Crossing the digital threshold
Identity and access innovation in financial services
01 Entering a new era

08 Securing the way

14 The path beyond

20 Crossing the threshold
Entering a new era

The financial services industry is changing rapidly as digital transformation enables new possibilities and changes the way we access our banks, engage with insurance companies, and interact with capital markets firms.

Financial platforms and services are increasingly able to integrate with every facet of an individual’s life. This increased access also means more data—and a greater need for trust between companies and customers that this data will be safe. Financial service providers must continue to increase their security and privacy abilities to meet these requirements.
New financial technology firms (sometimes referred to as fintechs) are disrupting the model of traditional financial service providers by taking advantage of new technologies and increasing amounts of accessible data to deliver an enhanced customer experience. These digital disruptions to traditional models have led to the creation of new technologies such as decentralized identity, which have the potential to alter the industry’s paradigm further. With more and more of our work and even our personal lives happening in the digital space, this innovation shows no signs of slowing down.

Due to continuing evolution in technology and digital services, operational resilience is crucial to companies today, enabling them to adapt to changing business conditions. Remote workers are increasingly driving the need for anywhere, anytime access. Between 2005 and 2017, there was a 159 percent increase in remote work worldwide (Flexjobs and Global Workplace Analytics Report, 2019), and the global onset of COVID-19 in 2020 has further accelerated this trend by heightening expectations for remote access across all industries for both employees and customers. At Microsoft, we’ve heard from customers
around the world that this crisis has accelerated a shift to a new era—one in which digital transactions are essential, and digital transformation must no longer be an ambition to be put off until tomorrow.

With increasing competition from new, digitally agile, financial technology firms—capable of setting up customers in seconds through quick digital onboarding experiences—banks and other financial service providers have been scrambling to keep pace. The variety of options for consumers and the accompanying ease of signing up has significantly lowered the cost of switching, forcing the industry to ramp up the integration of digital services.

This contest between traditional providers and new financial technology firms has resulted in expanding cloud ecosystems for financial services. The services that form these ecosystems are customer-centric and can offer unified value propositions that extend far beyond past financial service offerings to reduce customer costs, increase convenience, and provide new tools and services.
With 57 percent trust among the general population, financial services were the least-trusted industry measured.

*Edelman Trust Barometer, 2019*

These services are also leading to the creation of large, richly varied pools of data, that companies can use to target new offerings and services effectively.

To compete, traditional financial institutions need to enable their own digital ecosystems by integrating third-party services, improving customer onboarding, and delivering differentiated customer experiences. To do that in the cloud, they need safe and secure digital identity.
Managing identity and access in the cloud

Identity management is crucial to delivering digital services. Financial institutions must be able to verify users are who they say they are, as well as the level of access for which they are authorized. Identity platforms underpin our digital world and enable customers to access services remotely.
In an environment where customers expect a secure, unified, and seamless sign-on experience—and, further, where financial institutions need to foster partner ecosystems to deliver new products and services with greater agility—the imperative of transforming identity and access management has never been clearer. Institutions are looking for enhanced levels of security, faster rollout of new capabilities, scaling across the enterprise, and delivering better, easier-to-use products and services to their customers. On-premises identity solutions are simply inadequate.

Consider some of the downsides of on-premises identity—it often requires frequent and costly upgrades to meet security standards and remain compliant, sometimes involving equipment installation across multiple locations. Another concern for on-premises identity is that customers are increasingly accustomed to cloud-enabled concepts such as bring your own identity (BYOI), which allows users to select and use digital IDs (such as their social identity) to access multiple digital services, reshaping user expectations about seamless access and signup.

In contrast, digital identity effectively meets the needs of both institutions and customers by providing remote updates, efficient scaling, and seamless sign-on—all while potentially lowering costs. These advantages are particularly distinct when delivered by an identity-as-a-service (IDaaS) provider. By choosing a centralized cloud-based or hybrid identity service, companies create a single access point that is significantly easier to control and secure when compared to using multiple solutions, while also offloading the burden of managing access from internal IT departments to a managed service provider.
Partnering for the future

Financial institutions are traditionally trusted providers of identity with a system built on confidence. If a financial service provider’s security or reputation is lacking, business suffers. People must trust that financial institutions will keep their money as well as their personal data secure while also providing systems that are simple to use. Providing the best form of authentication and customer identification is increasingly vital as cloud-first financial technology firms and other businesses progressively partner with banks to access vast amounts of data to deliver more customized services. By taking advantage of this data, financial institutions are now able to provide superior user experiences and new services ranging from crowdfunding to tailored and integrated budgeting apps. The use of application program interfaces (APIs) to enable the creation of these applications and services around financial institutions has spurred the development of an open banking ecosystem which provides users with a wider array of services and financial transparency options. Successfully enabling this ecosystem requires a secure, simple, and unified authentication experience.
Securing the way

Financial service providers and the digital world at large are seeing an increasing number of cyber-attacks. While cloud computing has enabled vast transformations in the way society collaborates, does business, and otherwise interacts, it has also given bad actors the ability to massively scale their attack potential. Identity forms the control point of security. With attackers increasingly targeting users through credential spoofing, modernizing identity provides a strong return on investment by helping prevent breaches and improving ease of use for both administrators and consumers.
The cost of data breaches

Global cyber incident costs reached a record high in 2019, with an average cost of $3.92 million and the biggest breaches topping $42 million.

Security Intelligence 2019 Cost of Data Breach Report
In 2019, while finance and payment companies saw the largest drop in share performance post-breach, prices fell 7.27% on average after a breach.

*Comparitech, 2020*

Consumers expect banks to respond to breaches faster than other companies: two out of every three customers surveyed would leave their bank if their breach response was slow or ineffective.

*Banking Dive, 2020*

The global cost of cybercrime, $3 trillion in 2015, is expected to exceed $6 trillion per year by 2021.

*Cybersecurity Ventures, 2019*

The cost of cyberattacks is highest in the banking industry, reaching $18.3 million annually per company.

*Accenture, 2019*

83% of respondents said they expect to be notified within 24 hours if the breached company is a bank.

*Banking Dive, 2020*
The core security threats we see affecting customers in financial services include account takeover, ransomware, data targeting, legacy systems, and financial crime.

- **Account takeover.** Attackers are using a variety of techniques to target account credentials. Yet phishing attacks, ranging from simple to sophisticated, are still by far the most common with **inbound phishing emails having increased by 250 percent in 2018** (Microsoft Security Intelligence Report V24, 2019).

- **Ransomware:** Ransomware attacks are growing in sophistication as well as severity, with attackers assisting and guiding semi-automated systems in targeted attacks as well as broader automated efforts. Organizations pay a massive price in both downtime and often in ransom to recover their data.

- **Targeting data.** Cybercriminals have recognized that the immense stores of data produced in the digital open banking ecosystem are a lucrative target. Financial institutions need to be careful to protect this trove of valuable data.

- **Legacy systems.** Legacy systems are usually at the highest risk of being breached. As financial institutions try to integrate into the cloud-first world, legacy systems create negative user experiences and expose financial service providers to attacks. Properly patched and updated systems with centralized access management and risk mitigation controls can alleviate or thwart many potential attacks.

- **Financial crime.** Fraud and other forms of financial crime—such as money laundering, counterfeiting, and identity theft—are a fact of life for financial services, and they must be continually identified and mitigated.

The need for constant vigilance against security threats such as these is especially acute during times of financial system-wide strain: the onset of COVID-19 in 2020 has led to increased vulnerability to cyber-attacks and financial crime through both the exploitation of fear and the stress placed on the workforce of financial institutions (Financial Action Task Force, May 2020). By making security improvements such as multi-factor authentication for digital banking and by upgrading their security postures, financial institutions can protect both themselves and their customers. It is also crucial that financial institutions effectively scale and speedily implement these security solutions to assess the increasing amounts of data available to them and identify suspicious activity, otherwise they risk losing customers due to the theft of sensitive information.
Challenges to identity evolution

While banks have traditionally been innovators, specialized financial technology firms are challenging incumbents’ reputation in this regard by driving continuous improvement in the financial services available to individual and institutional customers.
The growing trend of specialized financial service technology providers has given consumers options and created new opportunities, but not without pitfalls such as:

- **Cumbersome security requirements.** While multi-factor authentication reduces the risk of attacks by 99.9 percent (Azure Active Directory Identity Blog, 2019), it can also prove cumbersome for some users. This is particularly true of senior citizens, who sometimes lack familiarity with emerging technology and may face personal mobility challenges. These challenges create issues with fraud protection and remote access for a population that broadly needs both. Ease of use for security systems such as multi-factor authentication is crucial, especially with increased competition in the financial services industry.

- **Low innovation uptake.** Some regions and financial institutions have been quick to take advantage of security advances; however, at times, there have been major issues with adoption. For example, 3-Domain Secure (3DS1) has been a useful innovation for securing online payments around the world and yet has had regional issues with adoption due to user confusion and negative user experiences, leading to high levels of transaction abandonment. This dissonance has led many companies to avoid the technology.

- **Integration with legacy systems.** Banks and other financial institutions have traditionally provided identity management, securely tracking their customers’ identities as custodians of their legacy systems. However, integrating legacy systems with cloud-based security has often proved challenging. Integration as part of a cloud transition is nonetheless essential if organizations are to succeed in the digital era.
The path beyond

As financial institutions and technology firms consider the future of cybersecurity and identity, they need to take note of the challenges that the industry is facing and move to address them while meeting customer needs.

It should be clear by now that achieving these goals requires a secure, cloud-based identity platform. And this platform must be able to easily integrate future security innovations, scale them quickly, and fight financial crime—all while providing a stellar customer experience. Scaling securely is a massive challenge for many organizations, and partnering with large-scale, cloud service providers is crucial to success.
Financial institutions are moving a step forward in creating a more secure banking environment by enabling multi-factor authentication, checking identities through text messaging, e-mail, or call verification. Some are also enabling access to online services by means of unique codes from multi-factor authenticator apps or biometric authentication used in their banking apps. However, if they are unable to easily integrate future innovations, they’ll soon be left behind. Cybersecurity is continually evolving, and passwordless access is a must in today’s environment. Cutting-edge firms like Microsoft partner Trusona are leading the way by providing secure, passwordless access through scannable QR codes and more. By removing passwords that are often duplicated, stolen, and otherwise breached, there is an opportunity to increase security while also providing a seamless and uncomplicated customer experience.

“By 2022, 60% of large and global enterprises, and 90% of midsize enterprises, will implement passwordless methods.”

Gartner

*Embrace a Passwordless Approach to Improve Security, 2019*
The next steps of identity innovation

There are many identity technology possibilities other than QR codes that firms will need to integrate as the digital enterprise continues to mature. Decentralized identities, for one, show promise in protecting individuals from fraud, breaches, and theft. They also offer opportunities for self-sovereign identity (SSI)—the idea that individuals should own and control their own identity. This approach to self-identification is a growing phenomenon in some parts of the digital world. Portable cards that issue and verify someone’s identity and then apply it to the matching authorizations of a given service also form a new means of authentication.

Another way to modernize identity and enable tomorrow’s innovations is by embracing single sign-on for business banking services. With evolving digital ecosystems and the growing expectation among customers for efficient access to new tools, single sign-on enables not just current services but also prepares the way for future innovations.

The trusted identity providers of the financial services industry have a significant opportunity to improve customer experience and engage new customers if they maintain positive user experiences and security while simultaneously scaling innovative solutions. With artificial intelligence (AI) and machine learning (ML) taking an increasingly important role, a plethora of new technology ideas are sure to follow.
Fighting financial crime with AI-secured, multi-factor authentication

One such evolving innovation is the use of AI- and ML-based models in securing identity authentication.

Securing identity has a natural impact on decreasing fraud by verifying if someone is who they say they are. However, this effort has become increasingly challenging
in a digital space where businesses may deal with many customers whom their employees have never met and will never see in person. Using AI- and ML-based models can help forward-thinking financial institutions stop malicious actors before they compromise critical systems or access sensitive data. After taking in authentication, transaction, and other forms of data from a variety of systems, these algorithms can make ML-informed fraud determinations that block suspicious access and transactions.

Multi-factor authentication until now has typically involved verifying identity along three vertices: something users know (like a password); something they have (like a phone); or something physically unique about them (such as a fingerprint). ML-based determinations are enabling a new, fourth form of multi-factor authentication that is increasingly used to fight compromised identity and fraud: authenticating identity through analysis of what someone is doing. Successful identity verification is thus moving to include behavioral modeling as a means of identifying suspicious trends over time or unusual actions in a user’s current activity.

**Tackling money laundering and more with data**

Financial institutions can now shape a more secure future by collecting and putting to work the vast amounts of disparate and disconnected data from across their organizations.

By combining this information into a data lake (a vast repository of raw data) and applying AI and machine learning, organizations can highlight suspicious activity, or networks of bad actors, with speed and accuracy not previously possible. Through the speed of computations and development of inference engines, possible only through the scale and computing power of the cloud, the financial services industry has an opportunity to fight various forms of financial crime—such as money laundering or terrorist financing—with more data, better accuracy, and improved results.
Today’s digital identity landscape is patchy, inconsistent, and what works in one country often won’t work in another. We have an opportunity to establish a system that puts people first, giving them control of their identity data and where it is used.

Ajay Bhalla
President, Cyber and Intelligence Solutions, Mastercard

*Mastercard, Microsoft join forces to advance digital identity innovations*
Crossing the threshold

Microsoft is working with our customers to prepare them for the future by addressing their security needs with scalable products and services for identity and authentication.

With cohesive digital identity that effectively authenticates and analyzes user risks, we make our identity solutions easy for both administrators and users.
Guided integration and use

We’re dedicated to making all of our solutions easy to integrate with existing partners and providers. When working with Microsoft, our customers benefit from our ability to incorporate different features across various platforms. Integration with the extensive capabilities of the Microsoft cloud can help to future-proof organizations by making it simpler and easier to enable emerging technologies.
Analyzing and managing risk

One of the ways we’re making our customers’ lives easier is by managing and mitigating operational risk. We help our customers manage their information, assess risk, and manage their technical environments. It is also essential to consider third-party risk from partners and vendors who access business systems. We’ve developed the unique ability to assign risk scores to the use of identities (whether by partners, customers, employees, or any other users) based on analyzing the massive number of security signals we receive daily and data on each user’s activities. We think about risk management and analysis in two ways in this regard:

- **User risk.** User risk represents the probability that a given identity or account is compromised. We calculate this offline using our internal and external threat intelligence in combination with other sources of information. These include security teams at Microsoft, law enforcement, security researchers, and other trusted sources. For example, we identify unusual user activity or activity that matches known attack patterns identified by our threat intelligence.

- **Sign-in risk.** We analyze each sign-in to calculate the probability that an authentication request is or is not authorized by the identity owner. This risk is calculated both in real time and offline. This analysis includes scenarios such as real-time indicators when a user signs in from locations outside their norm or offline analysis when sign-ins are coming from malware-linked IP addresses.

By using a unified identity experience, we evaluate these users and apply security policies to them based on their unique risk factors. Together, these abilities enable us to minimize our customers’ operational risks, limiting the potential hazards and uncertainties they face while providing digital continuity.

**MICROSOFT’S DATA ADVANTAGE**

At Microsoft, we collect a massive amount of telemetry data through our Microsoft Intelligence Security Graph to inform our security solutions. The graph compiles a vast array of signals from 450 billion user authentications to 400 billion emails scanned, 18 billion Bing web pages scanned, and 1.2 billion devices updated every month. This powers the machine learning models that help us to identify user risk through behavior-based authentication, perform early identification of security attacks, and more.
“In financial institutions, security and compliance in the public cloud environment are crucial and require high skills and knowledge. The access we had to Microsoft specialists—for example, interacting directly with our audit and legal personnel to confirm our full compliance—gave us the confidence to move forward and reduced the time to get regulatory approval to use confidential data in the public cloud.”

Jan Maarten de Klein
Product Development Manager, Microsoft Azure, ABN AMRO Bank

*ABN AMRO delivers industry-specific functionality in the cloud faster*
Removing roadblocks to change

We consider not only internal user experience and the experience of your own customers, but also your partner’s experience and that of your existing environment. We ensure that the services you need to run your business are available to you. With an unparalleled partner ecosystem, we know how important a secure, single sign-on experience is for your team and for your users, so we provide that, too, while meeting or exceeding privacy and security standards. This makes it easy for you to scale and deliver value for your customers while staying secure.
What’s next?

Microsoft understands that managing modern identity is a challenge for many organizations, regardless of industry. We recognize the heightened stakes for financial services firms especially.

We can empower organizations like yours to put innovation into practice using our global reach and ecosystem to deliver strategic business outcomes, maximize the value of cloud technology, and drive success through continual support. By using our ingenuity and expertise to define and deliver solutions on the Microsoft platform, we can guide your organization throughout your unique transformation journey with a program of change customized to your business needs.

Our customers push the boundaries of innovation and stay ahead of the curve by relying on our creative and resourceful experts in business and technology, vast network of partners worldwide, and preeminent customer support team—making Microsoft Services the trusted advisor for organizational and technological transformation.

Contact your Microsoft representative to learn more. For more information about consulting and support solutions from Microsoft, visit www.microsoft.com/services.
As a financial organization, we’ll never be able to build a cloud platform that can compete with Microsoft’s. Azure is one of the world’s leading cloud platforms, and it already meets our security and regulatory requirements.

Henk Van Driel: Manager
Cloud Competence Center, Rabobank

Rabobank reaps the rewards of investing in culture change with Microsoft Services
Credits

Many subject-matter experts contributed to the conceptualization and articulation of the story contained in this document.

Cigdem Aygun
Worldwide Azure Infrastructure and Security GTM Lead, Microsoft Services

Conor Bronsdon
Writer, Olive & Goose

Jon Farmer
Director of Marketing, Financial Services Industry

Ed Herman
Global Financial Services Industry Leader, Microsoft Services

Rupesh Khendry
Business Strategy Leader, Worldwide Financial Services

Nosos Kladakis
Principal PM, Customer/Citizen Identity and Access Management, Microsoft Identity

Steve Leigh
Financial Services and Public Sector Lead, Microsoft Services

Dave Morehouse
Worldwide Financial Services GTM Lead, Microsoft Services

Rupert Nicolay
Financial Services Industry Solutions Lead, Microsoft Services

Ian Ruthven
Strategy and Solutions, Microsoft Services

Caroline Sorensen
Program Manager, Microsoft Services

Adam Stoffel
Senior Program Manager, Microsoft Identity Customer Experience

Philippe Thévenin
Senior Industry Solution Architect, Microsoft Services

Umit Tiric
Digital Advisor, Microsoft Services

Adrian Yeoh
Financial Services Product Marketing Director
Turn innovation into practice with Microsoft Services

We empower organizations to put innovation into practice using our global reach and ecosystem to deliver strategic business outcomes, maximize the value of cloud technology, and drive success through continual support.

**EXPERTISE**
Navigate your transformation journey with confidence by relying on our experience, global partner network, and world-class customer support.

**INGENUITY**
Achieve breakthrough results at the intersection of creativity, technology, and security—powered by Microsoft innovation.

**EMPOWERMENT**
Activate your organization for digital growth with support at every step from a trusted partner committed to your success.
Turn innovation into practice with Microsoft Services.

microsoft.com/services