A WHITE PAPER PRODUCED BY FINEXTRA
IN ASSOCIATION WITH HID GLOBAL
OCTOBER 2017

THE ROLE OF DIGITAL IDENTITY IN THE FUTURE OF BANKING

01
INTRODUCTION
DIGITAL IDENTITY A NO-BRAINER FOR BANKS?

If, as leading fintech authority Dave Birch of Consult Hyperion has famously asserted, “identity is the new money”, then it surely goes without saying that the future of banking is keeping identity safe? Just as banks have been the trusted guardians of our money for millennia, so, as we enter into the connected age, we will trust banks to look after its currency – our digital identity.

This prized asset will be our passport through the digital world, our key to unlocking all the services we need as we navigate through our ecosystems. We will want both to be able to access and use it easily, and to be certain it is completely secure – exactly the conditions we have relied on our banks to ensure when it comes to our money for centuries. The logic of banks as leaders in digital identity is inescapable.

For their part, this new avenue of business for the banks could not come at a more opportune moment. With the imminent enforcement of the revised Payment Services Directive (PSD2) and the consequent unleashing of the phenomenon of open banking, incumbent banks are under siege.

PSD2 is mandating the creation of a new competitive landscape. Regulated Third Party Payment Providers (TPPs) must be given access by the banks to the account information of their customers, in order to enable innovative new entrants to offer exciting new payment initiation and account aggregation capabilities to those customers.

In other words, banks are being forced to make it easier for competitors to poach their customers.

PSD2 is not the only driver for the move to open banking. Other regulation in other markets is having the same effect, as is the rise of new banking entrants, the relentless development of technology and the increasingly demanding requirements of tech-savvy customers. In the EU, PSD2 is increasing the urgency around open banking – and the rest of the world is watching this leading example of transformation develop.

Certainly, incumbent banks have the same opportunities as new entrants in an open banking world. However, what they may not have is quite the agility – of technology and mindset – to react with the same speed, vigour and innovation as new competitors.

There is no doubt that, coming on top of the already powerful wave of new competition heralded by the rise of fintech, open banking is creating challenges for existing financial institutions.

Good news then, that, for all that they lack in contrast to nimble new entrants, incumbent banks have some very important assets – including trust as already mentioned, as well as, critically, data, about us, their customers: exactly the type of data that is needed to create digital identities.

If the future of banks as digital identity providers is so clear, why are all banks not already embarking on building this future with all speed? Why is there any need for papers like this one making the case for banks to do this?

One answer of course is that many banks are already active in digital identity, as will be explored later in this paper.

Another is that, though the argument for banks to follow this path is difficult to dispute, achieving the goal is not without its challenges.

There are some major outstanding questions to be addressed. Who will own the digital identity? The bank? Or the customer? Who will be liable if a digital identity is wrongly authenticated with damaging results? What would be the impact of a cyberattack that resulted in the hacking of a huge number of digital identities entrusted to the safekeeping of a bank? Should banks be attempting to provide digital identity for everyone? Just their own customers? Everyone in their home market? Across borders in our increasingly global village? How should banks and governments work together in the digital identity space? Will there ever be – and do we need – a universal digital identity, and if so, what role should banks play here?

These unanswered questions notwithstanding, the case for banks to look at new business opportunities around digital identity remains strong. This paper will argue that the case is especially convincing if banks build on both the core attributes they need to perform their central function – enabling secure, authenticated and compliant transactions – today, and as it evolves in the world of PSD2 and open banking.

In effect, viewed in this light, there is a natural path for banks towards becoming the main gateways for identification and authentication in the connected world.

02
WHY IS IDENTITY THE NEW MONEY?

According to Consult Hyperion's Birch in his much-acclaimed book, identity and money are both changing rapidly and profoundly, and will converge, so that all we will need for transacting will be our identities, captured in the unique record of our online social contacts.

Key to this vision are social networks and mobile phones, which will enable the creation of an identity infrastructure that can enhance both privacy and security. What happens next is impossible to predict, Birch argues – although he does contend that cash will become redundant, replaced by a proliferation of new digital currencies.

More prosaically, we need digital identity to work better in order to grease the wheels of digital commerce. This is related to that other much-cited truism about the digital world – that 'data is the new oil'.

Twenty years on from the first e-commerce sites, we are still typically using username, password and security question combinations to log-in online. These approaches are not only terribly old-fashioned, they are highly inefficient, requiring individuals and businesses to constantly re-enter the same information (while frequently forgetting key elements and facing the frustration of having to re-set everything or be forever locked out).

They're not all that secure either, as has been uncovered by a lot of very embarrassing and damaging data breaches in recent years.

It is also important to remember that this challenge will be multiplied as we see the impact of the growth of the Internet of Things and a wider connected ecosystem – we will need to log-on more and more often, and this problem of identifying people online will grow and grow.

In addition, different types of accounts require intrinsically different levels of authentication and identification. Logging on to a social media site is clearly not completely comparable to logging on to online banking, and the latter should require much more rigorous log-on processes than the former.

Therefore, wouldn't our digital lives be easier, wouldn't we be encouraged to do more online, and wouldn't digital interactions scale much more effectively if, instead of having to log-on using multiple different usernames and passwords and by answering lists of personal questions of varying lengths, we could simply grant the site we were using appropriate access to the right level(s) of our personal data – which is safely stored with a provider we trust to hold our digital identity securely?

> "Twenty years on from the first e-commerce sites, we are still typically using username, password and security question combinations to log-in online. These approaches are not only terribly old-fashioned, they are highly inefficient, requiring individuals and businesses to constantly re-enter the same information. They're not all that secure either, as has been uncovered by a lot of very embarrassing and damaging data breaches in recent years."

03

WHY DO BANKS NEED TO LOOK FOR NEW BUSINESS MODELS?

As mentioned above, PSD2 is coming, as one clear lever for and manifestation of the inevitable, global move to open banking. Open banking is an international trend – driven by other similar regulation in markets such as Australia and the US, and by the reality of technology evolution and more demanding customers.

Banks will simply not be able to maintain their former fortress-like existences, or their hold on a new age of personal and business customers who want choice, fairness, flexibility and an omni-channel experience, and are conditioned to get it.

PSD2 will legitimise and strengthen innovative new propositions in areas such as payment initiation and account aggregation, by creating new categories of regulated entity (Payment Initiation Service Providers and Account Information Service Providers) respectively.

PSD2 will also require account holding banks to securely share information about customers' transactions with these newly-regulated TPPs – in effect ramping up the pressure on banks to keep customer data secure while at the same time creating new opportunities for it to be breached.

And all this on top of the fact that the data the banks must share can be used by TPPs to offer services that could be more attractive than those that customers are used to getting from their incumbent banks.

"In its late 2016 research on Retail Banking: Digital Transformation & Disruptor Opportunities 2016-2021, UK-based fintech analyst Juniper Research predicted that more than 2 billion mobile users will have used their devices for banking by the end of 2021. This shows significant growth over the 1.2 billion who did so during 2016."

KEEPING THE CUSTOMER SATISFIED

Remember that banks already have a customer engagement problem. The famous and sobering statistic that 71% of millennials would rather go to the dentist than engage with their bank is a suitably punchy reminder of this. The stat comes from the Millennial Disruption Index, based on a three-year study by Viacom unit Scratch.

Further illustration of the engagement challenge banks face comes from the results of a survey carried out by Finextra early in 2017 among 242 consumers from 20 countries (customers of 99 different banks between them), which do not paint a particularly rosy picture. A lacklustre 49% of respondents actively agree that their banks work hard to engage them, and that they do feel engaged.

This statistic is especially concerning when viewed through the lens of findings of a parallel Finextra survey, which garnered 203 responses from 124 financial institutions in 36 countries, and which shows that banks are trying very hard to better engage with their customers. A large majority (84%) of banks in that study identified customer engagement as a top three priority – yet as we have seen, fewer than half of customers feel engaged as a result.

In short, new sources of competition from agile, customer-focused new entrants are arguably the last thing banks need in the current environment, but they have no choice but to face and tackle them.

GOING MOBILE

To combat the threat, bolster customer loyalty and underpin new customer acquisition, banks must provide services that are not only customer-driven, but work, are visible and add value where those customers are.

In this digital age, that means mobile. In its late 2016 research on Retail Banking: Digital Transformation & Disruptor Opportunities 2016-2021, UK-based fintech analyst Juniper Research predicted that more than 2 billion mobile users will have used their devices for banking by the end of 2021. This shows significant growth over the 1.2 billion who did so during 2016.

Indeed, mobile is the critical channel for banks to harness if they want to reach next generation customers, as is being demonstrated by the new breed of mobile-only banks targeting millennials.

It is also important to understand that as well as innovation in channel and delivery, these customers are also looking for innovation in product and service. They don't want to see their account information for the sake of it: they want their banking to relate to their lives.

For example, they might want to buy a car or a home, and what they then need from their bank is insights into whether they have the resources to do this – and failing that a plan to help them achieve their financial goals over time.

SAFETY IS PARAMOUNT

Last but not least, to cement their value in the digital world, banks must provide and ensure the highest levels of security. The environment in which they and their customers operate is transitioning from a closed system to an open platform. PSD2 and the connectivity required for open banking are predicated on the use of open APIs connecting the systems of TPPs and banks, and the regulation – and the customers – clearly expect the banks to make sure all this works in a secure way.

Maintaining security in an open ecosystem powered by open APIs will be challenging but essential for banks to reassure their customers that whatever the sexy new entrants are doing, their trusty banks are keeping their money safe.

In light of what banks must do to remain relevant to their customers it is not difficult to see that digital identity ticks all the boxes.

Safe, streamlined digital identity services are what will enable customers to easily and safely access all the different providers in their ecosystem, at the same time enabling connections between all the sources of information banks will need to deliver integrated financial information and products to support their customers' lifestyle choices.

Safe, streamlined digital identity services are what will enable customers to confidently use the mobile channel to interact with the connected world.

Safe, streamlined digital identity services are what will underpin online security in digital ecosystems.

Overall, leadership in digital identity is key to empowering banks to deliver the customer-driven, mobile, innovative and secure services they need to offer, in order to keep hold of existing customers and pick up new ones in an ever-more aggressively competitive banking landscape.

At the same time, digital identity could also present a new source of revenue to compensate for any losses as the new competition starts to bite.

04

HAVE BANKS REALISED THE POWER OF DIGITAL IDENTITY YET?

During recent months, we have seen a number of bank-driven initiatives in the digital identity space.

For example, in Canada, Bank of Montreal, Canadian Imperial Bank of Commerce, Desjardins Group, Royal Bank of Canada, Scotiabank and TD Bank are making good progress with the implementation of an identity solution running on blockchain – designed to enable customers to use an app to verify their identity to anyone in such a way that the service provider sees only what it needs to see, with all other personal information remaining private.

Meanwhile, the US unit of Spanish banking giant BBVA – BBVA Compass – has developed an authentication and tokenisation process to enable its account holders to make payments using third party apps without having to provide sensitive bank account information or credentials to any such third party.

In the UK, customers registered for Barclays online banking can now use this log-on as part of the UK Government's GOV.UK Verify registration process, which helps customers by pre-filling forms.

The Commonwealth Bank of Australia (CBA) has teamed with outsourcing company Airtasker to provide it with an identity verification function for its online platform. The "CommBank Identified" badge is added to the customer's Airtasker profile if the name and date of birth held by CBA match those listed on Airtasker.

For its part, USAA is partnering with a government agency on a project to allow USAA's 10.7 million members to authenticate themselves using the same username and password as for online banking.

Also in the fray, Capital One is using a digital identity API to allow websites and apps to authenticate the identity of their customers against the identity information stored by their banks. Instead of entering name, address and birthdate when registering for new accounts, Capital One customers will be able to enter their bank account information instead, and the bank will share the customer's verified identity information instantly and securely.

In short, federated identity systems enable customers to reuse credentials at multiple sites. Users can log in on one website and then access others without having to create another profile or type another username and password each time. The other sites trust that the identity provider has authenticated the user to a certain standard.

Logic suggests that banks' historical position of trust fits them well to provide federated identity systems – bringing advantages not just to customers but to the banks themselves.

Regulators increasingly require banks to do greater due diligence on their customers to screen for money laundering, and this cost banks money and time. In so far as federated identity systems increase security by limiting the passing around of personal information and minimising the opportunities for criminals to hack into customers' accounts, they would also save banks some of the time and money they spend investigating fraud cases, and the cost of reimbursing impacted customers.

As we have seen, banks are already trying their hands in this business. Representing a possible new business stream in the post-PSD2 world, digital identity solutions could offer a way for banks to monetise the considerable work they do already in vetting customers, by selling identity verification services to other businesses.

"The Commonwealth Bank of Australia (CBA) has teamed with outsourcing company Airtasker to provide it with an identity verification function for its online platform. The "CommBank Identified" badge is added to the customer's Airtasker profile if the name and date of birth held by CBA match those listed on Airtasker."

05
SO WHAT'S THE PROBLEM?

Perhaps the biggest is liability. When – if – something goes wrong, who is culpable? What happens if a bank says an actor is good when he is bad? Many banks have learned to their cost exactly what happens when they breach anti-money laundering (AML) and know your customer (KYC) rules: very big fines.

It's also important to remember that digital identities are vulnerable to hacking, social engineering and even basic errors, which happen just as frequently in the digital world as they do in the paper world – and because they touch databases, those errors can be multiplied by millions.

Recent headlines about data breaches and government snooping could also put consumers off the idea of having all their data stored in one place, no matter how well protected, and indeed the consumer mindset is a potentially major hurdle to be overcome in the race to crack digital identity.

We know what we mean by identity in the analogue world. Translating this concept into the digital world – and grasping the fact that different data attributes are used in different circumstances – could take time, as could consumers shifting the way they think about their banks, from guardians of what they earn to guardians of who they are.

Banks have traditionally been custodians of data, as they collect and verify identities when customers transact with them, and they also have established cross-border operations. They are clearly very well positioned to play a leading role in digital identity, acknowledging that there remain a number of challenges to overcome and questions to answer en route.

06

WHAT ASSETS DO BANKS BRING TO THE DIGITAL IDENTITY PARTY, AND HOW CAN THEY PRESS HOME THEIR ADVANTAGE?

The main asset banks have is their history of dealing with us, their customers. They know a great deal about our lives. They know what we earn and what we spend. They have more than enough information on us to aggregate it to build a digital identity.

Another plus is that banks' data on their customers is typically very good. Today's AML and KYC rules demand that banks maintain high standards for identity verification of new and existing customers.

In addition to this regulatory pressure, banks are also naturally incentivised to collect accurate data because the viability of their businesses depend on it. Banks cannot open an account or approve a mortgage if they do not have accurate information about the applicant's income, credit worthiness or employment.

As well as data and strength in compliance and data accuracy, banks also have trust, as previously discussed and, often, the cross-border infrastructure required to underpin digital identity solutions.

Critically, the demands being placed on banks by the very changes that are forcing them to look for alternative sources of revenue also strengthen the banks' hand when it comes to digital identity. Key to this is not so much controlling digital identities – the prevailing wisdom is that digital identities are best controlled by customers themselves – as the authentication role.

In Europe, under PSD2, the spotlight is on banks to ensure Strong Customer Authentication for all remote access to customer accounts, based on two-factor authentication (something the customer is, something the customer has and something the customer knows).

This rigour – this demand for instant validation of identity – is part of a journey the banks have travelled in recent times, evolving from authentication based only on face-to-face meetings in the branch, through authentication in the context of multi-channel and omni-channel banking interactions, towards multi-factor authentication to protect consumers and transactions in an open API-driven digital ecosystem.

Based on this rich background in authentication, the next logical step for banks is the 'platformification' of their expertise, under which they could share their authentication capabilities across not only the financial ecosystem, but the full connected world.

"The demands being placed on banks by the very changes that are forcing them to look for alternative sources of revenue also strengthen the banks' hand when it comes to digital identity. Key to this is not so much controlling digital identities – the prevailing wisdom is that digital identities are best controlled by customers themselves – as the authentication role."

07

CONCLUSION: OPEN BANKING, KEY THREAT AND KEY OPPORTUNITY FOR BANKS

Open banking is creating a competitive imperative for banks to seek new sources of revenue and new business models – but as well as representing a critical threat for banks, open banking also presents an exciting opportunity for them, by strengthening their credentials as authentication and identity providers in a world crying out for the digital identity problem to be solved.

As this paper has argued, the case for banks to be the main point of contact for authentication and identification in the connected world is a powerful one.

Banks need only build on their existing strengths – trust, infrastructure, customer data and regulatory compliance – to position themselves convincingly in this role within the financial ecosystem first.

Indeed, this is already happening: in addition to the bank initiatives in digital identity outlined above, just think how many of today's fintechs rely on established banks to identify and authenticate users.

Banks can also think bigger, however, and extend their existing expertise in authentication – being honed anyway by more demanding compliance requirements (eg PSD2) even further, to position themselves as the identification gateway to the entire digital world.

If identity is the new money, then the new banking is surely digital identity management, and banks have all the assets required to make a success of this new business model, turning the potential negative of PSD2 into a positive, and carving out new sources of revenue – and relevance – in the digital ecosystems of the future.

08 ABOUT

Finextra

This report is published by Finextra Research.

Finextra Research is the world's leading specialist financial technology (fintech) news and information source. Finextra offers over 100,000 fintech news, features and TV content items to visitors to www.finextra.com. Founded in 1999, Finextra Research covers all aspects of financial technology innovation and operation involving banks, institutions and vendor organisations within the wholesale and retail banking, payments and cards sectors worldwide.

Finextra's unique global community consists of over 30,000 fintech professionals working inside banks and financial institutions, specialist fintech application and service providers, consulting organisations and mainstream technology providers. The Finextra community actively participate in posting their opinions and comments on the evolution of fintech. In addition, they contribute information and data to Finextra surveys and reports.

For more information:
Visit www.finextra.com, follow @finextra,
contact contact@finextra.com
or call +44 (0)20 3100 3670

HID GLOBAL

HID Global powers the trusted identities of the world's people, places and things. We make it possible for people to transact safely, work productively and travel freely. Our trusted identity solutions give people convenient access to physical and digital places and connect things that can be identified, verified and tracked digitally. Millions of people around the world use HID products and services to navigate their everyday lives, and over 2 billion things are connected through HID technology. We work with governments, educational institutions, hospitals, financial institutions, industrial businesses and some of the most innovative companies on the planet. Headquartered in Austin, Texas, HID Global has over 3,000 employees worldwide and operates international offices that support more than 100 countries. HID Globa[l®] is an ASSA ABLOY Group brand. For more information,

For more information:
Visit www.hidglobal.com

Finextra Research Ltd
1 Gresham Street
London
EC2V 7BX
United Kingdom

Telephone
+44 (0)20 3100 3670

Email
contact@finextra.com

Web
www.finextra.com