ForgeRock

INDUSTRY BRIEF

Seven Trends That Will Shape the Future of the Financial Services Industry

The financial services industry is changing at an unprecedented scale across the globe. Whether your organization is facing regulatory pressure to protect consumer data, demands for greater consumer access and control over their financial data, or competition in an expanding financial services ecosystem, you need a consumer identity and access management (IAM) solution that can help to:

- Align with Open Banking and consumer protection regulations
- Drive revenue and maintain competitive advantage
- Make it easy to acquire, retain, and protect your customers with no-compromise Zero Trust security
- Provide seamless omnichannel experiences across all platforms: brick and mortar, web, and mobile devices

Below are seven key trends that will affect the future of the financial services industry. Understanding these trends can guide you in choosing the right IAM solution to help you meet these challenges head-on.

TREND ONE

Regulatory Compliance and Data Protection

Regulatory compliance is driving an increase in digital innovation and consumer protection. Since the European Union's (EU's) May 2018 adoption of the General Data Protection Regulation (GDPR), organizations around the world doing business in the EU must adhere to strict data privacy regulations, including the "Right to be Forgotten" (RTBF). All organizations are legally required to inform consumers of how their data is being used and enable them to remove their data.

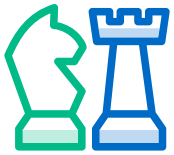
Regulations such as Open Banking in the EU and UK, the EU Payment Services Directive 2 (PSD2), and the California Consumer Privacy Act (CCPA), require banks to keep customer identities and financial information secure and to reduce risks to customer privacy. As a result, risk management professionals are looking for customer-centric technologies that offer security by design and integrate seamlessly with risk management and compliance strategies. With new threats to personal data emerging every day, your institution must become highly proficient at identifying and mitigating risk and supporting the identification and attribution of criminals.

When evaluating IAM products, look for a solution that can:

Identify and mitigate fraud through contextual authentication and authorization and

Detect environmental and behavioral signals, such as jailbreak detections, IP addresses, device matches, geofencing, location ranges, and more.

Your IAM solution should also be easy to integrate with industry-leading security solutions, such as fraud detection and identity verification, to protect your customers without sacrificing a great user experience.



TREND TWO

Increased Competition

To maintain a competitive edge as retail and other banking services shift to online channels, it's not enough to focus on process and cost. Financial technology (fintech) companies, along with third-party market entrants and digital-only "neobanks", are disrupting the financial services industry with increasing digital innovation and competition. Aggressive adoption of digital banking is driving the growth of incumbent and market-entrant digital banking competitors, particularly in Southeast Asia and Latin America. As banks lean into these new trends, they are accelerating their investments in digital transformation to generate revenue and shareholder profit while reducing costs.

To survive in this new landscape, your organization must have agility and a flexible IT architecture. If you aren't putting systems and platforms in place to support a fully digital service, you risk becoming less relevant to the new customer experience. When looking at an IAM solution, make sure it can support both your existing and future deployment plans – whether you will deploy your solution on-premises, in public, private, or multi-cloud environments, or consumed as a service.

TREND THREE

Legacy Constraints

Traditional brick and mortar banks are working to accelerate digital transformation, but they are also being held back by legacy processes, equipment, and software. Migrating off of a legacy system is inherently risky. It can result in loss of user access, failed compliance audits, cost overruns, and reputational damage. Digital transformation from legacy infrastructure requires planned, purposeful migration with the right tools and systems to avoid incurring excessive time, cost, and effort.

Many banks still rely upon legacy on-premises computer systems and legacy programming languages to handle transactions.[1] Because many of the experts that maintained these systems have retired, the workforce suffers a widening skills gap. Siloed legacy IAM systems are inflexible and cannot scale to support new use cases, better authentication methods, and more deployment models. To overcome legacy constraints, you'll need an IAM solution that can support migrating and centralizing identities from multiple identity management systems onto a single IAM platform – so you can quickly and easily streamline and build on existing investments with zero disruption. Simply adding modern authentication technologies and multi-factor authentication to legacy applications can immediately boost your applications' security and usability.

TREND FOUR

Open Banking and Open Finance

The Open Banking and Open Finance movements are driving increased adoption of digital channels and technologies and more robust open application programming interface (API) capabilities. Open Banking is expected to facilitate data sharing and allow banks and third parties to build bespoke solutions on top of new, common platforms. As banks and other financial services companies move to Open Banking, other parties can use their customer data for purposes such as cross-selling and direct marketing. Financial institutions will increasingly use customer data to offer loans, credit cards, mortgages, and other services.

Across the globe, financial service institutions are seeking to implement some version of an Open Banking framework based on three fundamental technologies:

- A financial-grade API (FAPI) from the OpenID Foundation
- A common authentication framework using OpenID Connect
- An identity management methodology that includes consent and delegation

While Open Banking and Open Finance are driven by government regulation in some regions like Europe, the U.S. is less encumbered by regulation and more motivated by market competition and the consumer demand for more control over financial data. Financial Data Exchange (FDX) is an open standards organization based in the U.S. and Canada, that aims to "unify the financial industry around a common, interoperable, royalty-free standard for secure and convenient consumer and business access to their financial data."[2]The proposed standard FDX API, supports secure authentication and data access to accommodate existing protocols for authentication and authorization. It enables sharing of consumer data without requiring "screen scraping" (shared credentials). Wider adoption of the FDX API will result in a more secure trust ecosystem that will enable innovative fintech companies to provide new services without compromising security.

To maintain relevance in the age of Open Banking and Open Finance,
look for an IAM solution that complies with the latest standards to support secure onboarding and staging and authorization of consent of third-party providers (TPPs).

[1]American Banker, Why some banks still lean on mainframes
[2]Financial Data Exchange, Frequently Asked Questions about FDX US

TREND FIVE

Consumer Demand for Control and Better User Experiences

The GDPR has spawned many data privacy and protection initiatives at the local, national, and international level. It has also inspired global consumer demand for control over their data. Consumers are increasingly dissatisfied with having their personal data collected and manipulated for marketing purposes without their consent. As a result, the financial services industry has seen a drastic increase in legal actions related to these data collection requests. Consumers are taking the lead and demanding control over their data.

Whether you want to seamlessly reach your customers on mobile or desktop platforms, in their homes or offices, **your IAM solution needs to provide a customer experience (CX) that:**

- Meets stringent privacy regulations
- Delivers the highest level of customer security and control over customers' personal data.
- Provides a single, consistent experience across all touchpoints

TREND SIX

Social Disruption

The financial services industry has long been a reflection of the wider economy and social trends. Take the developments we have seen in the services industry since the early 2000s. Jobs requiring high levels of "digitalization" – defined by the Brookings Institution as "the diffusion of digital technologies into nearly every business and workplace" – increased 4.6 times from 2002 to 2016, while jobs requiring little or no digital competency decreased by half.[3] This trend towards digitalization will continue to rise as technologies like artificial intelligence (AI) and machine learning (ML) change the way we work, live, and do business.

The sudden disruption in consumer behavior caused by the COVID-19 pandemic has increased the demand on banks and other financial institutions to provide secure online services in place of in-person visits to brick and mortar banks and offices. According to Gartner, financial services directors anticipate an average 11% uplift in post-pandemic IT budgets, prioritizing direct digital revenue growth.[4]

As the banking industry goes through its greatest transformation since the early 1990s, the roles and relationships of financial institutions, customers, partners, and employees are changing at an accelerating pace. With more financial transactions taking place online, your IAM solution must scale to support hundreds of millions of users without requiring a huge uplift from IT or causing disruptions to existing users.

[3]Mark Muro, Sifan Liu, Jacob Whiton, and Siddharth Kulkarni, "Digitalization and the American Workforce"
[4]Weiss, Juergen and Iyengar, Partha, "Financial Services CIOs Must Realize IT Investments' Revenue Potential to Drive Digital Acceleration," Feb. 17, 2021. https://www.gartner.com

TREND SEVEN

Cybersecurity Risks

The accelerating scale, scope, and sophistication of cyberattacks such as identity fraud mean that cybersecurity investment will always be a top priority. Ransomware attacks surged 150% from 2019 to 2020.[5] To stop account takeover attacks and protect employees, consumers, and internet-connected devices, you need an array of security methods, such as the Zero Trust model and the Continuous Adaptive Risk and Trust Assessment (CARTA) strategy.

One huge vulnerability for most financial institutions is entitlement creep, where the workforce, trusted third parties, and partners accumulate access to more systems or higher entitlement levels than are currently required for their job roles. If we assume that every organization has been breached in one way or another, entitlement creep and a lack of identity governance can leave user roles and access wide open across the organization. It enables attackers to infiltrate your organization, move laterally throughout your networks, and exfiltrate data with impunity. This vulnerability puts your organization at risk of internal audit failures, compliance fines, ransomware attacks, and loss of consumer trust.

Every enterprise supporting high-risk online transactions must design Defense in Depth (DiD) into all their systems. **Your IAM solution should also support and enhance identity governance with AI that can:**

- Identify and apply the appropriate user access levels
- Automate high-confidence access approvals
- Recommend certification for low-risk accounts
- Automate the removal of unnecessary roles

Your IAM solution should also help your organization:

- Understand how user access influences its risk posture
- Provide continuous contextual awareness of who has access to what resources and why
- Take immediate action when necessary

Conclusion

The key trends and developments driving progress in the financial services industry are:

1. Regulatory Compliance and Data Protection
2. Increased Competition
3. Legacy Constraints
4. Open Banking and Open Finance
5. Consumer Demand for Control and Better User Experiences
6. Social Disruption
7. Cybersecurity Risks

Armed with this knowledge, you can develop a successful strategy to capitalize on these trends. This strategy will help you navigate a changing market and anticipate changes to your customer base.

The rise of the digital-first and mobile-first consumer means your organization needs to shift from a product-focused strategy to a customer-first strategy. Give your customers the seamless, secure user experiences they demand, so your organization and the financial services industry as a whole can thrive in this changing market.

[5] Group IB, Get Ransomware Uncovered 2020/2021

About ForgeRock

ForgeRock, the leader in digital identity, delivers modern and comprehensive Identity and Access Management solutions for consumers, employees and things to simply and safely access the connected world. Using ForgeRock, more than a thousand global customer organizations orchestrate, manage, and secure the complete lifecycle of identities from dynamic access controls, governance, APIs, and storing authoritative data – consumable in any cloud or hybrid environment. The company is privately held, and headquartered in San Francisco, California, with offices around the world. For more information and free downloads, visit www.forgerock.com or follow ForgeRock on social media.

Follow Us

ForgeRock

Copyright © 2021 ForgeRock, All Rights Reserved.