Beyond Identity for FSI: Financial Services, Banking, Insurance & Fintech

BEYOND IDENTITY

Overview

Cybersecurity in the financial services insurance industry sits in the middle of a trifecta of challenges. First, employees, broker-dealers, agents, advisors, and clients have rising demands for frictionless experiences. Second, attackers are exploiting the move to digital with increasingly frequent and aggressive attacks capable of bypassing first-generation multi-factor authentication (MFA). Third, regulations are expanding in number and scope.

Adapting to the rapidly evolving security landscape requires a unified approach to securing access across disparate user groups—employees, broker-dealers and partners, and clients.

Beyond Identity allows companies to go beyond responding to attacks and start preventing them by shifting security left. As the only platform that delivers unphishable MFA with zero user friction, Beyond Identity enables companies to secure critical resources and applications with confidence. Moreover, the Beyond Identity Zero Trust Risk Engine enables continuous authentication using risk-based policies based on real-time user and device risk signals captured from the endpoint or ingested via detection and response tools.

Unique Benefits

- ✓ **Phishing resistant, invisible MFA** with two strong factors by default
- ✓ **Passwordless user experience** with no second devices, codes, or push notifications
- ✓ **Zero Trust Authentication** with dynamic risk-based policies and robust integration ecosystem

The challenge: balancing security and usability in a complex regulatory environment

Against the context of the move to the cloud, transitioning to remote work, and the influx of digital-native startups, competing effectively in the financial services insurance industry requires exceeding customer experience expectations, mitigating data breaches, and proactively preparing for increasingly stringent regulations.

Recent Phishing Resistant MFA Regulations:

- NYDFS 500.12 and Industry Letter
- FFIEC Guidance on Authentication and Access to Financial Institutions Services and Systems
- NAIC Insurance Data Security Model Law
- Federal Zero Trust Strategy
- NIST Update: MFA and SP 800-63 Digital Identity Guidelines

However, while 55% of financial services insurance companies cite customer experience and reputation as their primary competitive differentiators, over 30% of users report resetting passwords at least once a month for financial services insurance accounts. Employees, broker-dealers, and agents are also increasingly frustrated with first-generation MFA friction.

Research shows that only 29% of users agree that MFA was worth the convenience tradeoff, and 35% specifically cite difficulties with their phone not being immediately available when attempting to login.

Beyond decreases in customer satisfaction scores, users are dropping off to competitors after repeated offenses of poor digital experiences.

Making matters worse, requiring users to jump through MFA hoops does not guarantee security. Attacks are increasingly adept at exploiting first-generation MFA methods. The troubling rise of MFA bypass and phishing kits has rendered phishable MFA wholly ineffective.

In fact, both the US government and NYDFS issued statements calling for the "discontinued support of authentication methods that fail to resist phishing such as phone numbers for SMS or voice calls, supply one-time codes, or receive push notifications."

NYDFS has already issued multiple multi-million dollar fines for MFA violations.

The solution: MFA built for a zero trust world

As the front door to all data, resources, and services, authentication security is critically important. In order to meet the demands of the business, users, and regulators, authentication must be frictionless, unphishable, and risk-based.

- **Frictionless:** The burden of authentication should be removed from users to create a delightful and secure experience. This means there should be no extra steps such as copying one-time codes, clicking push notifications, or picking up a second device at all.
- **Unphishable:** There should be no dependency on any phishable factor for authentication to ensure account security and protect sensitive data. Phishable factors include passwords, push notification, and one-time codes.
- **Zero trust compliant:** Increasing adoption of zero trust strategies means authentication comply with the "never trust, always verify" primitive of a zero trust approach. Authentication should immutably verify user identity and the integrity of devices used.
- **Ease of deployment:** With accelerated digital transformation, most security environments are hybrid and must support various use cases spanning clients, employees, agents, and broker-dealers. Any technology employed must be built for a hybrid environment, high availability, and rapid deployment.

When you get authentication right, all users and your business benefit:

Employees	Broker-Dealers, Partners	Customers, Clients
Improved productivity from lowered authentication friction	Improved satisfaction from lowered authentication friction	Accelerated onboarding and login with zero-friction authentication
Secure access to resources and cloud apps from anywhere with any device	Consistent, universal experience across mobile and web apps on any device	Fully safeguarded from credential-based attacks
Lowered help desk costs associated with password resets	Secure access to data and resources to successfully complete their tasks	Consistent, universal experience across mobile and web apps on any device

Zero Trust Authentication Requirement	*Beyond Identity*	*Differentiation*
Frictionless: Easy for users to adopt and accelerates speed to resources.	✓	Beyond Identity lowers MFA friction to zero by completely removing the need for second devices.
Unphishable: No reliance on phishable factors including one-time codes, push notifications, and magic links.	✓	Beyond Identity delivers unphishable MFA with: • Something you have - possession of private key within device secure enclave • Something you are - local device biometric
Passwordless: Eliminate threat of password-based attacks and save on help desk costs for password resets and lockouts.	✓	Given our architecture, passwords can be fully eliminated from the user experience and database. What doesn't exist cannot be breached.
Zero trust compliance: Never trust and always verify every user and device, in real-time and continuously, that is requesting access.	✓	Given our architecture, each device is cryptographically bound to a specific user identity to ensure that the right person, with a secure device, is accessing the right data. Every authentication is also evaluated continuously for real-time device risk gathered from the endpoint directly or ingested from detection and response tools continuously.
Ease of deployment: High availability, able to support cloud-based apps, kiosks, and differentiated needs of clients, agents, and employees.	✓	Beyond Identity is highly available, elastically scalable, and integrates with all major IDPs/ IDaaS solutions while providing support for hybrid IT environments.

Beyond Identity

Beyond Identity is fundamentally changing the way the world logs in–eliminating passwords and all phishable factors to provide users with the most secure and frictionless authentication on the planet. Our invisible, passwordless MFA platform enables companies to secure access to applications and critical data, stop ransomware and account takeover attacks, meet compliance requirements, and dramatically improve the user experience and conversion rates. Our revolutionary zero-trust approach to authentication cryptographically binds the user's identity to their device, and continuously analyzes hundreds of risk signals for risk-based authentication. For more information on why Snowflake, Unqork, Roblox, and IAG use Beyond Identity, check out www.beyondidentity.com.