



Want to retain customer loyalty in an Open Banking world?
Start by building trusted digital relationships.

To differentiate in an Open Banking world, financial institutions must optimize the customer journey. This starts by creating an experience that makes it safe for people to bank.

There are few industries that understand the effects of disintermediation as well as the financial services sector. As new entrants crop up on an almost-monthly basis, the world's banks find themselves ceding market share to a growing number of non-traditional banking institutions, captive finance companies, and fintech firms.

It's a slow slide that will only accelerate as Open Banking becomes more prevalent. With consumers gaining greater ability to access the financial services of their choice through one trusted provider, banks may be on the cusp of losing their central position in the chain of finance. Back in 1994, Bill Gates said, "Banking is necessary, banks are not." As we crest into the digital century, consumers are poised to turn that prediction into reality.

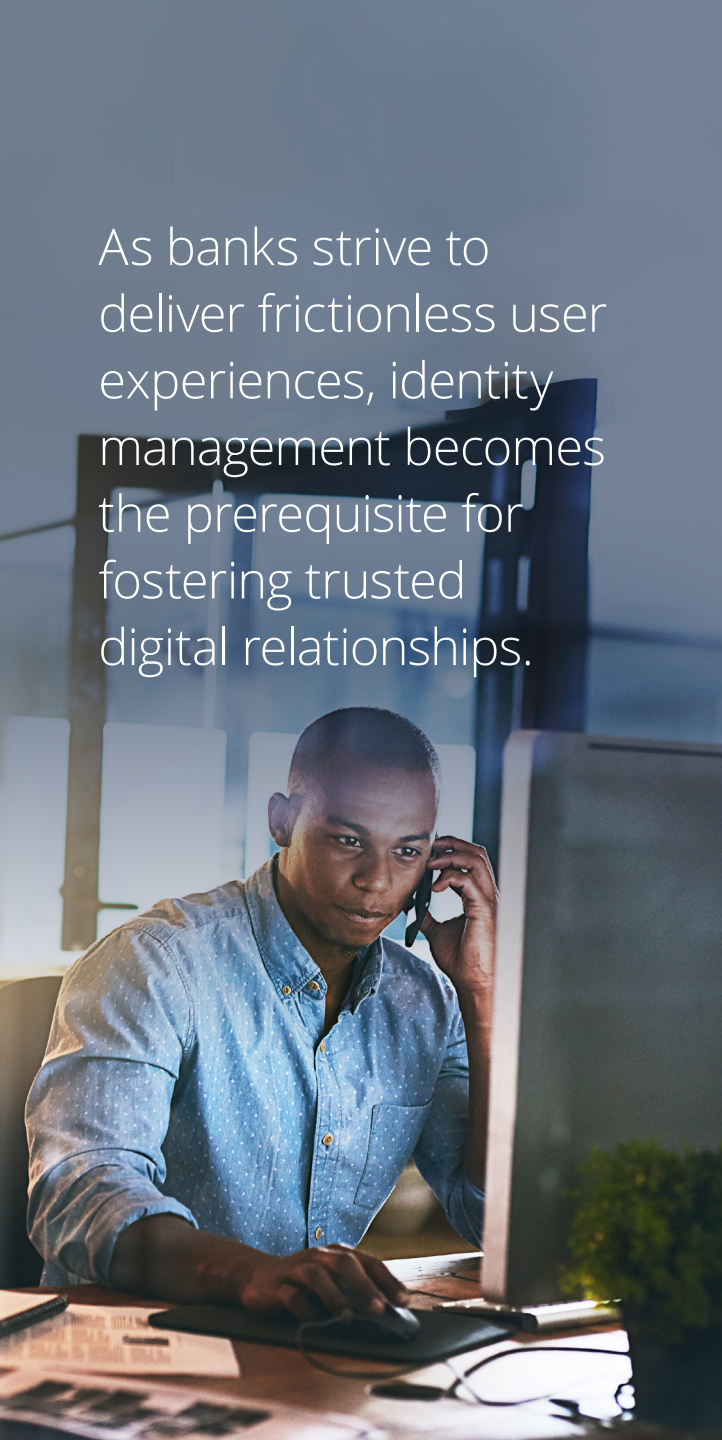
In the face of this existential crisis, banks are coming to realize that the only way to maintain market share is by creating a truly unparalleled customer experience. To make it easy for people to access the right services at the right

time, banks are leveraging the data at their disposal to create hyper-personalized customer journeys. Doing this effectively, however, requires them to systematically build trust by protecting their customers' data and identities.

While trust may seem like a nebulous concept, it has in fact become a rallying call in recent years. Consumers have become increasingly vocal in their demands that businesses and governments alike adhere to the highest standards of integrity. This has seen investors in numerous industries refusing to advance funds unless companies can demonstrate a meaningful commitment to the principles society holds dear.

For financial institutions, this means protecting what stakeholders value most. This is what cybersecurity is ultimately about—not a mere technological mandate, but a systemic promise to create an environment that makes it safe for people to bank. In many ways, this starts with identity management.





As banks strive to deliver frictionless user experiences, identity management becomes the prerequisite for fostering trusted digital relationships.

Digital identity and the future of banking

While not all banks currently consider identity management a strategic competency, it will likely form the backbone of the industry in the next five to 10 years. That's because digital identities are at the heart of any organization's ability to execute its strategy and leverage digitization effectively and responsibly.

This is true in several regards. For instance, Open Banking can only fulfil its potential if consumers can be digitally verified and authenticated. Banks that make that process too difficult may see higher rates of consumer abandonment. Banks that make it too easy, however, heighten the risk of cyberattack—a risk that threatens to cascade across multiple providers, leading to reputational damage and lowered consumer confidence in Open Banking products overall.

Identity management also plays a role in banks' efforts to safeguard consumer data when gathering marketing intelligence. Although this information is critical for organizations looking to personalize the customer experience, a 2019 poll of 4,000 global consumers showed that trust quickly erodes if people believe organizations are directly profiting from their data. This calls for an exquisite balancing act between customer experience and customer trust.

Some banks have even begun partnering with their peers—often through national banking associations—to offer true digital identity services. Executed effectively, these services can generate new streams of revenue, ranging from transactional fees earned through various digital commerce channels to fees earned from third parties interested in accessing the bank's know your customer (KYC) data (presuming customers have provided explicit consent). Should these services gain traction, banks have a unique opportunity to turn digital identity from a liability into a profit-generating activity.

Yet, despite its strategic role, identity management is unlikely to become a differentiator in itself. That's not only because it must become table stakes for the financial services industry as a whole. It's also because identity management only comes to the fore of the consumer conversation when security is breached—and no one wants the loss of trust to be a differentiator.

This means banks must look beyond identity management in their quest to retain customer loyalty. They must also take steps to safeguard consumer privacy, prevent the incidence of fraud, strengthen regulatory compliance,

improve internal governance, and develop a change management program capable of driving the cultural shifts necessary to meet the evolving needs of today's ever more sophisticated consumers. Only by adopting a business model that connects these dots can banks hope to unlock the promise of the future of banking.

Charting the way forward

Banks unquestionably have their work cut out for them as they seek to address the disruptive forces altering industry dynamics. Amid this volatility, however, there is one end goal they must bear in mind: to always and effectively protect the consumer.

By creating a safe and secure experience, banks have the opportunity to once again become their customers' most trusted brand. They could even leverage this trusted position to seamlessly integrate their digital identity capabilities with other ecosystem players, beyond the scope of traditional banking. Can banks ultimately become agents of disintermediation themselves by assuming the role of global identity protectors? Only time will tell.

¹ Deloitte Insights, October 16, 2019. "Are you a trust buster or builder?" <https://www2.deloitte.com/us/en/insights/topics/marketing-and-sales-operations/global-marketing-trends/2020/safeguarding-trust.html>

Authors and contacts



Nick Seaver | Global Cyber FSI Leader

nseaver@deloitte.co.uk



Mike Wyatt | Global Cyber Identity Leader

miwyatt@deloitte.com



Mark Nicholson | US Cyber FSI Leader

manicholson@deloitte.com



Jan Vanhaecht | NSE Leader Identity Services

Belgian Cyber Secure domain leader

jvanhaecht@deloitte.com

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the “Deloitte” name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.