Building the banks of the future

Table of Contents

The role of trust amid the seismic shifts occurring in banking was examined in "Trust and the Future of Banking". This e-Book now turns to the technologies and solutions that will help financial institutions get there.

What might the future look like for a typical small business banking customer?

The year is 2030 and Amina is reviewing the end-of-year accounts for her growing eco-travel consultancy. As the bullet train hurtles through the French countryside, her AI accountant, informs her that having just analyzed all transactions for the past three years against multiple different accounting models, there is one option that could reduce her tax bill by up to 11% for the coming financial year.

It has also suggested some changes to payment scheduling that could dramatically improve cash flow, and by cross referencing her personal accounts (held with one of the new FinTechs - FinSocial.com) has highlighted some living expenses that could be offset against her business income for further tax efficiency.

As the train enters one of the first tunnels cutting through the French Alps, she dons her virtual reality glasses and after a brief consultation with the manager of her high-street business bank, tells the AI to proceed immediately with all necessary changes.

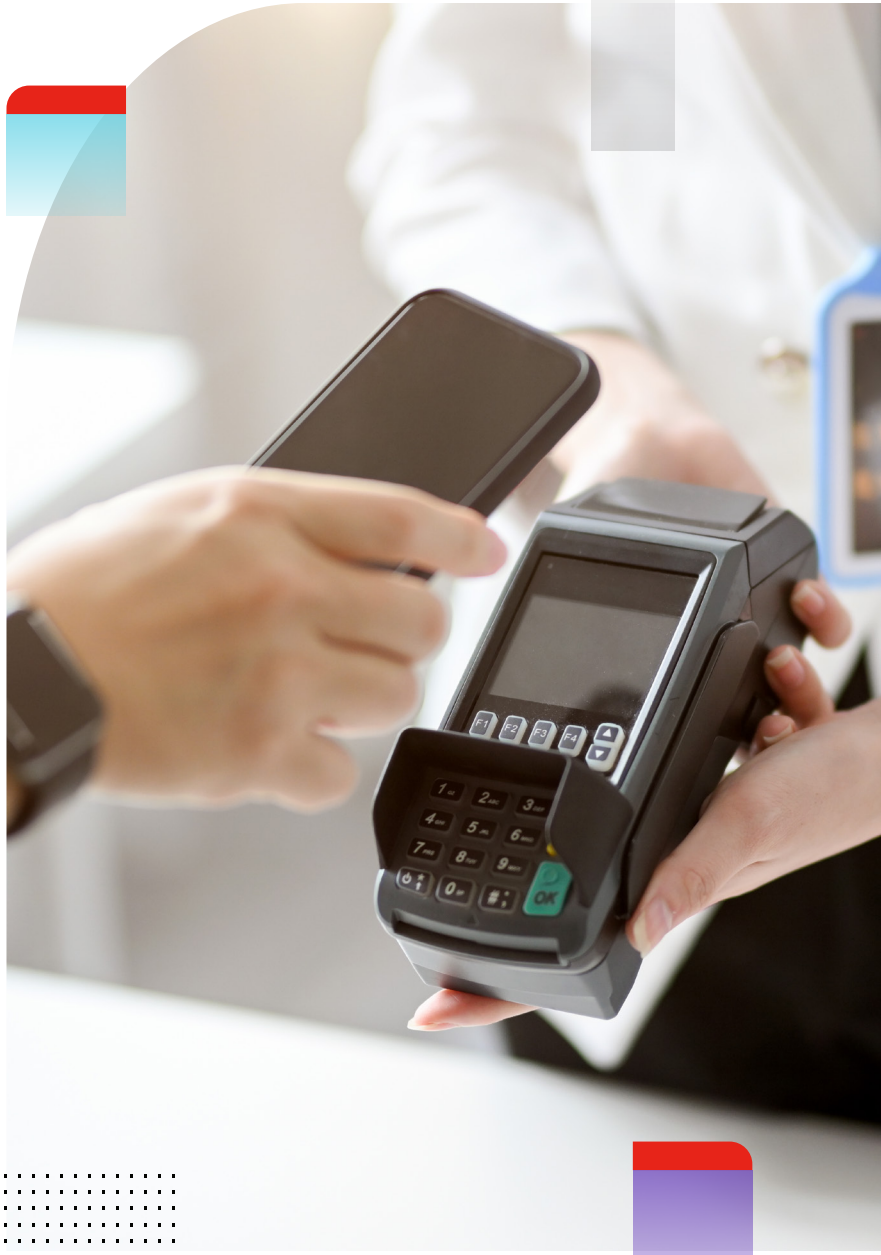
"That'll more than pay for my annual skiing holiday," she muses, reclining her chair and turning to the snow-capped mountains now coming into view.

From Dreams to Reality

While this imagined scenario might seem somewhat fanciful compared to the current reality, it is all based on trends and technology that are already playing a role in today's financial systems.

One of the most significant of these is the open banking initiative and associated Payment Services Directive 2 – (PSD2), which by granting access to customer transactions through open APIs, looks set to spawn a thriving new marketplace in value-added digital financial services, the first of which are already emerging.

As these services mature, the current migration from large monolithic IT systems to agile assemblies of modular services will accelerate, and providers able to take advantage of this trend will be giving customers what they desire most of all: complete visibility and control over their finances. As a result, they will be able to build levels of trust and loyalty not seen in the banking world for decades.



And it isn't just the private sector with eyes on the prize. In 2020, the UK's Revenue and Customs department (HMRC) invited "suppliers, including those from the financial industry & FinTechs, to contribute to building [their] knowledge regarding the possibility of using real-time transaction data in banking products for streamlined tax determination, automatic calculation, and payment to HMRC, simplifying this process for taxpayers."

Couple this with recent advances in machine learning (ML) and artificial intelligence (AI), and the arrival of new virtual services as powerful as Amina's AI accountant in the scenario above, seem only a matter of time.

With the long-awaited rollout of affordable 5G mobile data services and a rapidly expanding edge-computing infrastructure, consumers will soon have wire-speed, low-latency access to data and services from virtually anywhere on the planet.

Today, most of us are all too aware (sometimes painfully so) of our connection to data, applications, and services. It's a consideration that impacts where we live, where we set up shop, and even where we spend our leisure time.

But all these considerations will soon be as redundant as worrying where the electricity comes from when we turn on the light. We just assume that it will work and for the most part, it does.

So, whether at home, in the office, or entering an alpine tunnel on a high-speed train, data will continue to flow seamlessly and with no discernable interruption as we pass from WIFI to public 5G to private 5G and back to WIFI again. Of course, under the hood, there will be rapid, complex negotiations to establish authentication, authorization, data privacy, and quality of service etc., but all of this should be invisible to the user.

And while widespread adoption of remote digital, multimedia banking services may have seemed some way off only a few years ago, the recent global pandemic has propelled us all from early-adopters to early-majority in just two short years, effectively leap-frogging Geoffrey Moore's famous chasm.

The use of video conferencing skyrocketed during the pandemic, initially sparked by government work-from-home mandates across the globe, but then gaining a momentum of its own as the technology became accepted as part of the 'new normal'. This rapid uptake in multimedia communications has driven increased investment and innovation in new solutions, which in turn is fueling yet greater acceptance and adoption.

As COVID first took hold, regulators and banks worked together to support greater availability of digital and video services so customers could continue banking. For some banks this led to a 400% increase in client video calls within just the first three months of the pandemic, and the growing consensus seems to indicate that this trend will continue long after we have all learned to live with COVID.

And finally, assuming that the banking landscape of 2030 will include FinTechs (the progeny of Finance and Silicon Valley Big Tech), it seems probable that current hype surrounding the 'Metaverse' (where video gives way to more fully immersive virtual reality), will also play a role in the financial services of the future.

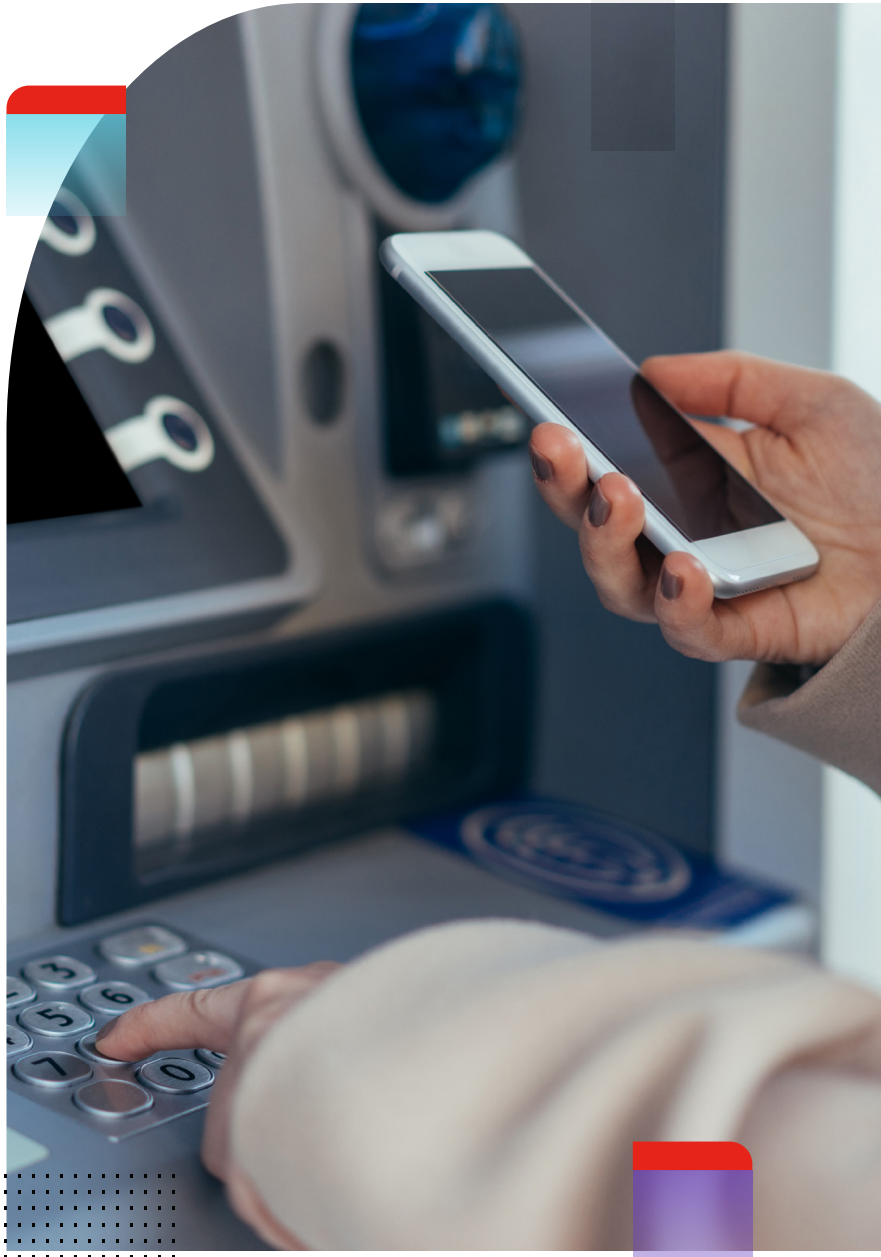
The Building Blocks Available Today

Of course, the availability of a technology and its successful implementation within the business are often two very different things, and the transition from legacy mainframe-based banking systems to more agile, cloud-based infrastructures is a case in point.

For most banks, the transition will be gradual, resource intensive, and result in a complex mix of in-house and cloud services - often from multiple cloud service providers.

And complexity, in addition to being a drain on resources, is the enemy of security.

Each cloud service provider will likely do a reasonable job of protecting their infrastructure, but securing the data and workloads usually remains the responsibility of the bank. And while providers may offer a range of tools to help achieve this, the scope of these will be limited to that part of the infrastructure and may not integrate well with the rest of the bank's security framework.



Without a single, comprehensive overview of what's happening across the entire infrastructure, configuration errors and vulnerabilities will inevitably creep in unnoticed, and some proportion of cyberattacks will be missed.

In addition to increased complexity, the transition to cloud renders the old notion of a secure perimeter around central resources redundant, while the potential surface area exposed to cyberattack is greatly expanded.

The transition to cloud is often accompanied by a migration of wide area networks, traditionally using Multi-protocol Label Switching (MPLS), to software-defined WANs (SD-WANs), onto which network access may be further extended through WIFI and 5G mobile.

SD-WANs can improve performance of cloud-based applications since user data no longer has to be backhauled through the central datacenter, and since local Internet connectivity is usually significantly less expensive than MPLS, there is the added incentive of cost reduction, though very often, organizations choose to use this as an opportunity increase resilience and performance by load-balancing across dual links.

But once again, both SD-WAN and the extension of access through WIFI and mobile also lead to increased complexity and an expansion of the potential attack surface.

With the increased complexity of these new environments, building defense in the traditional way – by adding yet more security point products - soon becomes unmanageable – especially given the current industry-wide skills shortage.

Instead, what's needed is a more joined-up approach in which security components collaborate in real time, making use of machine-learning and artificial intelligence to correlate and detect trends in the huge volumes of traffic data, and to automate some of the previously manual tasks. The combination of meaningful data intelligence and automation can ease the administrative burden for already-stretched security teams, reduce costs, and provide the broad end-to-end visibility and control that is vital for effective infrastructure management.

This approach, already exemplified in the Fortinet Security Fabric, is referred to by analyst firm, Gartner, as a 'Cybersecurity Mesh', and listed as one of their Top Strategic Technology Trends for 2022.

One way to overcome the challenge of the expanding attack surface is to change our concept of user trust. Rather than the traditional model of authenticating at the perimeter and then trusting the remainder of that user's session, we employ a 'Zero Trust' approach and reestablish authentication and authorization for each new network connection.

But the general concept of Zero Trust should not be confused with its technological manifestations such as Zero Trust Network Access (ZTNA), which provides a practical solution for establishing a logical access boundary around an application or set of applications to shield them from public visibility, and thereby shrink the potential attack surface.

Conclusion

The past two decades have seen the word of financial services shaken up and turned on its head. The birth of the digital economy, a global financial crisis, a raft of disruptive new technologies, regulations, and to cap it all, a global pandemic, have changed the face of banking forever.

And as if that wasn't already enough of a challenge, the continually shifting minefield of cybercrime through which banks must now navigate a safe path to the future, is also evolving at breakneck speed as malicious actors deploy some of the very same technological innovations used by banks such as AI and ML to create ever more advanced threats.

But with concepts such as Gartner's Cybersecurity Mesh to counter the escalating complexity of security management, combined with intelligent automation, and a redefinition of user trust, there exists a navigable path to the future glimpsed at the outset.

Not all of today's financial services providers will succeed, but the potential gains for those that do will be enormous. Amina and millions more like her are already looking for tomorrow's banking services. The future will belong to those who can build the organization best able to deliver them.

[1] Open Banking App Store

[2] Tax-Compliant Banking Products Exploration and Proof of Concept (POC)

[3] Crossing the Chasm

[4] How banking will change after COVID-19

[5] The State of Video Banking for 2022

[6] Top Strategic Technology Trends for 2022: Cybersecurity Mesh

www.fortinet.com

May 9, 2022 9:24 AM

ebook-building-bank-future

1579799-0-0-EN