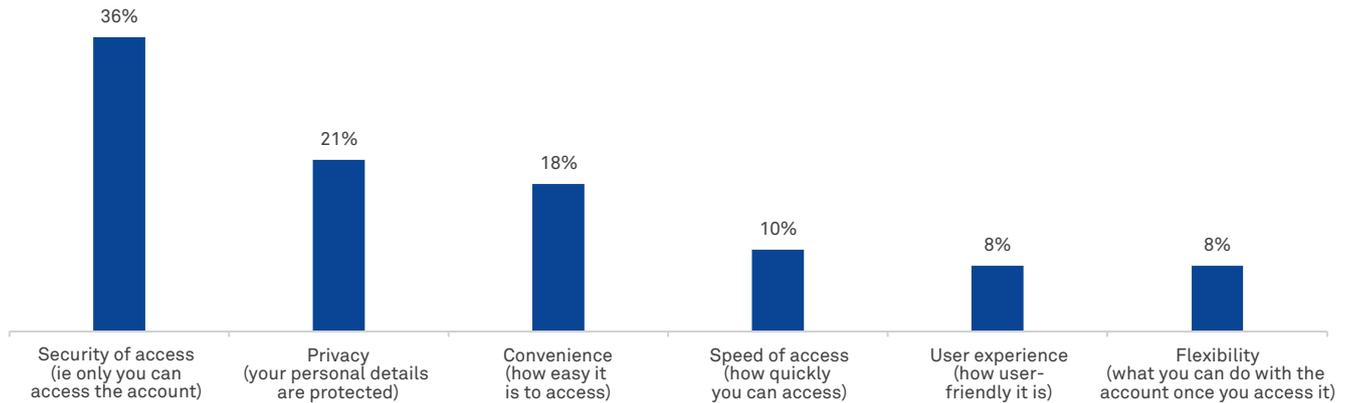
As the smartphone becomes the default access method for many financial accounts (globally, 51 per cent of consumers access day-to-day accounts through their smartphone. - see Section 2 Figures 22, 23 and 24), can it actually help provide the authentication solutions and security reassurance that consumers are looking for when accessing their financial accounts?

Consumers do, of course, want security and privacy from their smartphone app, but some also value convenience, speed of access, user experience and flexibility. Ideally an app must offer a great user experience and flexibility in managing financial accounts – and that includes the authentication method the app will use to ensure security and privacy (see Figure 17).



Figure 17: Smartphone Banking App Features

Importance rank of factors when using a smartphone app (% top ranked)



Source: Telstra Research 2015

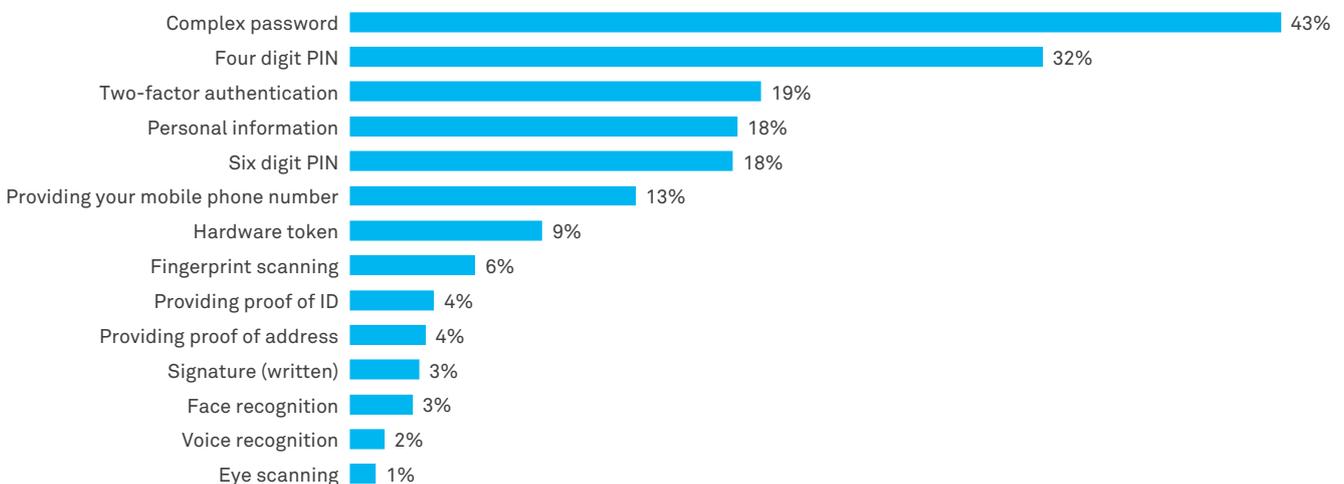
The most commonly used authentication methods for accessing smartphone apps today are complex passwords and four-digit PINs (six-digit PINs in some markets including Indonesia, Singapore, and Malaysia). As we saw earlier (see Figure 12) these are methods with low

perceived security levels. Two-factor authentication is already used by one in five consumers (19 per cent) globally – more in Singapore (51 per cent) and Malaysia (42 per cent), but fewer in the US (15 per cent) and UK (16 per cent). Fingerprint scanning has gained some traction following

its release in recent flagship devices like the iPhone, but it is only used for accessing financial accounts in six per cent of cases on average and seven per cent at best in Hong Kong. Similarly, other biometric authentication methods are only used by a select few currently (see Figure 18).

Figure 18: Smartphone Authentication Methods (Global)

Authentication methods used on smartphone app



Source: Telstra Research 2015

1.0 MOBILE IDENTITY

KEY INSIGHTS (CONT.)

10. Mobile authentication methods are highly appealing and can have a very strong business impact including acquisition, retention or defection. Gen X and Y are even prepared to pay for this security, particularly those with the most to lose

“USAA is committed to cutting-edge solutions to make our members’ financial transactions as secure as possible. The use of multifactor authentication through biometrics is one of the most effective ways to increase security protection as traditional passwords become increasingly obsolete.” - Gary McAlum, USAA’s Chief Security Officer, 2015

As part of our consumer research study, we tested the consumer appeal of three identity authentication methods: Federated Identity, Second-Factor Authentication and Mobile Digital Signature. All methods proved feasible options for institutions to offer their consumers. At a global level, it is clear that the Federated Identity, two-factor authentication and mobile digital identities that we researched all hold strong appeal for consumers. There is also a high likelihood of use, and such authentication methods would help to improve satisfaction, acquisition and retention of consumers (see Tables 3 and 4).

Table 3: Appeal of Authentication Methods (Global)

	A. Federated Identity	B. Second Factor Authentication	C. Mobile Digital Signature
Appeal of concept “Extremely appealing/somewhat appealing”	45	61	52
Likelihood to use concept “Extremely likely/somewhat likely”	41	60	49
Impact of satisfaction “Much more satisfied/a little more satisfied”	41	55	46
Likelihood to recommend provider “Would recommend 8-10”	27	35	29
Likelihood to consider new provider concept “Much more likely to consider/a little more likely to consider”	38	50	42
Likelihood to switch to concept provider “Much more likely to consider/a little more likely to consider”	37	48	42

Table 4: Appeal of Authentication Methods (by Country)

Appeal scorecard – top 2 box	A. Federated Identity	B. Second Factor Authentication	C. Mobile Digital Signature
Australia 	42	63	46
Hong Kong 	36	54	35
Indonesia 	61	77	70
Malaysia 	48	78	55
Singapore 	43	70	47
UK 	40	59	41
USA 	44	58	53

Source: Telstra Research 2015

Second Factor Authentication – is the most appealing concept tested across all countries. In particular, 78 per cent of respondents in Malaysia found the concept appealing, 77 per cent in Indonesia, 70 per cent in Singapore and 63 per cent in Australia. This aligns with consumer awareness – 72 and 62 per cent of respondents in Singapore and Malaysia respectively were aware of two-factor authentication, with the lowest awareness in the USA (45 per cent) and Hong Kong (47 per cent). This may suggest consumers are more comfortable with authentication approaches they already know and that significant education on other approaches may be required before consumers find them appealing.

Mobile Digital Signature – was the second most appealing concept in most markets, with Hong Kong being the exception.

Federated Identity – the idea of using a single set of personal credentials registered with a bank, mobile operator or identity provider to use across multiple financial services in a one-click process was also highly appealing to more than half of all consumers across all countries. At the recent Mobile World Congress, Jon Fredrik Baksaas, Chairman of the GSMA (Group Special Mobile Association), predicted that by the end of 2016, one billion users worldwide will be authenticating on a platform that offers a single sign-on feature⁹.

Indonesian respondents, in particular, reported that all three approaches had high appeal. This may suggest unmet demand for such methods of easing security concerns or may point to a cultural tendency to be positive when responding to research questions.



1.0 MOBILE IDENTITY

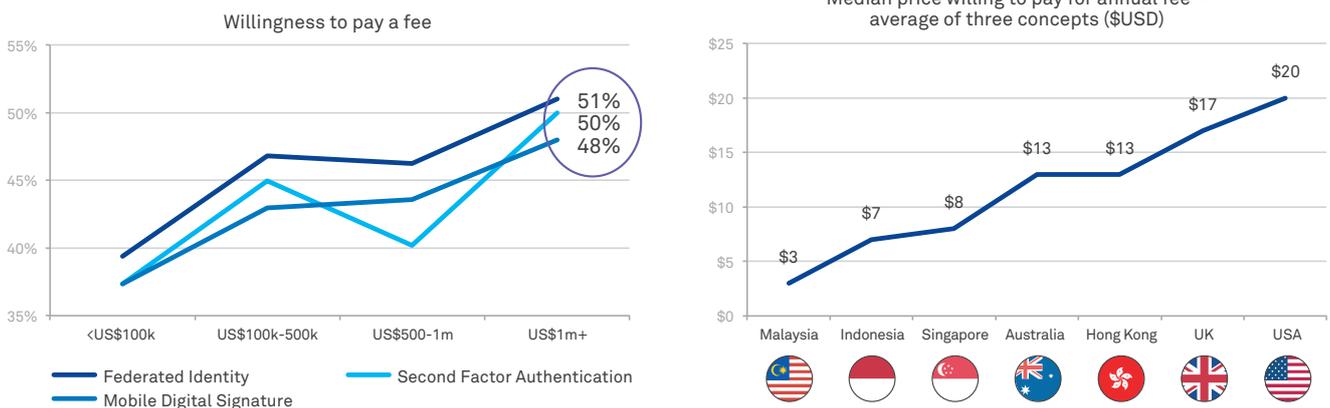
KEY INSIGHTS (CONT.)

Consumers are somewhat split over whether they would be willing to pay for such enhanced authentication methods. More than half consider authentication to be the institution's responsibility – arguably, this view is reasonable, given the potential positive impact on satisfaction, retention and acquisition for the institution.

However, a significant proportion of consumers would be prepared to pay a reasonable fee for such a service. For example, an annual fee ranging between US\$3 and US\$20 (depending on the market) would be acceptable to many (see Figure 19). Also clear is that the more that consumers 'have to lose', the more willing they are to pay

a little extra for peace of mind – half of those with a net worth of more than US \$1 million indicated a willingness to pay for such services (see Figure 19).

Figure 19: Propensity to Pay for Authentication Methods (Globally and by Country)



Source: Telstra Research 2015

Most institutions seeking more secure ways to identify and authenticate customers must balance the benefits of increased security against the risk of increasing friction in the customer experience. However, these same sensitivities mean that a flexible, well considered and well implemented Identity and Access Management architecture that does deliver a good user experience can be a key differentiator for financial service institutions. The good news is your 'no-finapp-phobic' Gen X and Y customers are willing to take this journey with you. We explore consumer reaction to the concepts in more detail in Section 3.3



2.0 FINANCIALLY MOBILISED OMNIPRESENT CONSUMERS

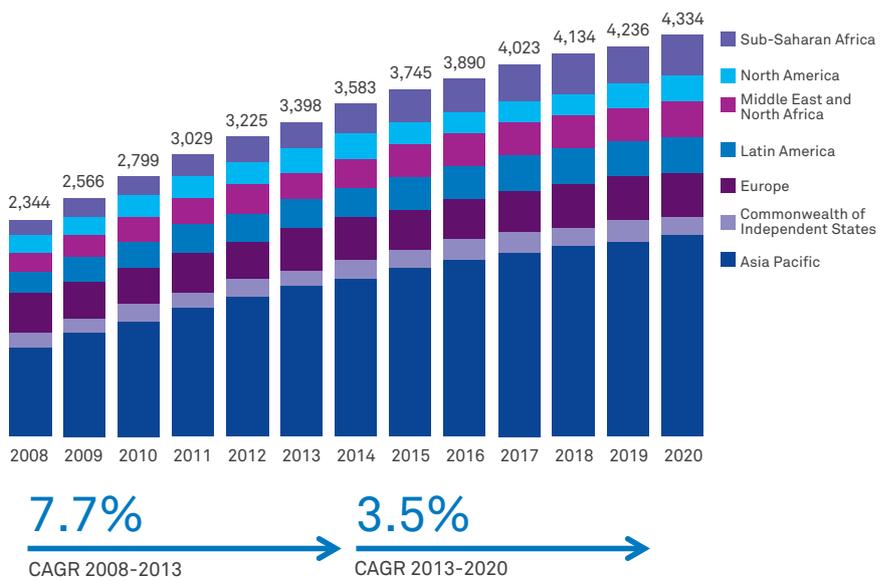
FUSION OF FINANCIAL SERVICES, MOBILITY AND IDENTITY

In this section, we take a look at how mobility, financial services and identity have become inextricably linked, and have set the scene for Omnipresence-based experiences.

2.1 The 'Omnipresent' Mobile Consumer

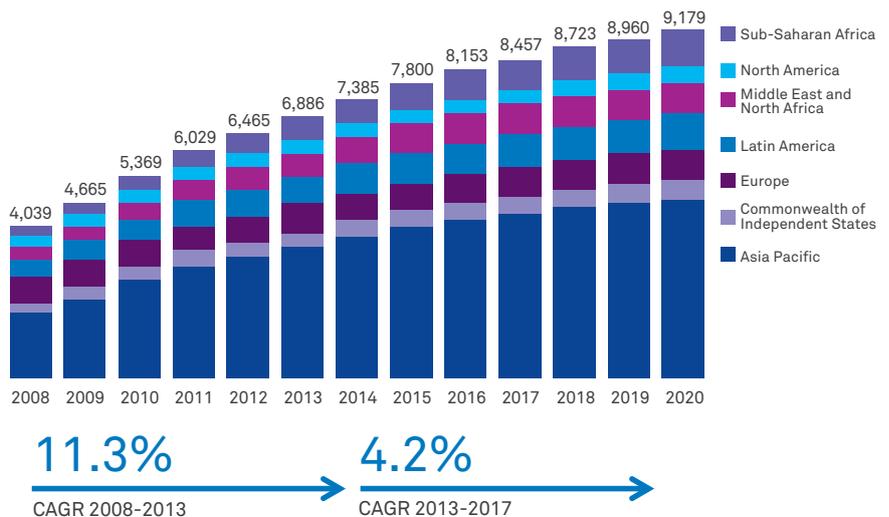
The societal and economic benefits of mobility help explain the unprecedented growth we have witnessed over the past decade so that today 3.4 billion people subscribe to mobile services¹⁰. According to the GSMA, this growth is predicted to continue at 3.5 per cent through to 2020, connecting 56 per cent of the people on earth (see Figure 20). Our unquenchable thirst for mobile services is further predicted to remain unabated at a device level with a CAGR of 4.2 per cent, from a current global SIM penetration that currently stands at 95 per cent and over 124 per cent in developed markets (see Figure 21).

Figure 20: Unique Mobile Subscribers (M)



Source: GSMA Intelligence

Figure 21: Unique Mobile Connections (M) (M, Excluding M2M)



Source: GSMA Intelligence

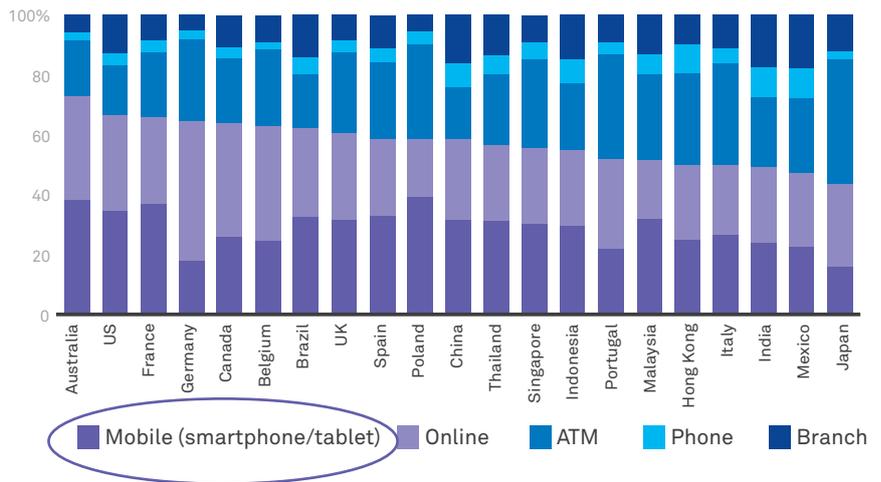
2.0 FINANCIALLY MOBILISED OMNIPRESENT CONSUMERS

FUSION OF FINANCIAL SERVICES, MOBILITY AND IDENTITY (CONT.)

This large-scale growth in mobile services has directly translated into the adoption of mobile banking. 2014 was a landmark year in banking, ushering in the age of mobile banking with mobile devices now being the most preferred way for consumers to engage with their bank. According to a report by Bain & Company¹¹, more than 50 per cent of interactions with banks are conducted through mobile devices in 18 of the 22 countries it surveyed (see Figure 22).

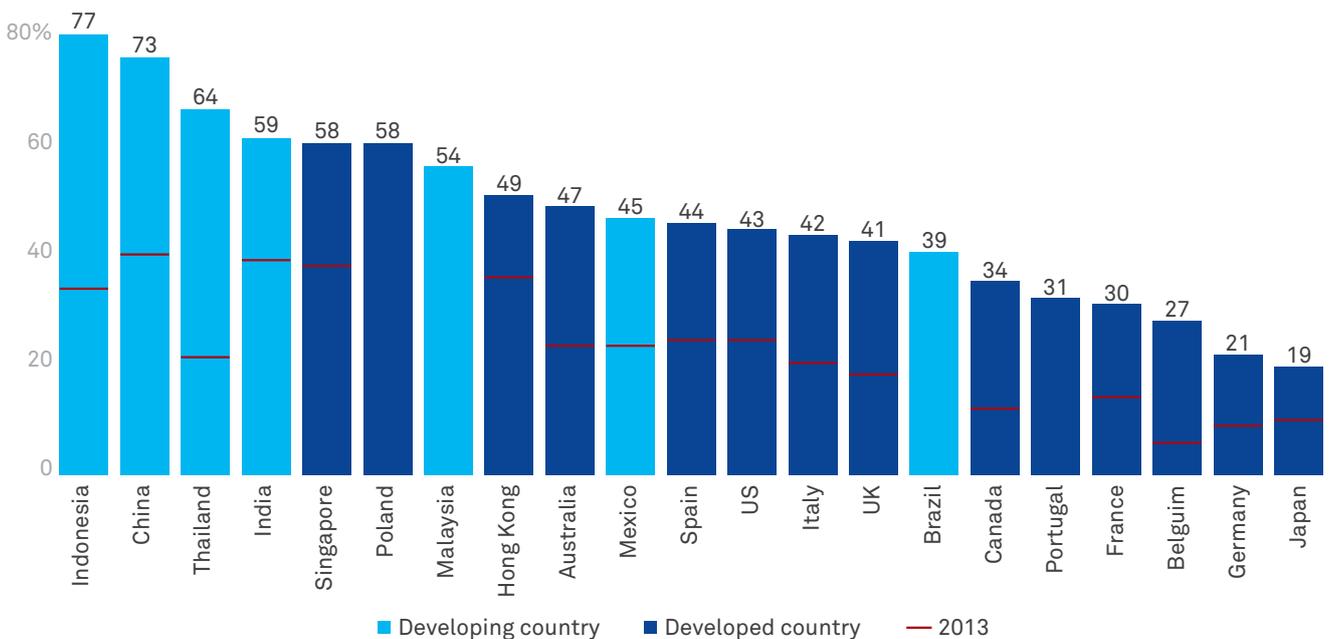
The significance of this development is eclipsed by the time it took to achieve. Bain & Company's report details a worldwide surge with 19 per cent year-on-year growth in consumers' use of mobile banking applications (see Figure 23).

Figure 22: Percentage of Total Interactions in Last Quarter, 2014



Source: Bain/Research Now NPS surveys, 2014

Figure 23: Percentage of Respondents Who Used Mobile Banking Apps in the Last Quarter



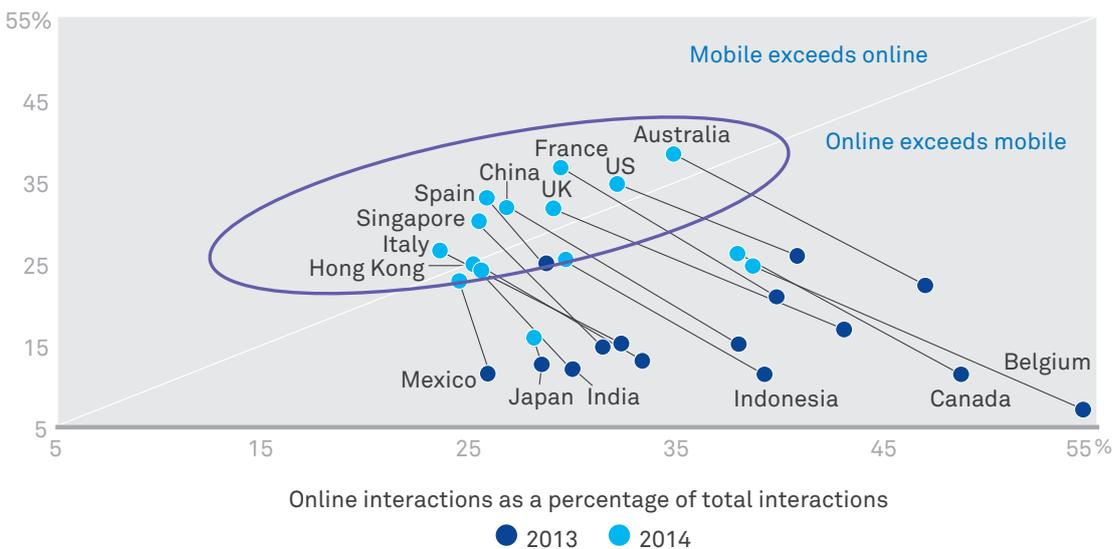
Source: Bain/Research Now NPS surveys, 2014

Mobile has also become a key enabler of socioeconomic development in developing nations, improving the financial inclusion of unbanked and under-banked communities and fuelling economic growth. This is illustrated by significant year-on-year growth in markets such as Indonesia, Thailand and India. Of the 2.5 billion people in lower and middle-income countries that are unbanked¹², one billion have access to a mobile phone¹³. At the end of 2014, there were more than 255 mobile money services in 89 countries; in nine of those markets, there are more mobile money accounts than bank accounts¹⁴. In their 2014 annual review, the Bill and Melinda Gates Foundation predicted, as one of their

top five bets, that by 2030, two billion people will be storing money and making payments on mobile devices (referring to the developments underway in unbanked and under-banked communities)¹⁵.

The rapid growth in mobile banking interactions reflects the unprecedented scale and pace of consumer behavioural change. There has been much commentary over the years on the shift from branch-based interactions to online (PC), but now we need to observe the shift from online to mobile paving the way for a new Mobile Pure Play era (see Figure 24).

Figure 24: Mobile Interactions as a Percentage of Total Interactions



Source: Bain/Research Now NPS surveys, 2014

2.0 FINANCIALLY MOBILISED OMNIPRESENT CONSUMERS

FUSION OF FINANCIAL SERVICES, MOBILITY AND IDENTITY (CONT.)



Mobile broadband is predicted to grow at a staggering CAGR of 15 per cent to 5.9 billion connections by 2020¹⁶ and this trend will only gain momentum through the coming years.

This behavioural change challenges traditional approaches to segmentation, as mobility increasingly influences consumers' expectations of interactions, engagements and experiences with financial services providers. Research reported by EY in its 2014 Global Consumer Banking Survey¹⁷ illustrates this point. The report highlighted eight global segments that represent shifting consumer sentiment. The 'Upwardly Mobiles' segment, while only representing six per cent of the population, has some very important characteristics, such as:

- Young (43 per cent 18 – 34 years, 37 per cent 35-49 years) and, highly educated (80 per cent college graduates) with high household incomes (median \$48,571) and the most significant investable assets of any segment (median \$250,000);
- Highest advocacy and trust (> 50 per cent);

- View banks as relatively undifferentiated compared with alternative providers (e.g. new type of bank);
- Own the most financial services products (mean products owned is 11.5);
- Most active in opening and closing accounts (71 per cent opening and 22 per cent closing accounts in past year; 34 per cent with alternatives to their primary provider);
- Most likely to experience problems requiring assistance, with great returns if resolution is highly satisfying;
- Value advice whether in person, on the phone, over video chat or via self-service; and,
- Use the mobile channel much more often per week than other seven segments (69 per cent).

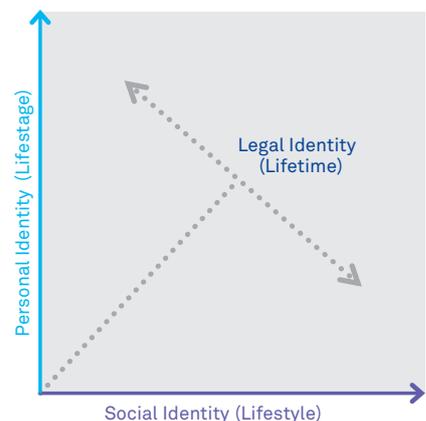
In light of this, it is hardly surprising that this important segment reported that 'keeping personal information safe' and 'protecting financial information' were the most important considerations in their relationship with their primary financial services provider (as also shown in Section 1, Figure 2).

2.2 The Confluence of Identity, Privacy and Security – this is now one conversation, not three

Identity, privacy and security have converged. Author David Birch¹⁸ highlights that traditional concepts of identity and money are changing due to the technological evolution of social and mobile networks, and that these will enable the creation of new infrastructure that can enhance both privacy and security. He further argues that identity is neither singular nor fixed and that a person's personal or social identity evolves and changes throughout a person's lifetime – unlike legal identity, which is mostly fixed.

Accordingly, we need to consider a flexible triage model for identity that adapts to the individual, interaction and institution (see figure 25). This is particularly important for those institutions taking a lifetime, life stage or lifestyle-based management approach. This model must take a long-term view of customer relationships and suggest we provide flexibility to accommodate evolving privacy needs throughout our lives. It must also foster trust.

Figure 25: Identity Triage Model (Lifetime, Lifestage, Lifestyle)



Source: Telstra Research 2015

The impact of identity theft on consumers (outlined in Section 1) explains the widespread data protection disclosure/notification standards and legislative initiatives underway. Recent developments in the US, Europe, Australia and Singapore indicate that regulators may impose reforms to obligate financial services institutions to implement revised security programs.

The Obama administration has urged lawmakers in the US to consider tightening cybersecurity at banks and other institutions, including mandatory public disclosure of any breach that compromised personal or financial information and notification of affected consumers within thirty days (Personal Data Notification and Protection Act).

In Europe, the European Union General Data Protection Regulation is expected to be completed in 2015. This will outline new requirements for firstly, issuing breach notifications to individuals and, secondly, conducting risk assessments and audits into how institutions handle personal information. These measures will be accompanied by proposed increased fines for non-compliance¹⁹.

In Asia, the Singaporean Personal Data Protection Act established new standards for the collection, use and disclosure of personal information. Non-compliance is subject to penalties up to USD\$788,955²⁰.

In Australia, the passing of reforms to the Privacy Act in 2014 have seen businesses face more onerous obligations when handling personal information, with penalties of up to AUD\$1.7million for a privacy breach. Privacy regulation remains a constant topic of public discussion, thanks largely to the introduction of local data retention laws and copyright regimes, as well as community concerns arising as a result of a series of large-scale hacks and data breaches. Further, in 2014 the Australian Law Reform Commission released its final report on serious invasions of privacy in the digital era. Recommendations included the introduction of a variety of new protections around the security of information, including the mandatory reporting of data breaches and the establishment of a civil case of action for privacy breaches.



2.0 FINANCIALLY MOBILISED OMNIPRESENT CONSUMERS

FUSION OF FINANCIAL SERVICES, MOBILITY AND IDENTITY (CONT.)

2.3 “Identity of Things”, “Privacy”, “Internet of Trust”

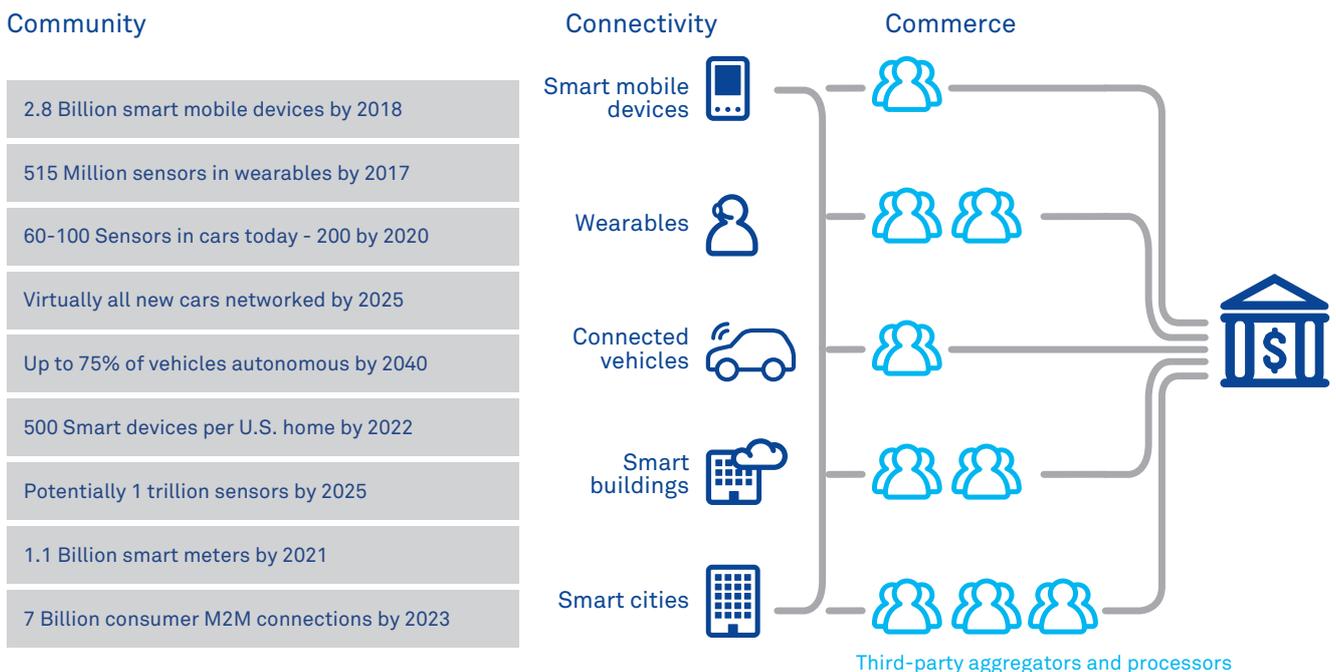
The mobile device revolution has made us completely rethink our approaches to identity and security. But before we’ve even adapted to the new mobile-enabled world, another potentially even more game-changing revolution is just beginning – the rise of the Internet of Things (IoT). In our previous report, “Analyse This, Predict That: How Institutions Compete and Win with Data Analytics”, we showed that the most adaptive and forward-thinking financial service organisations are already starting to shape the delivery of financial services based on big-data-style analysis of data from the Internet of Things. They are effectively becoming data-driven, software-defined businesses.

The sheer volume of data generated by the convergence of the mobility revolution and the Internet of Things is simply staggering. EMC predicts the amount of data in this “digital universe” will grow to 44 zettabytes (44 trillion gigabytes) by 2020²¹. The volume of data and the complexity of the IoT environment immediately creates security, identity and privacy challenges. IDC estimates that although 40 per cent of the data in the digital universe warrants some level of enhanced protection, less than 20 per cent actually has any such protection²². In fact, today many edge devices in the IoT are relatively unsophisticated devices with little inbuilt capability to protect either themselves or the data they produce from compromise. Essentially, we need robust and flexible mechanisms for establishing the “Identity of Things”. Today, the most common approaches involve the use of

verification and digital signing via Public Key Infrastructure (PKI). There is, however, no clear path for scaling well-managed PKI to the massive number of devices predicted in a mature IoT world.

It isn’t only data volume that increases the threat surface that must be managed. As Figure 26 depicts, the data that influences a single financial services decision can come from hundreds of devices and pass through numerous systems and platforms beyond the control of the financial institution or the customer. Our frame of reference for community, connectivity and commerce is predicted to exponentially explode, leading to a need for interconnected identity. Given that IDC predicts that over the next two years, 90 per cent of IT networks will have some form of security breach that is IoT-related²³, a key (as yet unanswered) question is:

Figure 26: Interconnected Identity



Source: Telstra Research 2015 – 24, 25, 26, 27, 28, 29, 30, 31, 32

“How do we ensure the integrity and confidentiality of data passing through a potentially complex chain of third parties?” This problem can also be conceptualised as: “How do we establish an Internet of Trust to support the Internet of Things?” Once again, there is currently no clear approach to developing the Internet of Trust, although the emergence of trust frameworks described in Section 4 may be an initial step on that journey.

Finally, from the perspective of the consumer, the IoT creates an unprecedented privacy challenge. If potentially thousands of sensors and devices are creating data that is used to shape the availability and delivery of financial services to me, how can I:

- i) Ensure the integrity of that data; and
- ii) Control what data regarding me is shared with other parties and how it can be used?

There are some emerging standards that deal with the problem of consent for sharing in a highly distributed world, for example, the UMA (User Managed Access) standard being developed by the Kantara Initiative³³.

Key Takeouts

1. The scale of growth in mobile services has directly translated into adoption of mobile banking application services. 2014 was the start of a new era in financial services, marking the first year where mobile devices became the preferred means by which consumers engage with their financial institutions.
2. With mobile broadband predicted to grow at a staggering CAGR of 15 per cent to 5.9 billion connections in 2020, we can anticipate the shift from online to mobile financial services to only gain momentum over the next few years, giving rise to the Mobile Pure Plays.
3. Identity is neither singular nor fixed and a person’s personal or social identity evolves and changes throughout their lifetime; unlike legal identity, which is mostly fixed. Therefore, we need to consider a flexible triage model for identity that accommodates a person’s lifetime, life stage or lifestyle.
4. Governments worldwide are responding to widespread data breaches. Data protection disclosure/notification standards and legislative developments in the USA, Europe, Australia and Singapore indicate that regulators may impose reforms to obligate financial services institutions to implement revised security programs.
5. Forward-thinking financial service institutions are already starting to shape the delivery of their financial services based on big-data-style analysis of data from the Internet of Things. They are effectively becoming data-driven, software-defined businesses.
6. The key unanswered question is: “How do we ensure the integrity and confidentiality of data passing through a potentially complex chain of third parties?” This problem can be conceptualised as “How do we establish an Internet of Trust to support the Internet of Things?”

3.0 MOBILE IDENTITY RESEARCH

FINANCIAL SERVICES EXECUTIVES AND FINANCIAL SERVICES CONSUMER RESEARCH

This section builds on the research and analysis presented in Section 1. Firstly, we gain an understanding from financial services executives of the current and future state of identity within their institutions. Secondly, through consumer research, we look to gain an understanding of how mobile and digital technologies have changed the ways Gen X and Y prefer to be identified and their attitudes toward a range of mobile identity services, their institutions and their associated business impact.

3.1 Methodology

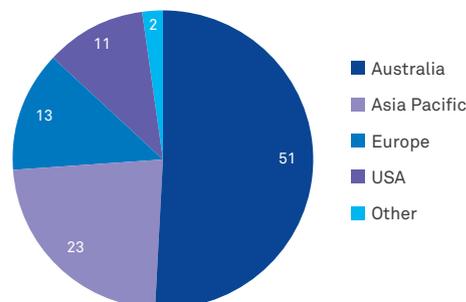
This section has two parts. In 3.2, we summarise the key findings from a quantitative study of financial institution executives conducted by Telstra between November 2014 and January 2015. By invitation, 318 executives from a cross section of financial services business types, roles and regions participated in a survey (see Table 5 and Figures 27 and 28).

Table 5: Participant Sample by Title & Role Function

Participant Titles	Participant Role Functions
Chief Executive Officers	Management
Chief Finance Officers	Product Management
Chief Information Officers	Information Technology
Chief Security Officers	Security
Chief Risk Officers	Risk Management
Chief Marketing Officers	Product Management
Executive General Managers	Finance
Presidents	Strategy
Executive Managers	Distribution
Managers	Marketing

Figure 27: Participant Sample by Geography

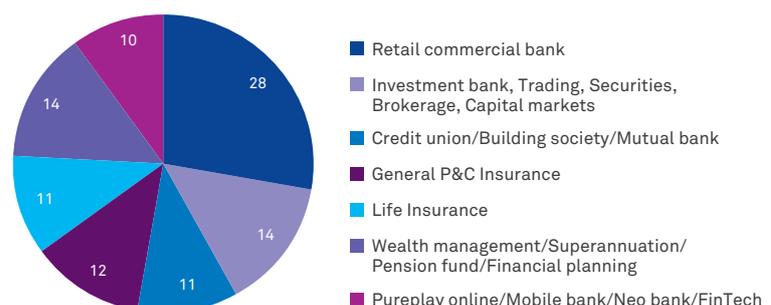
Select which geographic region your organisation is headquartered in



Source: Telstra Research 2015

Figure 28: Participant Sample by Business Type

Which activity best describes the primary business of your organisation?



Source: Telstra Research 2015

In Section 3.3, we present the key findings from a quantitative study, commissioned by Telstra, of consumers of financial services in seven countries: Australia, Singapore, Malaysia, Indonesia, Hong Kong, the United Kingdom and the United States of America. The objective of this research was to understand attitudes towards identity with current financial services institutions. Additionally, we wanted to gauge local perceptions to three mobile-based identity experiences and assess the potential impact of these on current behavioural patterns.

This study consisted of 4,272 surveys with a sample of consumers who have a financial product from a provided list, own a smartphone, have a mix of net worth levels and live in metropolitan areas. The online surveys were conducted from January to February 2015. The data set in each country was weighted to be representative of the total population, with an equal split of Gen X (1965-1979) and Gen Y (1980-1994), according to region, age and gender.

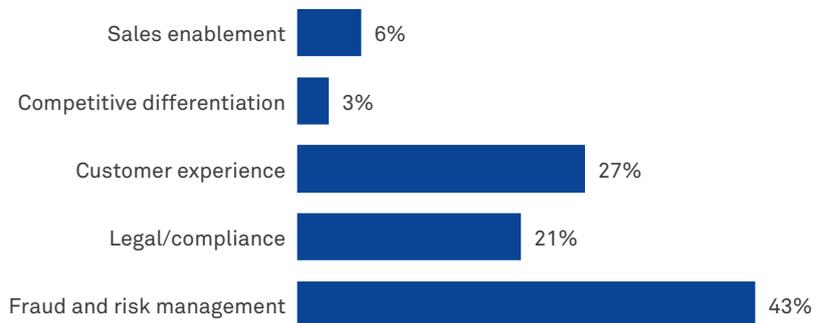
3.2 Financial Services Executive Study

The results from this study indicate that whilst financial institutions have under-invested, they are transitioning into a new phase of identity. However, disconnects remain with the expectations of their Gen X and Y customers.

3.2.1 Drivers of Existing Identity Systems and Processes

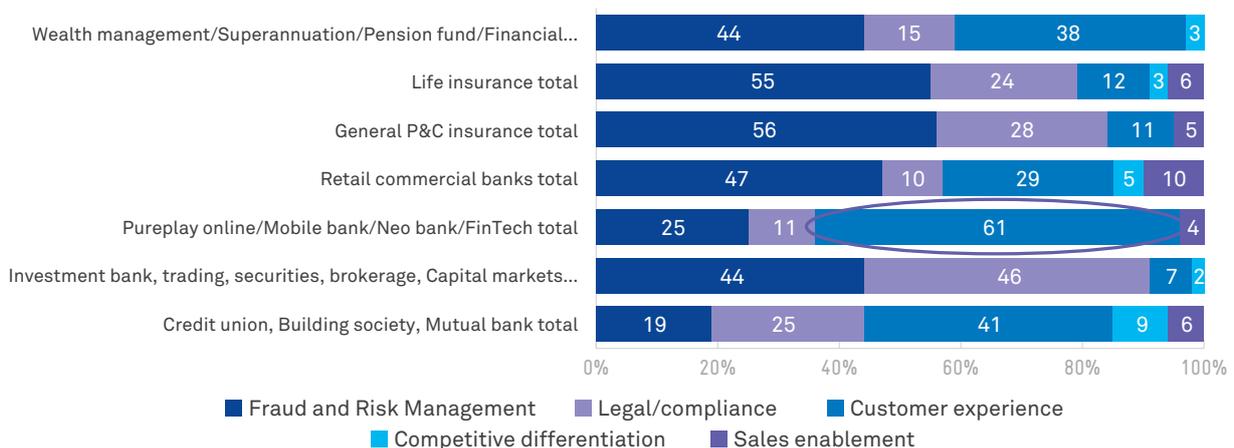
Across the industry and regions as a whole, Fraud and Risk Management has been the main driver for existing identity systems and processes (43 per cent), followed by Customer Experience (27 per cent) (see Figure 29). Interestingly, however, for Pure Play Online/Mobile Banks/Neo Banks/FinTechs, Customer Experience was ranked as the main driver (see Figure 30).

Figure 29: Business Drivers of Existing Identity Systems & Processes (Ranked 1)



Source: Telstra Research 2015

Figure 30: Most Important Driver of Existing Identity Systems & Processes by Business Type



Source: Telstra Research 2015

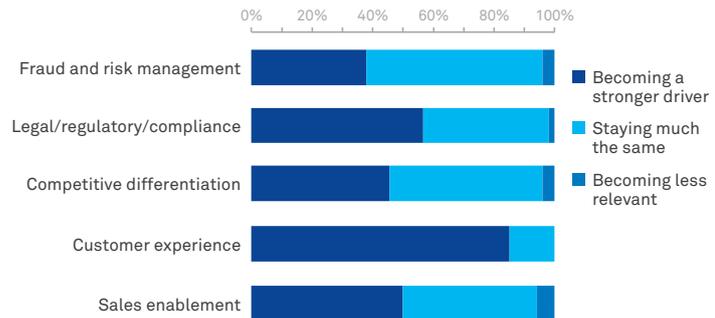
3.0 MOBILE IDENTITY RESEARCH

FINANCIAL SERVICES EXECUTIVES AND FINANCIAL SERVICES CONSUMER RESEARCH (CONT.)

3.2.2 Changes to Investments in Identity Systems and Processes

Moving forward, the customer experience emerges as the most important driver for investment in identity systems and processes right across the industry and region, with 87 per cent of respondents predicting that this will become a stronger driver (see Figure 31).

Figure 31: Anticipated Changes in Identity Systems & Processes (Total Institutions)

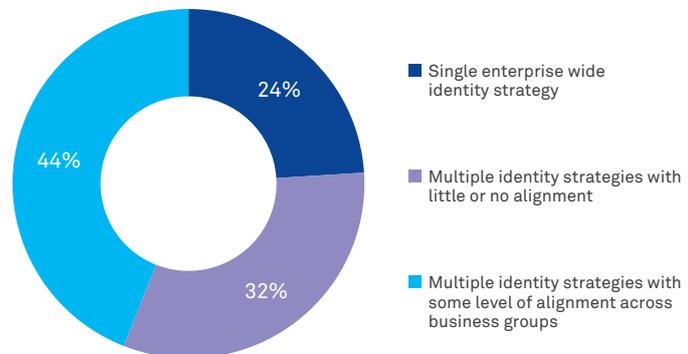


Source: Telstra Research 2015

3.2.3 Institution Identity Strategies and Responsibilities

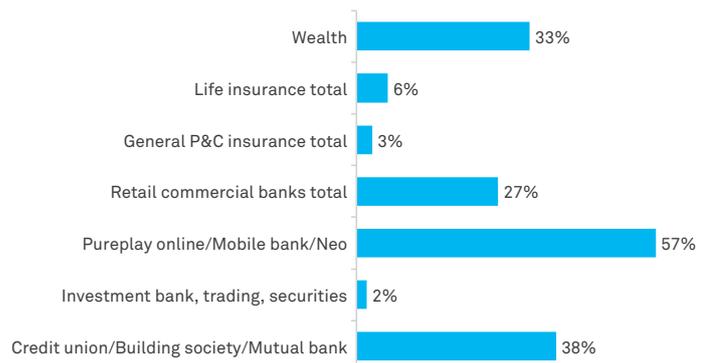
For many institutions, the pursuit of a single customer view and experience has been a strategic (but elusive) priority. Vertical integration strategies, acquisitions and operationally separated divisions and channel strategies have possibly hindered this pursuit. Not surprisingly therefore, 32 per cent of institutions reported multiple identity strategies with little to no alignment, and only 24 per cent report their institution as having a single enterprise-wide identity strategy (see Figure 32). This disconnect is particularly acute in the insurance and investment banking parts of the industry, with only 6 and 2 per cent respectively reporting single enterprise-wide identity strategies. The relatively new entrants in the form of Pure Play Online/Mobile Bank/Neo Banks/ FinTechs, perhaps unencumbered by legacy systems, lead the way with 57 per cent reporting a single enterprise-wide identity strategy (see Figure 33). These findings were consistent across all regions.

Figure 32: Single or Multiple Identity Strategies (Total Institutions)



Source: Telstra Research 2015

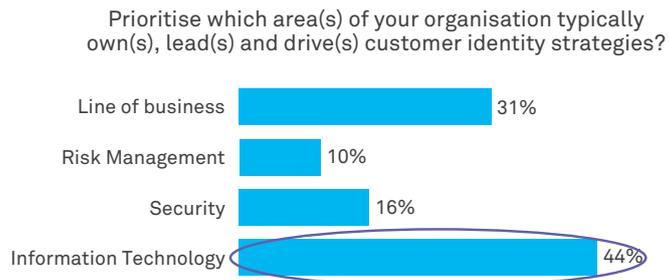
Figure 33: Single Enterprise-Wide Customer Identity Strategy by Business Type



Source: Telstra Research 2015

When it comes to responsibility for customer identity strategies, it's clear that the Information Technology function leads and drives the way (44 percent) (see Figure 34). This is more so for Investment Banks, Insurers and Wealth Management, but less so for Credit Unions, Pure Play Online and Retail Commercial Banks, where the line of business was reported as the main functional leader for customer identity strategies (see Figure 35). These findings were consistent across all regions.

Figure 34: Customer Identity Strategy Responsibility (Total Institutions)



Source: Telstra Research 2015

Figure 35: Customer Identity Strategy Responsibility (by Institutions)



Source: Telstra Research 2015



3.0 MOBILE IDENTITY RESEARCH

FINANCIAL SERVICES EXECUTIVES AND FINANCIAL SERVICES CONSUMER RESEARCH (CONT.)

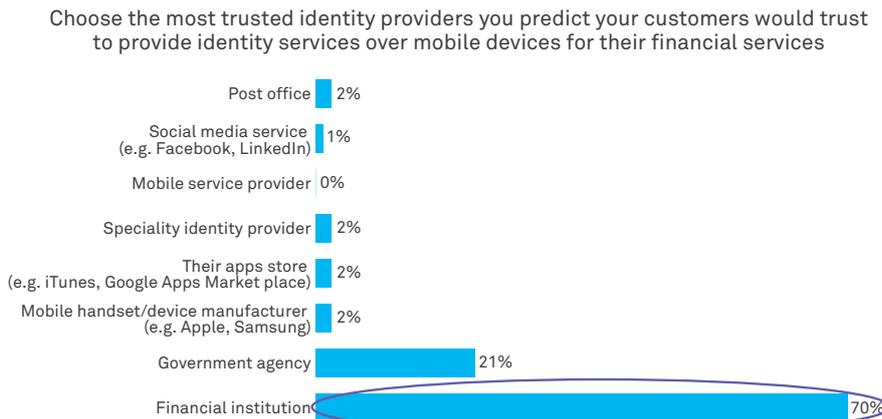
3.2.4 Trust and Third-Party Identity Providers

When it comes to the question of trust in identity providers, financial services executives in all regions and business types clearly view their institutions as being the most trusted (70 per cent), relative to other providers (see Figure 36). This reflects consumer perceptions, as our research detailed in Section 1.

According to Gartner, by 2020 60 per cent of all digital identities interacting with enterprises will come from external identity providers (up from 10 per cent in 2014)³⁴. With 16 per cent of institutions already allowing access from third-party identity providers and 48.6 per cent intending to (see Figure 37), caution will need to be exercised on the choice of identity services providers. Our research identified that consumers have clear preferences about who they trust to provide these services (see Table 1).

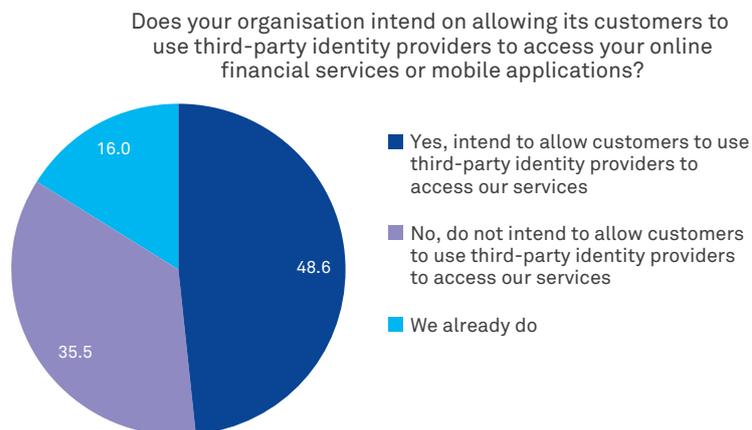
Regardless of whether financial service organisations seek to become consumers of external identity service providers, become external identity providers themselves or both, if they are to maintain their current position of trust in the eyes of consumers, strong and coherent identity management capability will be critical.

Figure 36: Trust in Identity Service Provider (Total Institutions)



Source: Telstra Research 2015

Figure 37: Third-Party Identity Service Provider (Total Institutions)



Source: Telstra Research 2015

3.3 Mobile Identity Consumer Study

Gen X and Y consumers across Australia, Singapore, Malaysia, Indonesia, Hong Kong, the UK and the US were asked to evaluate three mobile authentication methods. The methods were shown to respondents in a random sequential order in order to ensure a reliable analysis of all concepts. Descriptions of each concept are provided in 3.3.1.

3.3.1 Authentication Method Descriptions

Three authentication concept authentication methods were tested during the survey, described to respondents as follows:

<p>CONCEPT A</p>	<p>Federated Identity</p> <p>A single set of personal credentials registered with, for example, a bank, mobile operator or independent identity provider, to be used across multiple financial services websites in a one-click process, rather than having to register and remember credentials for each</p>
<p>CONCEPT B</p>	<p>Second Factor Authentication</p> <p>A code sent to your mobile is used as a second factor overlay for more secure access to your account, which you enter when you log in, to boost security of online transactions</p>
<p>CONCEPT C</p>	<p>Mobile Digital Signature</p> <p>The ability to safely, reliably and securely “sign” or commit to financial services documents, loan agreements etc. using your mobile device, for example swiping a secret gesture, signing with either your finger or a stylus, or entering a PIN or passcode</p>

We do note that across almost all aspects of all concepts, Indonesian respondents gave the highest rankings. This may reflect a genuine unmet demand for any form of

advanced identity management for financial services consumption in Indonesia, or it may reflect a cultural bias with regard to how Indonesians respond to such research.

3.5 Second Factor Authentication

CONCEPT

B

Second Factor Authentication

A code sent to your mobile is used as a second factor overlay for more secure access to your account, which you enter when you log in, to boost security of online transactions

For those who find this concept appealing and indicate that they are likely to use it should it be offered, the impact is significant across a number of areas, including improved satisfaction with the institution, increased likelihood of retention and increased potential for acquisition. Satisfaction, retention and acquisition are particularly strong in Indonesia and Malaysia (see Table 8).

Table 8: Second Factor Authentication (by Country)

Scorecard	Australia	Hong Kong	Indonesia	Malaysia	Singapore	UK	USA
Appeal	63	54	77	78	70	59	58
Likelihood to use	61	55	78	77	72	56	56
Appeal and likely to use concept	57	45	74	73	65	53	51
Of those who find the concept appealing and are likely to use							
More satisfied with their financial provider	86	88	97	95	93	91	85
More likely to recommend provider	57	33	69	58	60	57	58
More likely to consider provider when taking up new product/service	79	84	93	91	83	81	78
More likely to consider provider when switching accounts/ services	76	75	88	91	80	79	75

Source: Telstra Research 2015

Similarly, two-factor authentication has a positive impact on consumer attitudes to the security of their account. In particular, it provided reassurance that they would be the only ones able to access their account and that fraudulent access would be reduced.

Australia (82 per cent agree) and the USA (81 per cent) are the countries happiest to share information such as their mobile number with financial institutions as a basis for two-factor authentication, while consumers in Hong Kong are potentially more hesitant, with only 59 per cent agreeing (see Table 9).

Table 9: Sharing Mobile Number with Financial Institution (by Country)

"Strongly agree/agree"	Australia	Hong Kong	Indonesia	Malaysia	Singapore	UK	USA
I would feel more secure knowing only I can access my information	89	78	84	88	86	86	88
There would be less threat of fraudulent use of my information	88	78	80	81	83	80	86
It will make accessing my information a lot faster	54	43	72	62	58	59	49
It will make accessing my information a lot more convenient	61	46	81	63	60	64	54
I would feel comfortable sharing this information with my banks or financial institutions	82	59	79	70	70	73	81

Source: Telstra Research 2015

3.0 MOBILE IDENTITY RESEARCH

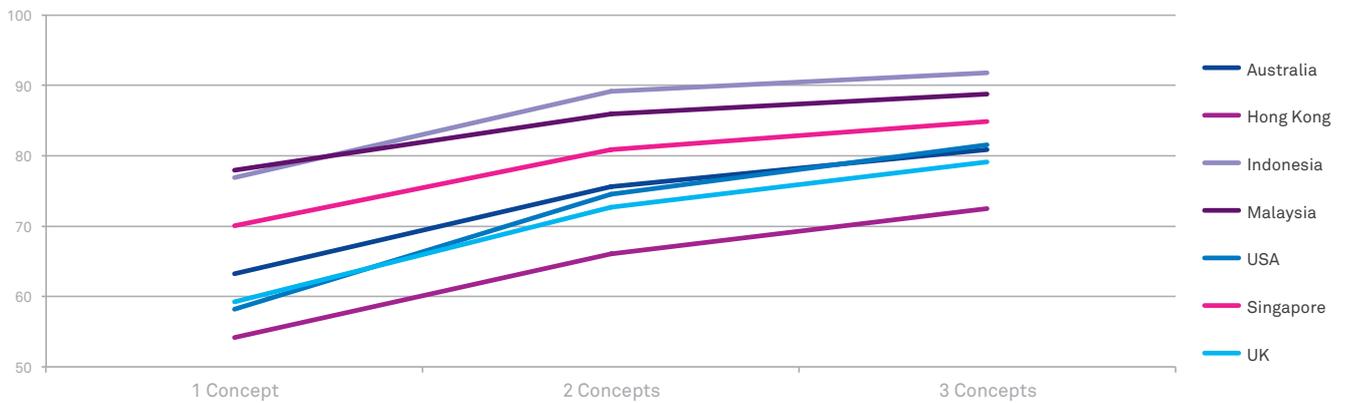
FINANCIAL SERVICES EXECUTIVES AND FINANCIAL SERVICES CONSUMER RESEARCH (CONT.)

3.7 Incremental appeal of authentication methods

So should financial institutions stake their bet on one or more of the authentication solutions tested: Federated Identity, Second Factor Authentication or Mobile Digital Signature? The answer is yes, at least one, but offering consumers choice could achieve even greater impact.

Analysis was conducted to assess the optimal number and combination of concepts that would reach the largest number of consumers who would find at least one of the concepts appealing (see Figure 41).

Figure 41: Incremental Appeal of Authentication Methods (by Country)



Source: Telstra Research 2015

In Indonesia and Malaysia, incremental appeal beyond two concepts is limited, but in all other markets there is benefit to be gained in offering all three concepts.

Offering consumers a choice of methods would ensure that the majority use at least one of them when accessing their financial accounts (see Table 11).

Table 11: Incremental Appeal of Authentication Methods (by Country)

Concept combinations (based on three concepts)	Australia	Hong Kong	Indonesia	Malaysia	Singapore	UK	USA
1 Concept	B 63	B 54	B 77	B 78	B 70	B 59	B 58
2 Concepts	BC 76	BC 66	BC 89	BC 86	BA 81	BA 73	BC 75
3 Concepts	BCA 81	BCA 73	BCA 92	BCA 89	BAC 85	BAC 79	BCA 82

A = Federated Identity; B = Second Factor Authentication; C = Digital Mobile Signature

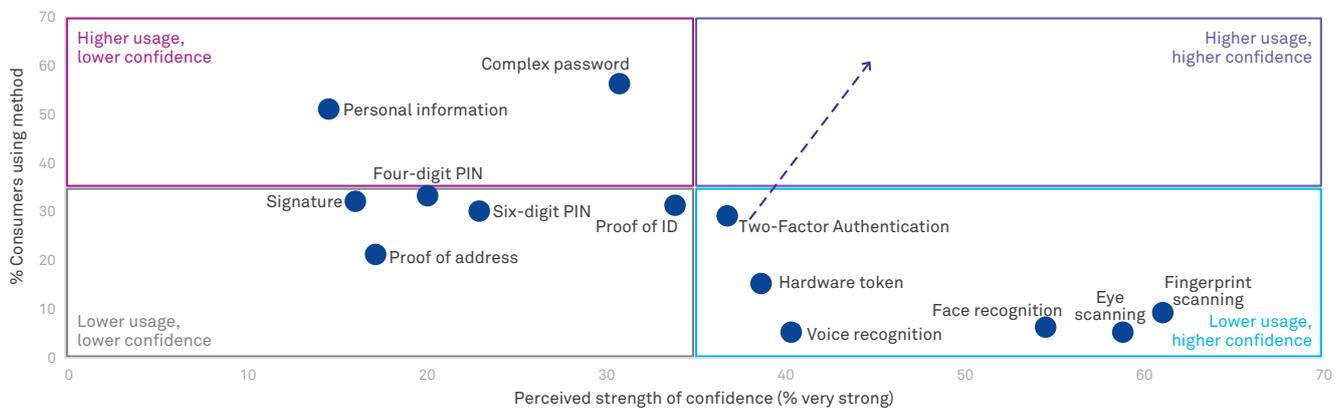
Source: Telstra Research 2015

If we look at which combination of two concepts would maximise appeal, in Australia, Hong Kong, Indonesia, Malaysia and the US, Two-Factor Authentication plus Mobile Digital Signature yield most appeal. Meanwhile, in Singapore and the UK, it is a combination of two-factor authentication plus Federated Identity.

Two Factor Authentication provides the 'easiest win' for financial institutions right now as it is already a known entity for most, is used by many consumers (one in five) and has a high level of perceived security. Referring back to the matrix presented in Figure 2, it provides the best opportunity to move one of the

authentication methods into the top right box – highly used and very secure. Further education on the security of the approach could also increase that perception, making it an ideal solution to implement in the short term (see Figure 42).

Figure 42: Usage & Perceived Strength of Authentication Method (Global)



Source: Telstra Research 2015

Key Takeouts

1. Financial services executives predict that the customer experience will become a much stronger driver (87 per cent) in their institution's identity systems and processes, and are anticipating significantly increasing investments in this area (87 per cent). However this won't be at the expense of fraud and risk management – 38 per cent of executives report this as a strong driver for their institutions.
2. A lack of a single customer view perhaps explains why only 24 per cent of financial services executives report that their institutions have a single enterprise-wide identity strategy. This is particularly so for Investment Banks, General and Life Insurers (<6 per cent).
3. Whilst financial services executives perceive their institutions as being the most trusted (70 per cent), most either already do (16 per cent) or intend to allow customers to access them using third-party identity providers (48.6 per cent).
4. Mobile identity-based solutions are highly appealing to consumers and, if offered, would likely result in improving customer satisfaction and advocacy. Importantly, they would also likely result in acquisition or reduced likelihood of defection.
5. For Federated Identity, institutions will need to carefully select their identity providers in order for consumers to trust that their personal information is safe and secure.
6. The combination of concepts that would maximise appeal is Second Factor Authentication and Mobile Digital Signatures across most countries studied.
7. Second Factor Authentication has the highest appeal for consumers – increasing its usage will likely result in the easiest win in terms of enhancing levels of trust and security, but more education is required for biometrics.

4.0 MOBILE IDENTITY TECHNOLOGY FOR THE INTERCONNECTED FINANCIAL SERVICES INSTITUTION

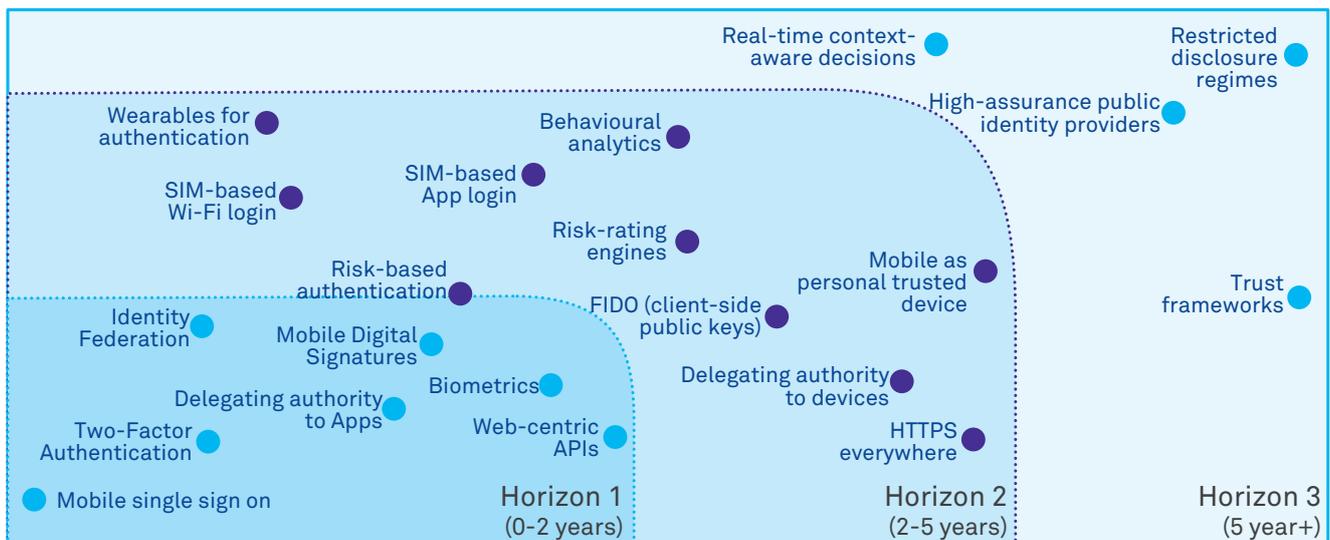
We now bring together the insights from previous sections to describe the technology environment and key developments for each of the identity concepts we researched. Finally, we then present a vision for a secure, intelligent, omnipresent identity institution.

4.1 Identity Technology Key Developments and Roadmap

We have seen from Figure 31 that customer experience will become a much stronger driver in terms of the investments made by institutions. This reflects a trend toward simplifying identity access management – in other words, reducing the friction associated with identity for consumers, and there is a corresponding focus on the enabling technologies. We can see that the three concepts (Federated Identity,

Two-Factor Authentication and Mobile Digital Signature) tested in this research are anticipated to reach the mainstream within the next two years. What our research further found was that consumers perceive biometrics technologies as providing stronger identity and security, but much work is yet to be done to increase uptake, as is reflected by the low levels of consumers using this method today. We predict these technologies will become mainstream within the next two years (see Figure 43).

Figure 43: Identity Technology Roadmap



Source: Telstra Research 2015

Horizon 1

- **Delegating Authority to Applications:** Explicitly asking the consumer to grant rights to an application to access or share confidential data (for example, authorising a smartphone app to access your contact list).
- **Identity Federation:** An institution accepts evidence of a consumer's identity from other organisations that the consumer has an existing relationship with (for example, logging into a new website using an existing Twitter, Google or Microsoft account).
- **Mobile Single Sign On:** Consumers use their mobile number to securely access applications such as the GSMA's Mobile Connect initiative.
- **Two-Factor Authentication:** Using two different identity factors (for example, "something I know" and "something I have") simultaneously to provide stronger evidence of identity.
- **Biometrics:** Using voice, iris, facial, fingerprint or other human credential to access applications.
- **Mobile Digital Signature:** A broad category of technologies utilising PKI, enabling consumers to execute legally binding documents.
- **Web-Centric APIs:** Various internet companies and Pure Play identity providers have provided cloud-based identity and access management services targeting web and mobile applications for quite some time – for example via RESTful APIs. However, the last couple of years have seen some "higher trust" organisations such as communication service providers beginning to offer similar services. For example, AT&T and Verizon in the US both provide mobile identity services APIs, although with very different approaches³⁶ (see also Case Study 1).

Horizon 2

- **Behavioural Analytics:** Observing patterns of behaviour and comparing them with our expectations of a consumer, based on previous interactions or existing population models.
- **Delegating Authority to Devices:** Explicitly asking the consumer to grant rights to a particular device to access or share confidential information (for example, authorising a vehicle's telemetry system to share location and data relating to driving behaviour with an insurer).
- **FIDO (client-side public keys):** The FIDO Alliance defines a mechanism whereby a consumer has a device or service that can generate and securely store new public/private cryptographic key pairs, which can be used for signing or authentication. This means a single consumer hardware device can act as an authentication factor for many services, while ensuring service providers do not have access to keys used with other providers.
- **HTTPS Everywhere:** Means the point where effectively all web-based interactions that may contain or expose confidential information use the encrypted HTTPS protocol rather than unencrypted HTTP.
- **Mobile as Personal Trusted Device:** A Personal Trusted Device (PTD) is a device that is always present with or in the control of a consumer that they trust to be sufficiently secure to be their primary means of securing, accessing and controlling sensitive information. "Mobile as personal trusted device" refers to the point in time where the majority of active consumers see their mobile device in this way.
- **Risk-based Authentication:** Using a wide range of identity and risk factors to make prior decisions about when to challenge a particular user to authenticate their identity in a particular way.
- **Risk-rating Engines:** The widespread availability of largely cloud-based services that aggregate and analyse a range of data from various sources to help establish the risk associated with a current interaction (for example, providing a reputational score for a given mobile number or social platform identity).
- **SIM-based App Login:** Using the mobile device SIM (and the secure, high-assurance relationship it establishes with a communication service provider) as the basis of authentication for mobile applications.
- **SIM-based Wi-Fi Login:** Adoption of publicly available Wi-Fi has been significantly impeded by perceived insecurities in the way Wi-Fi networks and mobile devices identify and authenticate with each other. SIM-based Wi-Fi login technologies such as HotSpot 2.0 are now being deployed – these use the mobile device's SIM to allow devices and networks to discover each other and authenticate in secure and convenient way.
- **Wearables for Authentication:** Wearable devices (such as smartwatches or fitness trackers) can be used as part of the authentication process. For example, an NFC-equipped smartwatch containing credentials can be swiped past an NFC reader or a fitness tracker can provide biometric evidence of identity.

4.0 MOBILE IDENTITY TECHNOLOGY FOR THE INTERCONNECTED FINANCIAL SERVICES INSTITUTION (CONT.)

Horizon 3

- **High-Assurance Public Identity Providers:** 'High Assurance Public Identity Providers' (IDPs) are service providers who create digital identities for individuals. These entities can be relied upon for high assurance-based interactions or transactions such as those required by financial institutions. This development creates two opportunities for institutions. Firstly, as institutions are an identity issuer, they could commercialise the identity assets inherent within the institution – thus becoming an IDP and creating a new revenue-generating set of services. Or secondly, as institutions are also relying parties, using third-party IDPs and thus reducing the costs required to support these internal functions. Gartner predict that by 2020, 60 per cent of all digital identities interacting with enterprises will come from external identity providers, up from less than 10 per cent today³⁷.
- **Real-time Context-Aware Decisioning:** Analysing a wide array of data to make decisions regarding a particular interaction in real-time – for example, making decisions in real-time about whether to explicitly challenge a given consumer to authenticate themselves in a particular way during a particular transaction.
- **Restricted Disclosure Regimes:** An umbrella term for technology-enabled architectures and protocols that allow consumers to share with another party, in a securely encrypted manner, only the minimum required relevant personal information to complete an interaction or transaction. These may ultimately help provide greater protection to consumers required to provide more trustworthy personal information to service providers.
- **Trust Frameworks:** These are sets of specifications and accompanying certification programs that codify the trust relationships between identity providers and service providers, enabling them to trust each other's respective identity, security and privacy policies.

Case Study 1 Payfone – Identity Tokenisation

Payfone announced a pilot of its product called Identity Certainty with three financial institutions in 2015 through a partnership with fraud protection and risk management company, Early Warning. Early Warning is owned by the Bank of America, BB&T, Capital One, Chase and Wells Fargo.

Through its partnerships with four major US mobile operators, Payfone already has 300 million mobile identities in its databases. The pilot will include an additional layer of protection for banks to confirm a mobile banking customer's identity when logging into the service. Payfone assigns each identity a unique tokenised ID that is based on a mobile subscriber's phone number, SIM card and account number. Banks will then correlate those to their records.

4.2 Authentication in an Interconnected Financial Services World

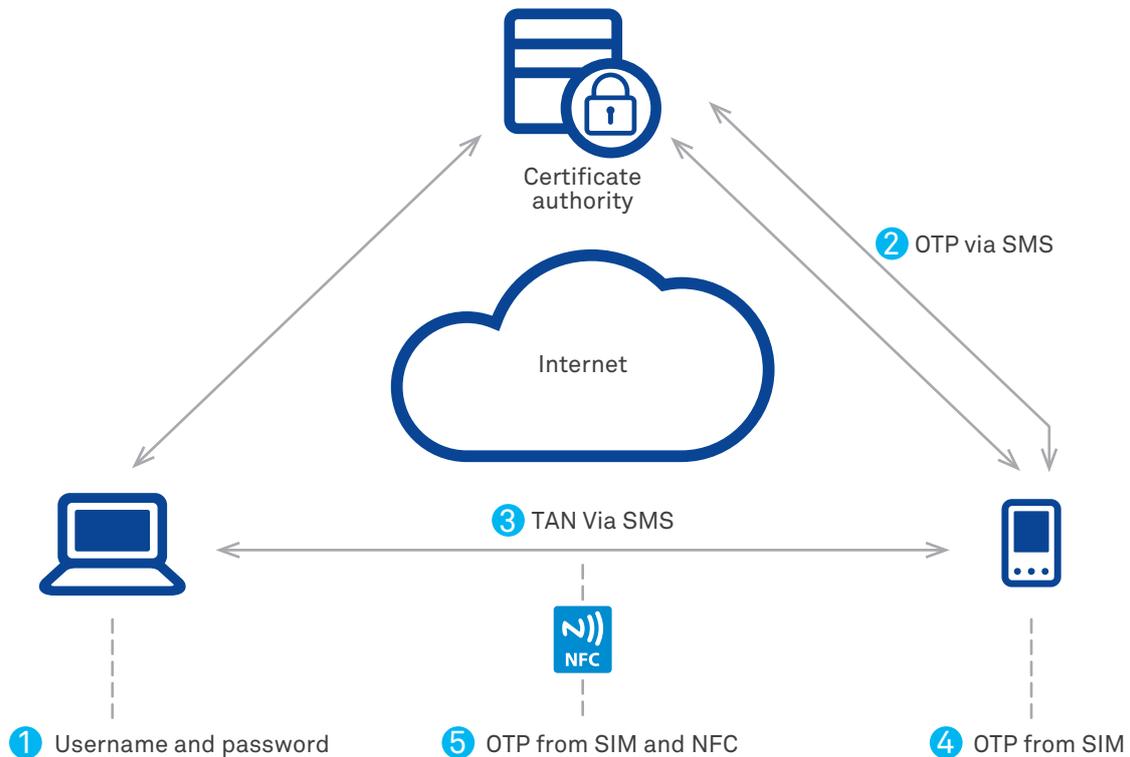
Authentication Tokenisation – Tokenisation of personal information is a major advancement, limiting the exposure of consumers and institutions. When used with one-time passwords (OTP) or out of band authentication – both of which are gaining much greater penetration with smartphones and other mobile devices, as these are now the primary access method for financial

services – they provide a much better user experience compared with hardware-based tokens. Our research found that hardware tokens are not as commonly used as two-factor authentication methods.

The authentication market is highly fragmented, and inconsistent both across and within institutions. At one end of the spectrum, we have ‘unmanaged’ soft credentials such as usernames, passwords and PINs (Something That I Know) (see 1 in Figure 44 below). Next we have

much stronger multifactor methods such as One-Time-Passwords (OTP) (Something That I Know) + OTP via SMS on mobile (Something That I Have) (see 2 and 3 in Figure 44 below). From there, we have ‘managed’ soft credentials such as software certificates. We also have credentials derived online; for example, secure cloud-based server and also derived credentials on Universal Circuit Card (UICC) (Something That I Know) + OTP, generated on SIM and transferred via phone or PC using a NFC reader (see 4 and 5 in Figure 44 below).

Figure 44: Second Factor Authentication Methodologies



4.0 MOBILE IDENTITY TECHNOLOGY FOR THE INTERCONNECTED FINANCIAL SERVICES INSTITUTION (CONT.)

The financial services sector is seen as the biggest driver for the multifactor authentication market, which is expected to reach USD \$5.45 billion by 2017³⁸. Many institutions increase security through the use of One Time Password (OTPs). These are single-use codes (often numbers) sent via an independent channel such as SMS or via an app on a mobile device and manually entered by the user. An intercepted OTP can only be used to compromise one interaction. OTPs are a useful way to increase security. Both VISA and MasterCard have been working on a new authentication standard '3DS 2.0'. This standard will utilise richer cardholder data and result in fewer password interruptions at the point of sale. Should an authentication challenge be required, card (or phone) holders will be able to identify themselves with OTP or fingerprint biometrics.

The popularity of highly-capable mobile devices replete with sensors, interfaces and services coupled with pervasive high-speed wireless connectivity offer a range of options for additional authentication factors. Most mobile devices can determine their location and report it to authorised applications or organisations. This can be used to help secure location-centric interactions such as device-present mobile payments. Although simple in concept, there are various subtleties associated with using the mobile device as a location-based factor in authentication:

- Some approaches require yet another separate app to be installed on the device, introducing extra complexity for on-boarding and creating potential compatibility and maintenance issues;

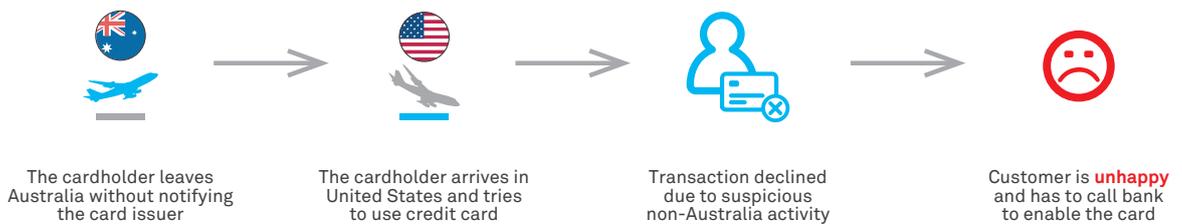
- Some solutions demand international data roaming or Wi-Fi to be enabled. The cost of data roaming is a sensitive issue for many travellers and may limit uptake;
- The customer experience of some approaches is sub-optimal. For example, lacking the ability to proactively notify customers that their card is approved for use in that country may mean a customer misses out on a "top of wallet" opportunity; and
- Constant monitoring of a traveller's location maybe viewed as excessive use of personal information.

Case Study 2: TeleSign Push Roaming Traveller Notification Solution

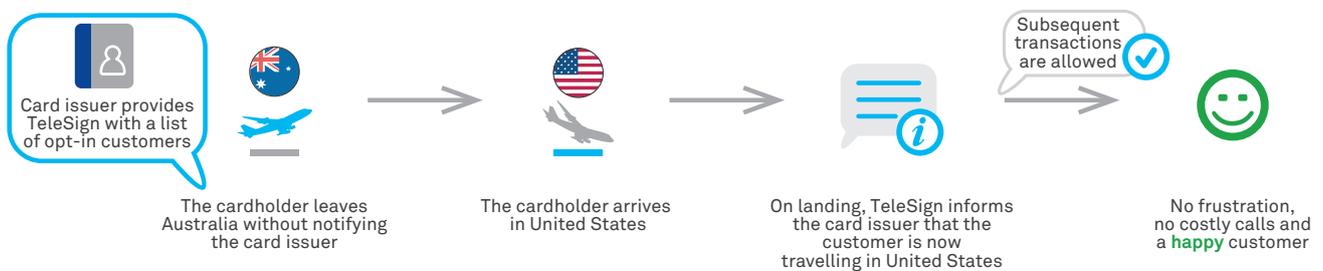
TeleSign and Telstra are working with financial institutions on an SMS-based Traveller Notification solution utilising the mobile roaming networks. This solution will enable a bank's customer to opt into a messaging service advising the bank of their international travel location. This reduces the cost and friction associated with pre-travel interactions, reduces exposure to risk and fraud for all parties, and delivers a great mobile-based banking experience for the customer.



Travelling Today



Travelling Tomorrow



Apart from location, a mobile device's accelerometers can be used to determine proximity to another device – for example, by observing the vibration of the two devices being touched together. Device cameras can be used to capture images – for example, a unique QR-code displayed on point-of-sale terminal. Short-range wireless communication technologies such as Bluetooth, NFC and even Wi-Fi can be used to prove proximity to a particular location or device (such as a payment terminal) and can be used to exchange credentials or other information with other devices.

Mobile devices are also driving a resurgence in interest in the use of biometrics (measuring some characteristic of the human body) for convenient authentication. There are numerous approaches using voice, retinal scanning, facial recognition, blood vessel scanning, fingerprint scanning, and many more esoteric forms of biometrics. High-end mobile handsets and operating systems from Apple, Samsung, HTC and Huawei now incorporate fingerprint scanning. Biometric authentication is nothing new to financial services institutions – for example, National Australia Bank with Telstra piloted voice biometrics over its telephone banking channel in 2009, which has been subsequently deployed. However, mobile devices offer scope for much wider deployment of biometrics and other technologies (see Case Studies 3, 4 and 5).

4.0 MOBILE IDENTITY TECHNOLOGY FOR THE INTERCONNECTED FINANCIAL SERVICES INSTITUTION (CONT.)

Case Study 3: USAA – Facial and Voice Biometrics³⁹

In a claimed industry first for America, USAA, the San Antonio-based financial services company, announced the deployment of facial and voice recognition technology across its entire membership base (10.7 million members, four million of whom use the mobile banking app).

Improvements in biometric technology over many years have reduced false negatives and friction associated with facial recognition, taking approximately two seconds for facial recognition, but up to 20 seconds for voice recognition. An impressive four out of five end customers who have experienced the technology, prefer it above use of a PIN, with 10 per cent of customers adopting the technology so far.

To avoid impersonation (facial or vocal), USAA's device identification technology provides additional security. Once a member logs in, an encrypted token is sent from the member's device to USAA, which is matched against the ID of the device registered at enrolment.

USAA report that 94 per cent of its members' biometric logins are successful on the first attempt and 100 per cent on subsequent attempts.

Case Study 4: Westpac – Fingerprint Biometrics⁴⁰

In what was reported to be a world first, Westpac Banking Corporation of Australia announced that from January 2015, users with Samsung Galaxy S5 and Note 4 smartphones can use the fingerprint sensor on their device to securely sign into the bank's digital banking platform. This capability is also available on the iPhone 5S, iPhone 6 and iPhone 6 Plus.

The bank claimed this would enhance security and convenience for customers accessing the bank on their smartphones. Westpac's executives report that over half of their three million digitally active customers are using mobile banking, and that the bank is now processing more than AUD\$50 billion worth of transactions each year.

Case Study 5: Royal Banking Of Canada, Halifax – Electrocardiogram (ECG) Authentication⁴¹

Royal Bank of Canada, Halifax and other issuing banks have been reported to be trialling ECG technology that communicates their identity through an embedded sensor which recognises the wearer's unique ECG to their wearable devices using Bluetooth. Once activated, customers can make payments with a simple tap of their wrists.

Halifax is testing the use of this technology for logging onto online banking, alleviating the need for consumers to use PINs or other security details.

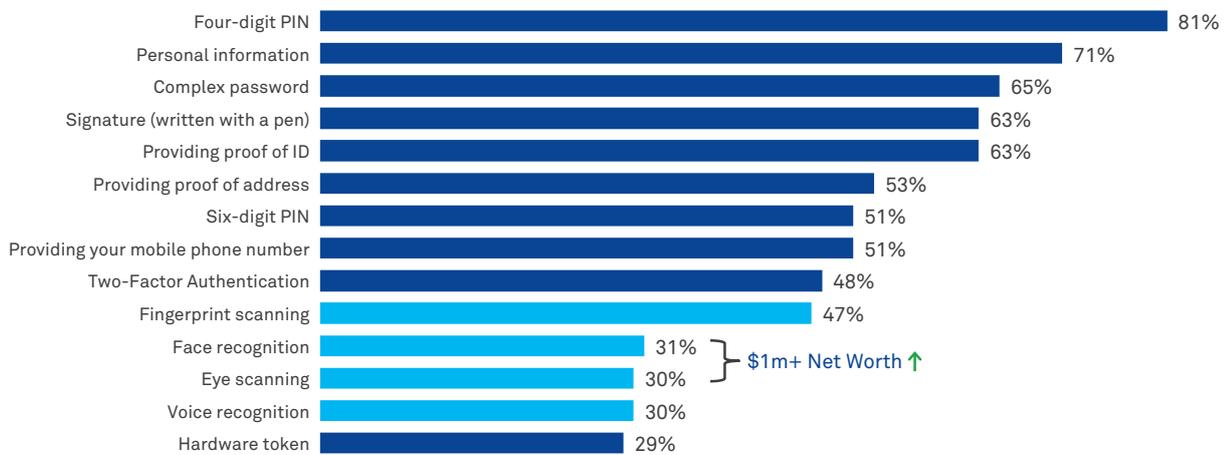


Fingerprint scanning has the highest levels of awareness of all biometric identity methods, no doubt aided by its deployment on major smartphone

platforms of late. Face recognition and eye scanning have the highest levels of awareness amongst those with a net worth of more than US\$1

million, although only 38 per cent of them are aware of eye scanning and 37 per cent are aware of facial recognition (see Figure 45).

Figure 45: Authentication Methods Awareness



Source: B1: Which of the following identity authentication methods are you aware of?

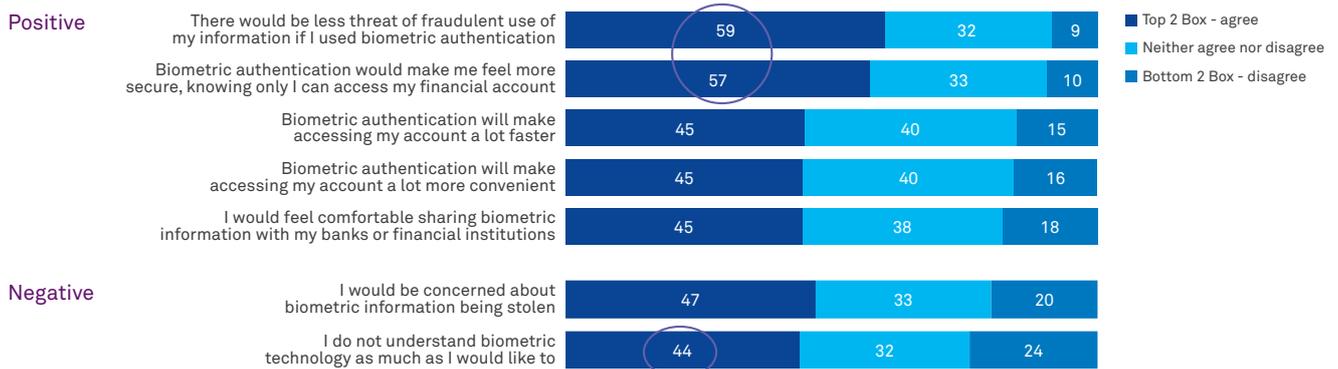
Source: Telstra Research 2015

Awareness of biometric solutions is similarly low across all countries we surveyed, with the highest levels of awareness in the US and Australia: Fingerprint scanning (US 50 per cent), Face recognition (Australia 34 per cent), and Eye scanning (USA 32 per cent) and Voice recognition (USA/Australia 33 per cent).

Alongside low levels of awareness, many consumers are still unclear about the benefits that biometric authentication would provide. The clearest benefits are that biometrics would help reduce the threat of fraudulent use (59 per cent agree) and help consumers feel more secure that only they could access the

account (57 per cent agree). However, 44 per cent of consumers also feel that they do not understand biometric technology as much as they would like to (44 per cent agree), pointing to the need for greater consumer education alongside technological development (see Figure 46).

Figure 46: Perceptions of Biometrics for Authentication



Source: Telstra Research 2015

4.0 MOBILE IDENTITY TECHNOLOGY FOR THE INTERCONNECTED FINANCIAL SERVICES INSTITUTION (CONT.)

4.3 Federated Identity in a Interconnected Financial Services World

Federated Identity management technologies allow consumers to sign into a range of service providers using a single set of credentials. As we saw from our research, only one in four (24 per cent) of institutions today have a single enterprise-wide identity strategy. We further found that 65 per cent of institutions either already, or intend to, allow access using third-party identity providers. Whilst Gartner's prediction that by 2015, 50 per cent of bank mobile apps will be accessed using partly or entirely proprietary device authentication systems rather than bank

authentication systems⁴² may have been ambitious, we expect that with the widespread adoption of mobile banking, social banking and cloud-delivered technologies; Federated Identity services will become more mainstream.

The fact that most institutions have many options available for authentication introduces a problem for customers – they must authenticate themselves in many different ways using different credentials for different service providers. This often results in compromises such as reuse of usernames and passwords and the use of password managers (cloud-based or device-based databases

of a given user's credentials). One approach to simplify life for users is Federated Identity. In a Federated Identity environment, providers of services to customers (such as financial service institutions) rely on selected third parties (known as identity providers or IdPs) to authenticate users. Our research in section 3 illustrated how 16 per cent of financial institutions already allow third-party IdPs, with 48.6 per cent of institutions planning to do so in the future. Examples include when online services offer users the options to "Log in with Facebook, Google or Twitter" or when a university allows students to log in using credentials from another institution in which they are enrolled (see Figure 47).

Figure 47: Federated Identity



Source: Telstra Research 2015

Identity Federation has benefits beyond reducing the number of credentials a user needs. Customer enrolment is simplified since a customer can exploit an existing relationship with an employer, a university, or their favourite Internet behemoth to access a broader range of services (as exemplified

in Case Study 6). Federation can allow institutions to effectively offload many aspects of the often problematic management of user credentials in-house. As our research in Section 3 highlighted, Federated Identity appealed to one in two consumers.

Case Study 6: Social Banking

Billions of people around the world have now incorporated social media in their personal and professional lives. Facebook has more than 1.2 billion active monthly users with a staggering 800 million people accessing the site daily⁴³. Banks have begun creating services on this platform that are resonating well with consumers. For example, Fidor is a highly innovative online bank in Germany that has deeply embraced social media.

Fidor uses a Federated Identity approach, allowing customers to authenticate using a variety of social media platforms and uses reputational metrics as a factor in their risk analysis. In fact, customers can establish an account with Fidor using only a Facebook identity (albeit with limited account functionality until regulatory requirements are met). Interestingly, Fidor uses the number of “likes” for its Facebook account as one factor in determining overdraft interest rates – the more likes the page receives, the lower the overdraft rate.

Fidor have recently announced their intention to expand into the US market, primarily targeting Gen Y consumers.

DenzBank of Turkey and the Commonwealth Bank of Australia have introduced social banking on Facebook to allow customers to pay utility bills, check account balances and transfer money to Facebook friends.

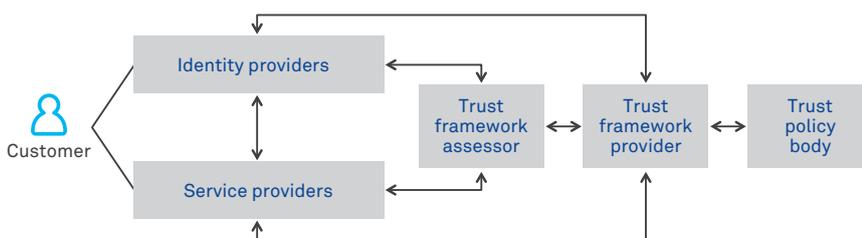
Even seemingly simple tasks such as establishing what information should be conveyed during authentication can be complex. In an analytics-driven world where authorisation can be nuanced and contextual, the data around the context of an authentication may be just as important to a service provider as the act of authentication itself. In some schemes, even identifying which IdP a given visitor is associated with – known as Where Are You From (WAYF) – is difficult. Conversely, the authenticating IdP may gain

significant user intelligence, even though the service being accessed is unrelated to them. Institutions need to negotiate how resulting data can be used and who carries legal or financial liability for incorrect authentication, incorrect denial of access or misuse of customer information. Making Federated Identity commercially viable will require cross industry business models that provide an acceptable return in investment – commensurate to risk encouraging collaboration within appropriate trust and legal frameworks.

Many of these concerns around Identity Federation are driving the development of “Trust Frameworks”. These are specifications and certification programs that enable service providers and IdPs to trust each other’s respective identity, security, and privacy policies. Trust Frameworks are relatively immature and both the specifications and assessment programs can be quite complex. For an example of a relatively mature trust framework, see FICAM TFS – the trust framework for the US Federal Government⁴⁴ (see Figure 48).

One of the key recommendations of the Australian Government’s Financial Services Inquiry of 2014 was the establishment of “a national strategy for a federated-style model of trusted digital identities”⁴⁵. The recommendation includes initiatives that the Government should consider as a means of fostering collaboration. As institutions are both an issuer of identity and a relying party, Federated Identity models offer an industry-led way forward. In 2006, Australian banks, led by the Westpac Banking Group, collaborated in the design of such a model, titled ‘The Trust Centre’. However, operationalising this model proved challenging due to conflicting commercial interests.

Figure 48: Trust Frameworks



Source: Telstra Research 2015

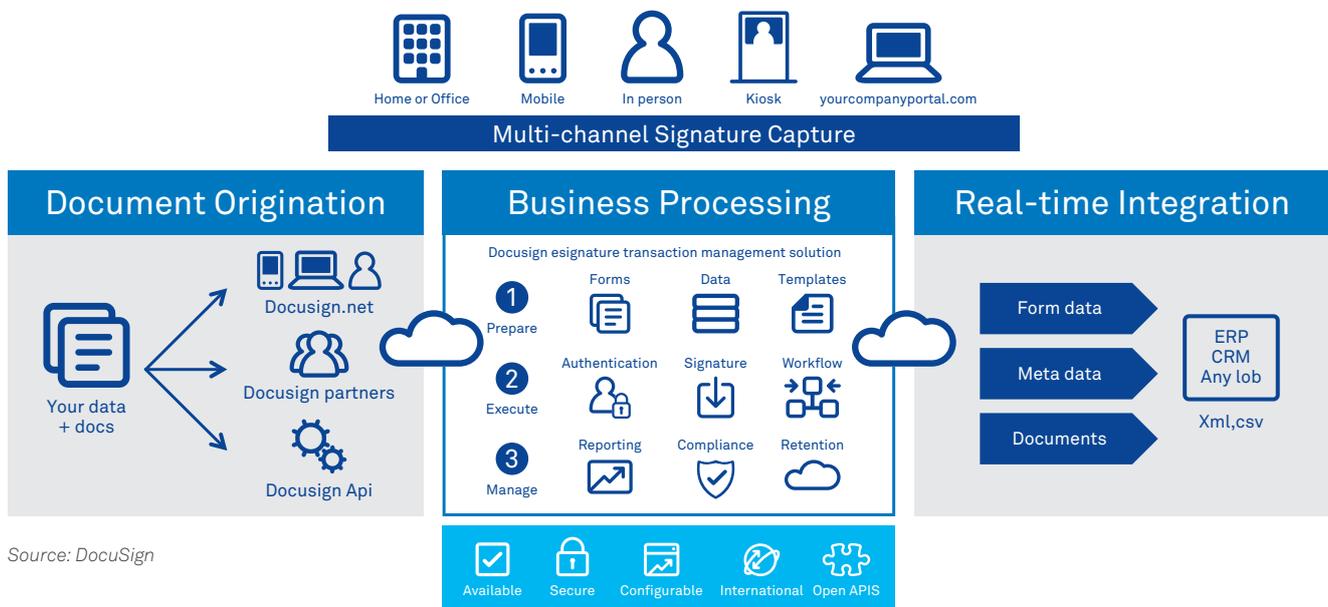
4.0 MOBILE IDENTITY TECHNOLOGY FOR THE INTERCONNECTED FINANCIAL SERVICES INSTITUTION (CONT.)

4.4 Mobile Digital Signature in a Interconnected Financial Services World

Electronic signatures draw upon a broad range of technologies. One that has seen accelerated adoption in the financial services industry is the digital eSignature. DocuSign, a world leader in this area, reports examples of implementations covering front, middle and back office use cases⁴⁶

(see Figure 49). From a user perspective, digital signatures go a long way to removing the friction associated with origination, enrolment and adds/moves/changes within the paper-intensive financial services sector.

Figure 49: eSignature Applications



Source: DocuSign

Case Study 7: Commonwealth Bank of Australia – eSignature SmartSign

In 2013, in what was reported as an Australian banking sector first, the Commonwealth Bank of Australia launched its SmartSign service, which allows customers to execute loan and equipment financing documents electronically using a secure online portal. The bank reports that SmartSign has reduced the time taken between signing documents and accessing funds from 48 hours to four hours⁴⁷.

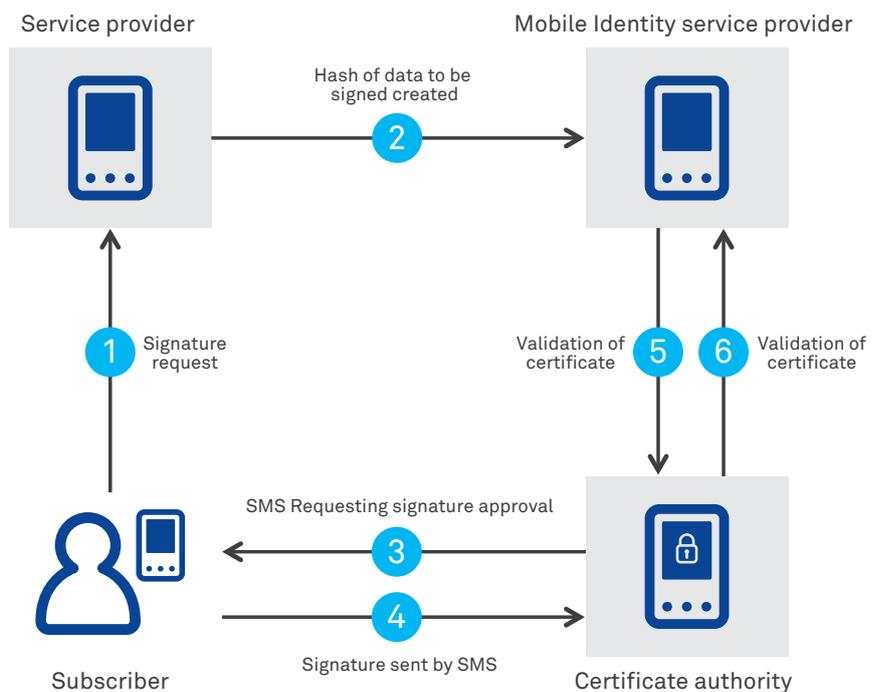
Typical two-factor authentication uses “Something I Know” (e.g. a password) and “Something I Have” (e.g. a handset to which an OTP is delivered). Where a higher level of security is required, additional authentication factors can be added. The smartphone is well equipped to handle these additional factors – for example, “Something I Am” (via biometrics), “Somewhere I Am” (location) or “Something I Do” (behavioural analytics).

When a legally binding proof of an authentication or authorisation transaction is required, the introduction of a mobile signature based on PKI (Public Key Infrastructure) technology adds robust identity proofing and the generation of digital certificates for identity validation. Digital signatures assert identity by using Public Key Infrastructure to digitally sign and secure a message sent between two parties (see Figure 50). In some respects therefore, digital signature has a slightly different purpose to other mobile identity management solutions, and focuses on non-repudiation:

- Only the sender and recipient can read it (message is encrypted);
- The message is authentic and has not been tampered with in transit (legal/compliance); and
- The recipient knows who signed and sent it.

If personal information is now seen as a new ‘asset class’ that is key to the efficient operation of the digital economy (as stated by the World Economic Forum), mobile identity could be seen as the simple, private and secure authentication solution that enables the authentication of personal information and identity over a full range of assurance levels.

Figure 50: Digital Signature Flow



Case Study 8: Estonia Mobile ID – Swedbank

Estonia has been acknowledged as a pioneer in Mobile Identity since 2007. Today it boasts one of the world’s most advanced digital signature systems, with over 80,000 digital signatures made each day. The success of Estonia’s Mobile ID initiative is underpinned by four key principles – decentralisation, interconnectivity, an open platform and open-ended process. Today, over 300 organisations use this service in both the public and private sector. Banks in Estonia were among the first users of Mobile ID. Swedbank attributes Mobile ID for the significant increase in transactions via its mobile banking app to 26 per cent of its mobile banking customers use Mobile ID and make up 38 per cent of all logins⁴⁸.

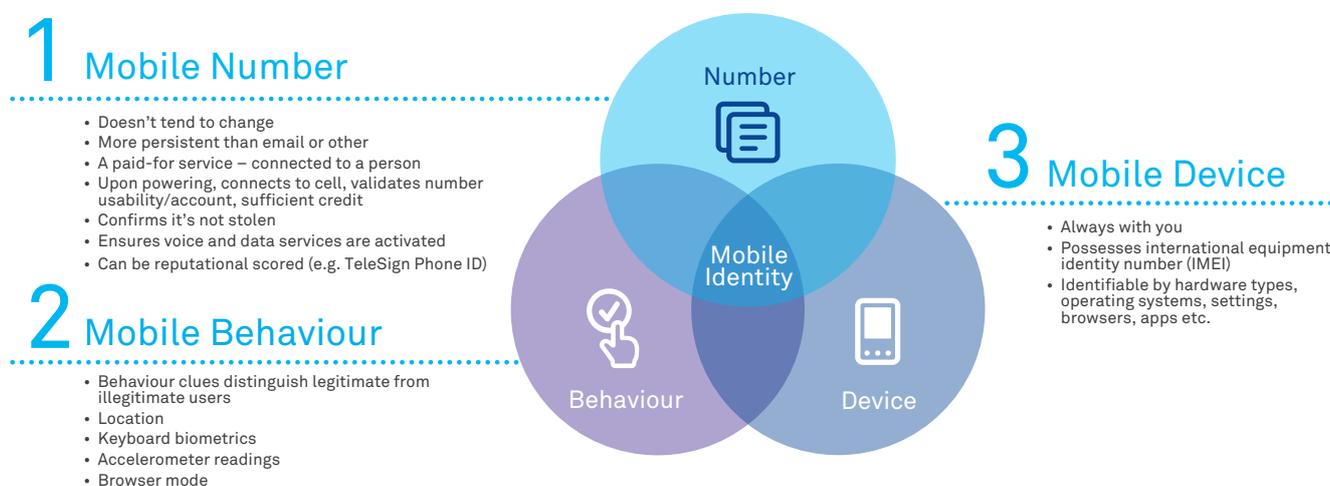
4.0 MOBILE IDENTITY TECHNOLOGY FOR THE INTERCONNECTED FINANCIAL SERVICES INSTITUTION (CONT.)

4.5 Mobile ID = Mobile Number + Device + Behaviour

Defining Mobile Identity. The concept of Mobile Identity is defined by three inter-related components: your phone number, your device and your mobile

activity or behaviour, and when these components work together this power is multiplied many times over (see Figure 51).

Figure 51: – Mobile Identity Overview



Your Mobile Number

It's less likely that you'll change your phone number frequently. Mobile number porting enables the consumer to retain their number when moving from one mobile operator to another within a country – in other words, you can keep your number and assign it to a new SIM card. This stickiness means that a phone number is better and more persistent than identifiers such as an email address. What's more, because you are paying for your mobile phone service, you are more likely to be a real person.

More significantly, every time you turn on your phone, your mobile operator connects you to the nearest cell tower, validates that your number is usable and linked to a valid account, which is in credit or is billable.

It confirms your device isn't stolen, and ensures that the voice, text and data services are ready to use. These actions create data that you can use to identify yourself quickly and effectively. This data is factually accurate and very hard to fake.

Technologies have now emerged that enable reputational scoring of a mobile number. For example, TeleSign, a world-leading mobile identity company that Telstra announced an investment into, has patented a solution called Phone ID. When reputational scoring of a mobile number is incorporated within enrolment/registration/event workflow, it provides institutions with real-time, powerful, context-based intelligence to either block, question or allow an activity.

Your Device

Your device is the next key to Mobile Identity. In general, it is always present on your person. Wherever you go, your phone goes with you. What's more, every mobile device is unique. Each possesses its own International Mobile Equipment Identity number (IMEI). There are also hundreds of attributes that can be used for identification: hardware types, operating systems, settings, browsers and apps.

Your Behaviour

The final aspect of Mobile Identity is behaviour. Behavioural clues can often distinguish legitimate from illegitimate users. Location is an obvious one. Is that Nigerian transaction on your credit card occurring while you are sitting at home in Sydney? Keyboard biometrics and accelerometer readings can yield behavioural data like typing speed and the way the device is held, revealing patterns inconsistent with those of the legitimate device owner. A browser kept on private mode or the downloading of apps used to crack passwords may also be behavioural clues that point to potential fraudsters.

With customer's permission, the security information described above can help institutions prevent registration fraud, account takeover, and assist in secure account or password recovery. Here are three ways Mobile Identity can really help:

Mobile Identity in Action

1. Account Registration

Two-Factor Authentication is already widespread – for example, using SMS or a voice call to confirm you are a live person and in possession of that phone number. This is now being taken a step further, with risk scores being applied to phone numbers depending on whether they are landlines, free voice-over-IP numbers masquerading as mobiles, or legitimate mobile numbers, and whether fraud has previously been detected.

These techniques are becoming more sophisticated, and your mobile number will be used to check specific data to confirm that you are you. For example, if you've had a post-pay mobile phone account for 10 years, always paid your bill, and your phone hasn't been stolen, you'll have a very low risk score. But if you have reported your phone stolen, or someone has fraudulently forwarded your calls to another number to attempt to take over your account, that number will be assigned a high-risk score.

This risk score can be used to decide to allow you to register for an account, or to actively verify you are in possession of the phone by sending you a verification code, or simply to block the registration completely. Requiring phone verification during account creation significantly slows the rate at which fraudsters can create fake accounts and increases the fraudster's cost for each account created. Typically, phone-verified accounts cost at least 160 times more on the black market than accounts that are not phone verified.

2. Account Access and Usage

Once you have set your account up and linked it to your mobile number, Mobile Identity can be used to keep you secure. Using a mixture of on-device authentication, such as SMS or push notifications, and frictionless off-device checks done in the background (such as confirming your location), a far higher level of security can be put in place, with minimal impact on your online experience.

3. Account Recovery

Account recovery is a problem whenever an account is compromised, you forget your password, or change your email address. Password resets sent by SMS or voice call are more secure and save time and money. Help desk calls can mount up for password reset and these costs add up quickly when there are millions of users online.

With Mobile Identity, once a verified phone number is linked to an account, that account can easily and securely be recovered using an out of band SMS message, voice call or mobile app push notification. If an account is breached, subsequent "domino" or "cascading" account takeovers will be prevented by institutions using a cooperative alerting system. This will enable the institution that has detected the breach to inform a central register, which will then alert other institutions that have an account linked to that phone number. If a fraudster tries to then reset passwords on those other accounts, they can be blocked immediately.

4.0 MOBILE IDENTITY TECHNOLOGY FOR THE INTERCONNECTED FINANCIAL SERVICES INSTITUTION (CONT.)

4.6 Mobile Threat Defence

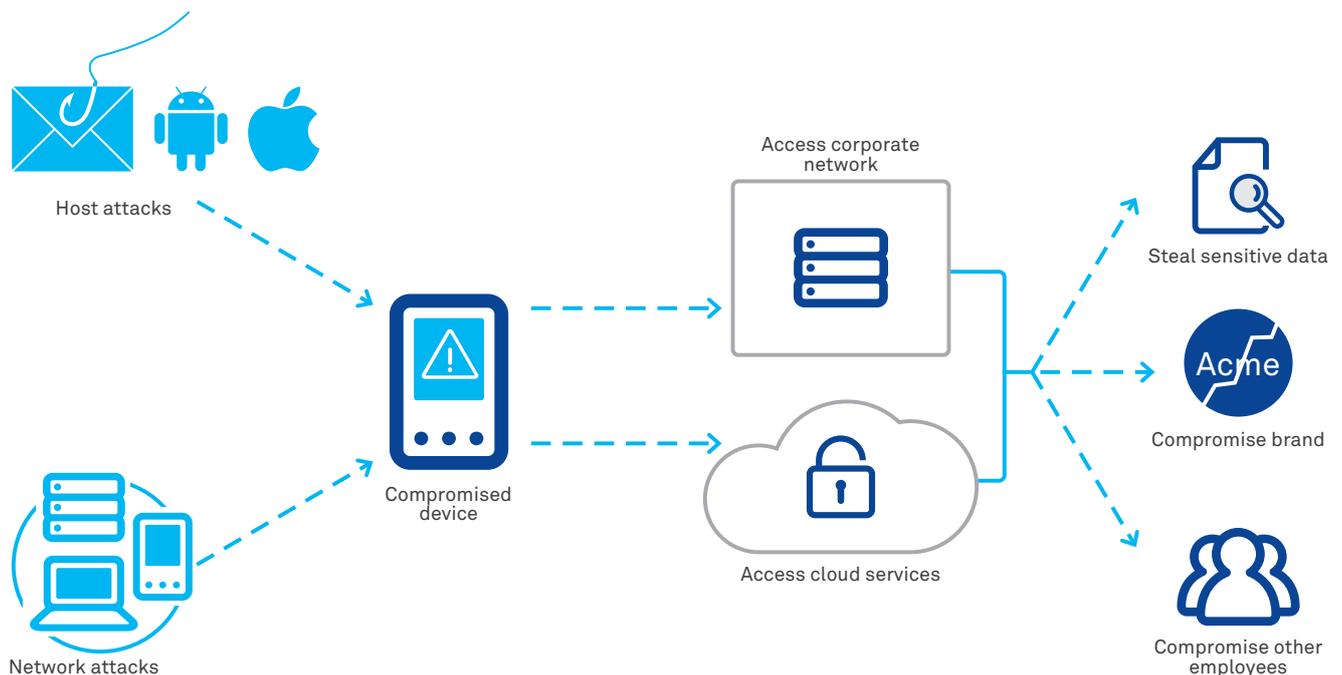
The speed and scale of mobile financial services developments together with flexible working and BYOD are beginning to redefine our future way of working and bring new risks – often at unprecedented levels. It's estimated that cyber-attacks will cost the global economy \$3 trillion in lost productivity and growth by 2020⁴⁹. With more institutions mobilising workforces – such as financial planners, mortgage lenders, business bankers, insurance agents, investment managers and relationship managers, business is being conducted on the go, outside of the office, on Wi-Fi or cellular networks like never before. The risk, therefore, of a targeted cyber attack has significantly increased exponentially. One compromised mobile device from either a host or network attack can result in a security breach, compromising an institution's data, assets and brand.

Attacks have had an impact on all parts of the sector. A study of 46 Global Security Exchanges by the International Organisation of Securities Commission found that more than 53 per cent had experienced a cyber attack⁵⁰. Another study by Price Waterhouse Coopers (PwC) in 2014 reported that 45 per cent of financial services Institutions have suffered economic crime⁵¹. The scale of individual attacks is also unparalleled. In February 2015, the New York Times reported analysis from Kaspersky Lab of an attack targeting more than one hundred banks and other financial institutions in thirty nations, estimating losses of over US\$1 billion – describing it as potentially the largest bank theft ever⁵². Cybercrime has now become the most significant threat to growth in the financial services sector over the coming years, as outlined by a study by PwC of 175 banks CEO's⁵³.

In 2015, Telstra announced an investment in Zimperium, creators of the world's first mobile intrusion prevention system™ (IPS) powered by artificial intelligence. Zimperium's Mobile Threat Defense (zMTD) suite delivers enterprise-class protection for Android and iOS devices against the next generation of Advanced Persistent Threats (APTs) and Nation-State attacks. Zimperium uses patented, behaviour-based analytics that sits on the device to detect and protect against network and host threats in real time. It prevents identity theft on mobile devices by protecting against all different types of MITM attacks and unknown, zero-day attacks.

Zimperium Mobile IPS (zIPS) also puts the sensor power of expensive IPS appliances into a mobile device; allowing institutions to transform BYOD from a threat to an advantage (see Figure 52).

Figure 52: – Mobile Threat Defence

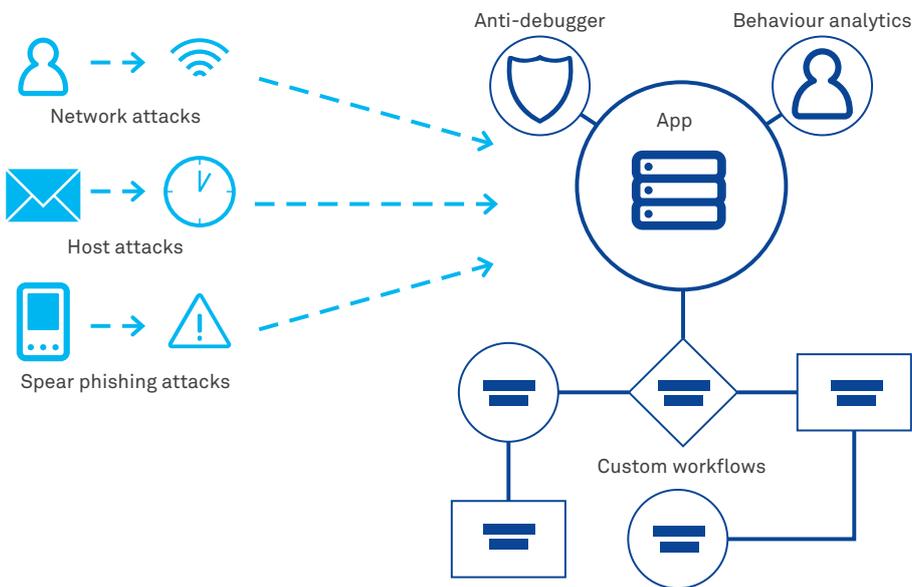


Source: Zimperium

But with the mobile now becoming the primary and preferred means for consumers to interact with their institution, the device-related risks and threats need to expand well beyond those of its works forces. Research by RiskIQ identified that 11 per cent of 350,000 Android banking and finance-related apps found across 90 app stores contained malware or suspicious binaries. Of these apps, 21,000 contained adware, 20,000 contained Trojan malware, 3,823 spyware, 209 exploit code and 178 malicious Javascript⁵⁴.

In a future development, Zimperium Mobile App Security (zMAS) suite will allow mobile application developers to leverage the power of its behaviour analytics engine to protect application sandbox from cyber attacks. zMAS comes with an anti-debugger, which prevents theft of sensitive data from an application's cache or memory. Developers can also use APIs to interact with zIPS and implement custom workflows (disable login, truncate transaction, or raise fraud alert) when under attack (see Figure 53).

Figure 53: Mobile App Security



Source: Zimperium

4.0 MOBILE IDENTITY TECHNOLOGY FOR THE INTERCONNECTED FINANCIAL SERVICES INSTITUTION (CONT.)

4.7 Secure Omnipresent Intelligent Identity

The convergence of social, technological and financial trends mean the identity and access management (IDAM/IAM) environment for financial service institutions has quickly become much more complex and much more demanding. It must provide greater flexibility and evolve and react within shorter timescales than ever before. Previously a key consideration for identity and access management architectures was:

“Does this person have the right credentials to gain access to the system?”

Now the questions are more complex and nuanced, such as:

“Does this person have the right credentials and the authorisation to gain access to the system?”

“How can I be certain that it is actually the person gaining access? Should they have access to this system at this time and in this context?”

“What level of confidence do we have in the identity of this individual person, at this particular time, in this unique context?”

“What options do we have for this individual customer in this particular context for increasing that confidence while meeting their service expectations?”

The utilisation of the 4As – Authentication, Authorisation, Access management and Audit – provide a framework for handling the identity questions above. They provide a mechanism for verification, policy management, authentication and allowing users access in a consistent and flexible way.

Most institutions seeking more secure ways to identify and authenticate customers face a balancing act between increased security and the risk of increasing friction for customers. However, these same sensitivities mean that a flexible, well considered and well implemented IAM architecture that does deliver a good user experience can be a key differentiator in the market. Case Study 9 shows an example of how Google are using intelligence to reduce the impact of Two-Factor Authentication on the user experience – a simple case of identity intelligence being used to drive Intelligent Identity Management. To securely meet the escalating service requirements of a new generation of customers with increasingly sophisticated financial product needs, financial services institutions will need to similarly embrace Intelligent Identity Management – and extend it.

Case Study 9: Google 2-Step Verification

To help users better protect their online accounts, Google supports Two-Factor Authentication for many of its web-based services (called 2-Step Verification⁵⁵). For example, in addition to a username and password, a user connecting to Google’s Gmail service may be asked to authenticate using a second factor such as hardware token or by entering a one-time-password sent to their mobile device. The important word is “may”. Google claim to take hundreds of factors about a given interaction into account when deciding whether to ask for a second factor.



The introduction of Intelligent Identity Management no doubt provides customers with a great user experience where the ability to access their financial institutions services on the move, how they want, doesn't come at a cost to security. The downside of introducing Intelligent Identity Management is the impact on the underlying infrastructure, the checks and balances that are needed, and the extension of the attack surface for the financial institution (as more devices and networks are involved, there are more devices and networks that can potentially be compromised).

To combat these negatives, some additional controls will need to be implemented within the financial institution to maintain the confidentiality, integrity and availability of the infrastructure.

Physical controls for the infrastructure need to be applied and regularly verified via threat assessments and regular auditing. Only authorised personnel should have physical access to systems, and this access must be reviewed regularly. Access to data centres, system racks, etc. should all be controlled, regularly reviewed and audited. Of course, this means that robust, consistent enterprise-wide IDAM strategy for internal users such as staff and contractors is even more vital. As detailed earlier, something as simple as stealing staff username/passwords can lead to significant financial and reputational losses.

Additional controls need to be applied at the network level. Firewalling (to control access to systems), intrusion prevention and detection systems (to detect anomalous behaviour on the network and systems) provide additional mechanisms for maintaining confidentiality, integrity and availability of the infrastructure. Feeding system logs into a Security Incident and Event Management system (SIEM) to detect and correlate events, ensures that in the event

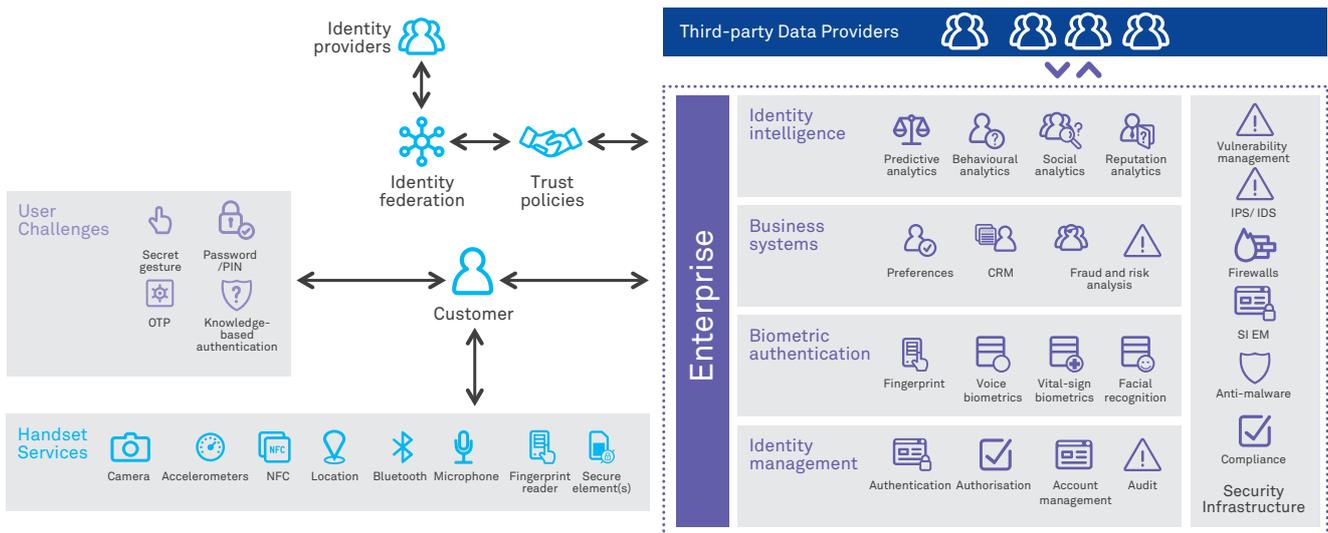
that an anomaly is detected, then remediation and recovery steps can be swiftly taken. Incident response and problem management policies and procedures are critical in the secure recovery of the service.

Verification of the environment via vulnerability testing (also known as penetration testing) and compliance testing is recommended. Continuous vulnerability management solutions can regularly and automatically test the environment for vulnerabilities and compliance, and report on required actions. These systems have the benefit of being regularly updated with the latest compliance data and vulnerability signatures, so that scans are performed with the latest information. They can track the history of vulnerabilities (in the event that if vulnerability resurfaces due to a patch being missed or rolled back, it is detected and reported); provide automated reporting and can be linked into other security systems and tools (SIEM, etc.) to provide an enterprise-wide view of threats, compliance and events. These systems take out the human factor involved in reviewing the results of vulnerability testing.

Finally, our previous report "Analyse This, Predict That: How Institutions Compete and Win with Data Analytics"⁵⁶ details some of the opportunities and impacts that cloud-enabled big data-style analytics will create for financial service institutions. In many organisations, marketing has spearheaded the use of techniques such as behavioural analytics, predictive analytics, social network analytics and sentiment analysis to understand and influence the decisions made by customers. The same techniques can be used to provide evidence relating to the authentication process. Some time ago, Gartner Research coined the term "Identity Intelligence" to describe the gathering and collation of data from a wide range of sources to build a profile of an individual.

4.0 MOBILE IDENTITY TECHNOLOGY FOR THE INTERCONNECTED FINANCIAL SERVICES INSTITUTION (CONT.)

Figure 54: Anatomy of Secure, Omnipresent Intelligent Identity



Source: Telstra Research 2015

Key Takeouts

1. The three concepts (Federated Identity, Two-Factor Authentication and Mobile Digital Signature) tested in this research are anticipated to reach the mainstream within the next two years. What our research further found was that consumers perceive biometrics technologies to provide stronger proof of identity, but much work needs to be done to stimulate uptake of this method, given the relatively low numbers of consumers using it today.
2. The financial services sector is seen as the biggest driver of the multifactor authentication market, which is expected to reach USD \$5.45 billion by 2017.
3. Emerging technologies will give consumers significantly greater control of personal information. These regimes allow consumers to share only enough relevant and encrypted personal information as is required by the interaction at hand. The other option includes High Assurance Public Identity Providers, who create and manage identities for individuals.
4. Techniques such as behavioural analytics, predictive analytics, social network analytics and sentiment analysis – used to understand and influence the decision of customers – can also be used to provide evidence for the authentication process.

5.0 CONCLUSIONS

Unlocking Trust for the Mobile First 'no-finapp-phobic' Gen X and Y



Competition by institutions to cater for the expectations of Gen X and Y is separating players within the market. This battle is about digital relevancy, and is increasingly being played out through mobile technology. In Australia, and indeed in many other markets, the Online Pure Plays are leading the way, while in the US, the Mobile Pure Plays have changed the game again and have already secured share.

Consumers have decided that smartphones will be the connection between our human identity and our digital one. The speed with which this has occurred has outpaced the financial services industry's ability to adapt. This gap has created new industrial-scale risks and exposures that have already had a significant impact:

1. 38 per cent of consumers we studied across seven countries had been directly or indirectly impacted by identity theft, and;
2. 45 per cent of financial institutions suffered economic crime, with incidents reportedly rising by eight per cent and the costs of security incidents jumping 24 per cent in 2014⁵⁷.

The rapid uptake of social media, mobility and the cloud requires institutions to relate to identity in different ways, in order to address our changing lifestyles and life stages. Further, institutions can become leaders in creating the Internet of Trust, facilitating greater community, connectivity and commerce.

As the centre of financial services gravity moves to Gen X and Y, who today account for around half of the world's population and primarily

interact with financial institutions through their mobile devices – we need to respond by designing identity services that accommodate the fusion of financial services, mobility and identity and that engender consumer trust and confidence. Our research highlighted that mobile identity services can both meet and exceed these expectations.

For institutions, mobile identity services deliver a wide-ranging payload in terms of:

1. Acquisition and retention of Gen X and Y customers by developing trust in keeping their finances secure;
2. Improved customer satisfaction and increased advocacy by developing trust in keeping personal information safe and sound; and
3. Reduced incidences of fraud, security and privacy breaches.

These benefits, however, can only be realised through new models of collaboration within the broader digital mobile ecosystem.

For 'no-finapp-phobic' Gen X or Y consumers, digital mobile technologies have indeed changed how they prefer to be identified. We now need to shift the trust paradigm from making them prove their identity, to recognising them for who they are. The good news is that consumers are keen to travel on this transformation journey with you.

It's time to change the conversation.

For More Information

Visit: www.telstraglobal.com/mobile-identity

Contact Rocky Scopelliti directly
Rocky.Scopelliti@team.telstra.com

Contact your Telstra account representative:

- Asia: +852 2827 0066
- Americas: +1 877 835 7872
- EMEA: +44 20 7965 0000
- Australia: 1300 835 787

6.0 ABOUT THE AUTHOR



Rocky Scopelliti is the Global Financial Services Industry Executive at Telstra Global Enterprise Services. Rocky is Telstra's thought leader in Banking, Finance and Insurance.

Rocky has more than 20 years' senior management experience in the information technology and financial services sectors, encompassing Product Development, Strategy and Planning, Business Development, Research and Strategic Marketing.

A distinguished author and international speaker, Rocky has produced 10 thought leadership research reports that have become widely recognised for their contribution to the development of digital financial services.

These include:

- ICT as a Driver to Improve Service to Generation Y for Financial Services
- Servicing Micro Businesses – What Financial Services Need To Know
- Mobile Innovation – The Next Frontier for Growth and Productivity for Insurers
- 2012 for the Financial Services CIO – Why Agile IT Strategies are Key to Meeting the Requirements of a New Financial Age.
- The Digital Media Bank – How Video Can Better Engage Your Customers and Workers
- Cross-Industry Innovation – The Secret May Well Be In Another Industry (co-produced)
- Towards a Clever Australia – Banking, Financial Services and Insurance Industry Insights Whitepaper
- The Digital Investor – How Changing Demographics and Digital Technologies are Impacting the Wealth Management Market
- Analyse This, Predict That – How Institutions Compete and Win with Data Analytics
- Mobile Identity – The Fusion of Financial Services, Mobility and Identity

Educated in Australia and trained in the United States – at Sydney University and Stanford University respectively – Rocky has a Graduate Diploma in Corporate Management and a Masters in Business Administration. He is also a Graduate and Member of the Australian Institute of Company Directors.

7.0 ACKNOWLEDGEMENTS

Warren Jennings

Warren Jennings is a Senior Technology Strategist in Telstra's Chief Technology and Innovation Group. He has decades of experience in developing strategies, products and service offerings that combine emerging technologies and mature technologies from a wide variety of disciplines to solve real-world issues for organisations and their customers.

Warren has an honours' degree in science and engineering from Monash University and a Masters degree in Electronic Commerce from Deakin University.

Roy Morgan Research

Roy Morgan Research is the largest independent Australian research company, with offices in each state of Australia, as well as in New Zealand, the United States and the United Kingdom. A full-service research organisation specialising in omnibus and syndicated data, Roy Morgan Research has more than 70 years' experience in collecting objective, independent information on consumers.

In Australia, Roy Morgan Research is considered to be the authoritative source of information on financial behaviour, readership, voting intention, consumer and business confidence. Roy Morgan Research is a specialist in recontact customised surveys that provide invaluable and effective qualitative and quantitative information regarding customers and target markets.

TeleSign

TeleSign is the leader in Mobile Identity solutions, helping customers secure more than 3.5 billion end user accounts worldwide and prevent registration fraud, while improving user experience and managing costs. TeleSign delivers account security and fraud prevention with Two-Factor Authentication based on each user's Mobile Identity (phone number, device and behaviour) and driven by real-time, global intelligence, including reputation scoring and device data.

TeleSign solutions address the full spectrum of account security – registration, access, usage and recovery – while also streamlining the user experience to help increase adoption, retention and trust. TeleSign prevents registration fraud, stops account takeovers and securely authenticates end users via SMS, voice and mobile app.

With its proven global infrastructure and operations, TeleSign is able to build and manage a clearing house of predictive data, including reputation scores based on phone types, carriers, subscribers, device status, traffic patterns and reported fraud.

Today, 20 of the top 25 global web properties and nine of the top 10 US web properties – with end users in over 200 countries and 87 languages – secure their accounts, prevent fraud, remove friction and manage costs with Mobile Identity solutions from TeleSign.

8.0 NOTES & REFERENCES

- 1 No-finapp-phobia is the fear of being without mobile financial applications, inhibiting the ability to save, spend, borrow or invest. The term, is an abbreviation for “no-financial-application-phobia”, and was created during a 2015 study by Rocky Scopelliti of Telstra Corporation Limited, an Australian Communications Company, who researched and authored a report titled ‘Mobile Identity – The Fusion of Financial Services, Mobility and Identity. This report looks at how mobile digital technologies have changed how Generations X and Y prefer to be identified and how the trust paradigm has shifted from having to prove who they are, to being recognised for who they are.
- 2 World Midyear Population by Age and Sex for 2015; <https://www.census.gov/population/international/data/idb/worldpop.php>
- 3 Banking 2020, Accenture, November 2013.
- 4 McKinsey & Company, Strategic choices for banks in the digital age’ January 2015.
- 5 Average Footings (\$): also referred to as ‘Average Wallet’. It is calculated by dividing the total amount of Dollars held by Gen X and Gen Y customers in Traditional Banking Products at an institution by its number of Gen X and Gen Y customers. The Average Wallet shows how more or less valuable customers of an institution are when compared among its peers. Traditional Banking Products include: Deposits and Transactions; Mortgages; Personal Lending; Major Cards.
- 6 Telstra Research, 2014.
- 7 Reference: <http://www.bain.com/publications/articles/customer-loyalty-in-retail-banking-2012.aspx>
- 8 PwC Global State of Information Security Survey, 2015.
- 9 <http://mobileidworld.com/mwc-2015-mobile-identity-on-day-one-3029/>
- 10 GSMA The Mobile Economy, 2014.
- 11 www.bain.com/publications/articles/customer-loyalty-in-retail-banking-2014-global.aspx
- 12 Jake Kendall, Nataliya Mylenko and Alejandro Ponce, “Measuring Financial Access Around the World”, June 2010, Policy Research Working Paper 5253, The World Bank. Available at <http://elibrary.worldbank.org/doi/book/10.1596/1813-9450-5253>
- 13 CGAP, GSMA, and McKinsey & Company “Mobile Money Market Sizing Study”, 2010.
- 14 GSMA The Mobile Economy, 2014.
- 15 Finextra: Gates makes mobile banking bet, 26 January 2015.
- 16 GSMA The Mobile Economy, 2014.
- 17 EY Global Consumer Banking Survey, 2014; Winning through customer experience.
- 18 Identity is the New Money; David Birch 2014.
- 19 Varmetic Data security, security measures to go under spotlight as new Data Protection Directive Approaches, 8 July 2014.
- 20 Singaporean Personal Data Protection Commission, Personal Data Protection Act Overview, 2014.
- 21 “Digital Universe Invaded By Sensors”, EMC, (<http://australia.emc.com/about/news/press/2014/20140409-01.htm>).
- 22 “The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things”, IDC 2014 (<http://idcdocserv.com/1678>).
- 23 See <http://iotinternetofthingsconference.com/2014/12/07/iot-market-forecast-worldwide-iot-predictions-for-2015/>
- 24 “2 Billion Consumers Worldwide to Get Smart(phones) by 2016”, (<http://www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones-by-2016/1011694#sthash.90Sj0V1C.dpuf>).
- 25 “Forrester Research World Tablet Adoption Forecast, 2013 To 2018 (Global), Q4 2014 Update”, Forrester Research Inc. December 2014.
- 26 “515 Million Mobile Sensing Health & Fitness Sensor Shipments in 2017” (<http://onworld.com/news/mobile-sensing-health-wellness.html>).
- 27 “Baby, You Can Crash My Simulated Car” (<http://readwrite.com/2014/08/21/carvoyant-connected-car-app-simulation-hack-sandbox>).
- 28 “Look Ma, No Hands!”, IEEE 2012(http://www.ieee.org/about/news/2012/5september_2_2012.html).
- 29 “Gartner Says a Typical Family Home Could Contain More Than 500 Smart Devices by 2022”, Gartner Inc, September 2014 (<http://www.gartner.com/newsroom/id/2839717>).
- 30 “Need for a Trillion Sensor Roadmap” (<http://tsensorssummit.org/Resources/Why%20Sensors%20Roadmap.pdf>).
- 31 “The Installed Base of Smart Meters Will Surpass 1 Billion by 2022”, Navigant Research, 2013 (<http://www.navigantresearch.com/newsroom/the-installed-base-of-smart-meters-will-surpass-1-billion-by-2022>).

- 32 "Press Release – Consumer Electronics M2M Connections Will Top 7 Billion in 2023, Generating USD\$700 Billion in Annual Revenue", Machina Research 2014 (<https://machinaresearch.com/news/press-release-consumer-electronics-m2m-connections-will-top-7-billion-in-2023-generating-usd700-billion-in-annual-revenue/>).
- 33 See <http://kantarainitiative.org/confluence/display/uma/Home>
- 34 Gartner; The Future of Managing Identity, 2014.
- 35 SIM Swapping - Fraudsters can manipulate an account if they can control both the SIM (to receive security OTPs) and the login credentials. SIM Swap allows fraudsters to intercept a phone-based OOB authentication from financial institutions to execute a targeted attack against a specific user. It also defeats location checking and other anti-fraud measures.
- 36 For an interesting comparison of the AT&T and Verizon approaches to identity services, see <http://www.trishburgess.com/trishs-blog/attand-verizon-mobile-identity-initiatives>
- 37 Gartner; The Future of Managing Identity.
- 38 Markets and Markets, 2012.
- 39 <http://www.americanbanker.com/news/bank-technology/biometric-tipping-point-usaa-deploys-face-voice-recognition-1072509-1.html>
- 40 <http://www.theage.com.au/it-pro/business-it/westpac-launches-fingerprinting-access-for-online-banking-on-ios-and-android-devices-20141205-120yr9.html>
- 41 Finextra: Canadian banks to test heartbeat bracelet for contactless payments, 3 November 2014; Halifax trials heartbeat authentication technology, 13 March 2015.
- 42 Gartner; Predicts 2014: Banks and Investment Services Firms Must Adapt to a radically Changing Business Environment, November 2013.
- 43 Facebook News Room, company information, May 2014.
- 44 See <http://www.idmanagement.gov/trust-framework-solutions>
- 45 "Financial System Inquiry Final Report", Australian Federal Government, November 2014. (http://fsi.gov.au/files/2014/12/FSI_Final_Report_Consolidated20141210.pdf).
- 46 <https://www.docusign.com.au/solutions/industries/financial-services>
- 47 <https://www.youtube.com/watch?v=i7mwh0QTWg0>
- 48 GSMA Estonia's Mobile ID: Driving Today's e-Services Economy.
- 49 http://www.mckinsey.com/insights/business_technology/risk_and_responsibility_in_a_hyperconnected_world_implications_for_enterprises
- 50 IOSCO and the World Federation of Exchanges Office, cybercrime securities markets and systemic risk, July 2013.
- 51 Pricewaterhouse Coopers 2014 Global State of Information Security Survey.
- 52 Sydney Morning Herald; Cyber criminals steal millions of dollars in massive malware bank heist, 15 February 2015, Finextra; Hackers nab \$1 billion in global cyber heist, 16 February 2015.
- 53 Finextra, Bank chiefs frightened by cyber risks – PWC, 17 February 2014.
- 54 Finextra: 11 per cent of Android banking apps 'suspicious' – Risk IQ.
- 55 See <https://www.google.com.au/landing/2step/>
- 56 Available from <http://www.telstraglobal.com/big-data-in-financial-services>
- 57 PwC Security deficits in an interconnected world; Key findings from The Global State of Information Security® Survey 2015.

© 2015 Telstra Corporation Limited. All rights reserved. This work is copyright. The Copyright Act 1968 permits fair dealing for study, research, news reporting, criticism or review. Permission to use selected passages, tables or diagrams must be obtained from Telstra and if granted, must be appropriately referencing Telstra and the report. Telstra reserves the right to revise this document for any reason without notice. The information in this document is based upon assumptions, forecasts and reflects prevailing conditions and Telstra's views as of June 2009, all of which are accordingly subject to change. In preparing this document, Telstra has relied upon and assumed, without independent verification, the accuracy and completeness of all information available from public sources or which was otherwise reviewed by Telstra. To the extent permitted by law, Telstra is not liable for any errors in this document nor any damage, loss or other liability (including without limitation direct, indirect, special or consequential) suffered or incurred any person in reliance on this document. ™ Trade mark of Telstra Corporation Limited. © Registered trade mark of Telstra Corporation Limited ABN 33 051 775 556

