Using digital identity management to prioritize security and efficiency in the financial services industry

Despite heavy investments in cybersecurity, financial organizations continue to remain a major target for cyberattacks. Threats from insiders and third parties can leave financial institutions fighting a war on two fronts. And while attempting to protect themselves, they also need to adhere to stringent and complex regulatory requirements.

Financial institutions are feeling the pressure mounting to keep data secure, preserve customer privacy, and maintain a reputation as secure and trusted organizations.

When it comes to maintaining cybersecurity requirements for financial services, traditional security methods simply aren't adequate anymore.

Challenges impacting compliance and security

Whether it's for banking or investment purposes, consumers want to do business with institutions that keep their money – and their data – safe.

So, what challenges will financial institutions face as they attempt to comply with regulatory standards while maintaining optimal security?

Here are just a few examples of the obstacles that need to be overcome:

- **The constant threat of a data breach |** Data breaches are more common than ever in the financial services sector: **58% of financial services organizations** have experienced a third-party data breach within the past 12 months, and a full **40% of financial data breaches** involve compromised credentials

- **Suboptimal password security |** **48% of financial services organizations** do not enforce the use of complex passwords

- **More users, more devices, more data centers |** Many financial institutions hold rich sources of data across numerous applications; this data must be made available to more users than ever across a growing number of devices

To avoid sensitive financial data falling into the wrong hands, leading to a loss of business or status in the industry, financial organizations need to level up their strategy.

Strategic solutions

Protecting financial data while complying with strict requirements and helping IT teams stay productive with simple, efficient workflows is a tall order. It's one that only a well-defined, comprehensive digital identity management strategy can solve.

Knowing what to do and how to do it can seem overwhelming, but here are the main tenets a solid security strategy should include:

- Enable secure third-party access | Many people both inside and outside the organization need to access IT systems, so it's critical to minimize risks associated with compromised privileged credentials.

- Streamline regulatory compliance | If solutions don't comply with the necessary regulations, or skip some steps, they've missed the mark; risk analytics can accurately detect threats in critical systems.

- Improve workflow efficiency | Staying secure shouldn't come at the expense of sacrificing operational efficiency, so frictionless access to all applications on any device, anywhere, and at any time is crucial.

To enact the best digital identity management strategy, organizations partner with a trusted provider of digital identity solutions. Imprivata is that industry-leading partner.

The Imprivata difference

Driven by our extensive experience and expertise, Imprivata is uniquely positioned to help organizations in the financial service industry overcome security, workflow efficiency, and compliance challenges. That difference includes:

Want to learn more? Check out these customer case studies highlighting real-world examples highlighting real-world examples of how Imprivata partners with financial services institutions to optimize both security and efficiency:

Case Study – Stock Yards Bank and Trust makes employees productive and keeps data secure

Case Study – Verity Credit Union streamlines access and reduces cost

- **We provide unmatched support delivering user-friendly workflows on shared endpoints including workstations and mobile devices**, eliminating risks surrounding generic user accounts without sacrificing efficiency

- **Unique solutions for managing and simplifying user access to shared mobile devices**, enabling fast provisioning and secure, seamless workflow access

- **Quick, flexible, user-friendly authentication** to satisfy multifactor authentication requirements, while providing users with options to best meet their workflow needs

- **Single sign-on for both legacy and cloud applications**, resulting in a fast, secure, consistent authentication experience

- **A full complement of implementation and managed services**, ensuring prompt deployment and success at scale in a fast, cost-effective way

To enact the best digital identity management strategy, organizations partner with a trusted provider of digital identity solutions. Imprivata is that industry-leading partner.

Request demo

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

For more information, please contact us at:

Global headquarters USA
Waltham, MA
Phone: +1 877 663 7446
www.imprivata.com

European headquarters
Uxbridge, England
Phone: +44 (0)208 744 6500
www.imprivata.com/uk

Germany
Langenfeld
Phone: +49 (0) 2173 99 385 0
www.imprivata.com/de

Australia
Melbourne
Phone: +61 3 8844 5533