okta

What Financial Institutions Need to Know About the NYDFS Cybersecurity Regulations

Okta Inc.
301 Brannan Street, Suite 300
San Francisco, CA 94107

info@okta.com
1-888-722-7871

What Financial Institutions Need to Know About the NYDFS Cybersecurity Regulations

Note to readers: While this article discusses legal concepts and recently-enacted regulations, it does not constitute legal advice and is provided for informational purposes only. If you or organization requires legal advice, be sure to contact an attorney.

Data breaches across industries have been increasing dramatically since 2008, especially those associated with hacking, malware, and social engineering. 2016 saw no deviation from this trend, especially for the financial services industry. According to IBM X Force research, more than 200 million records were compromised in the industry, a 937% increase from 2015. Financial services saw a 29% increase in cyber attacks, with 1,684 attacks in 2016 compared to 1,310 in 2015. As a response to these increasing cybersecurity risks, in March 2017, the New York Department of Financial Services instituted 23 NYCRR 500, a cybersecurity regulation unlike any other. The regulation establishes minimum security requirements to protect financial institutions (and their customers) from cyberattacks.

The regulation impacts anyone "operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law." This means the vast majority of banks, insurance companies, and financial institutions in New York will be held accountable by the regulation. It also applies to third-parties (located outside of New York) that provide services to these institutions as well as other organizations who, while not based in New York, are doing financial business in the state.

23 NYCRR 500 has been described as the "harshest" and "strictest" of cybersecurity regulations. According to the New York Law Journal, this regulation "marks a watershed moment in cybersecurity regulation in the United States. For the first time, a single state is regulating cybersecurity on a potentially global scale, and it has done so via the regulatory process, not legislative action."

There are four phases of the regulation.

Phase 1, which went into effect August 28, 2017 requires firms to: establish a formal cybersecurity program, appoint a Chief Security Officer, regularly review user access privileges, hire cybersecurity personnel, and develop a written incident response plan.

Phase 2, which goes into effect March 1, 2018, requires financial services organizations to: regularly perform penetration testing and vulnerability assessments, conduct a risk assessment of information systems, use multi-factor or risk-based authentication, conduct regular cybersecurity awareness training, and produce an annual report on their cybersecurity program and any risks.

Phase 3, which goes into effect September 3, 2018, requires firms to: maintain records and audit trails, establish and follow guidelines for application security, limit data retention and establish proper procedures for safe data disposal, monitor and detect unauthorized access of sensitive information, and encrypt nonpublic data in motion and at rest.

The final phase, which goes into effect March 1, 2019, requires firms to: be in compliance with 23 NYCRR 500 and also obligates their third-party service providers to comply.

Multi-factor authentication (MFA) is one critical component of 23 NYCRR 500. It requires any employee or third-party service provider accessing company apps or data from an external network to use MFA. As financial institutions meet this requirement, they should consider balancing security with simplicity and ease-of-use for end users/ease-of-management for IT teams. They can do so by offering a comprehensive set of second factors, and the ability for IT to dynamically adapt authentication policies based on user's location, IP address, the device being used, etc.

Organizations have historically required employees to use MFA to access specific critical apps that housed more sensitive data or when accessing corporate resources from and data outside their company firewall. However, with today's cyber attack techniques, simply protecting access to critical apps with MFA is no longer sufficient. Once attackers are inside an organization, they can easily move laterally, and any app or account can become the next target for obtaining additional credentials and access. MFA should apply to all applications (regardless of whether they are for the cloud or on-premise), user groups and devices.

MFA has also traditionally been thought of as a separate security tool, deployed in a somewhat ad hoc fashion instead of part of an overall plan. In today's world, financial services firms need to think about MFA as one part of a fully integrated security strategy. Cloud Identity and Access Management (IAM) delivered entirely as a service enables financial services to take a comprehensive approach to security and address other requirements of 23 NYCRR 500. Solutions like lifecycle management give financial services organizations visibility and control of all user identities across all lifecycle states. A robust reporting system plus API integration with other security tools enable firms to monitor authentication events. And, a central source of truth enables financial services organizations to easily manage all their users, devices and groups, regardless of how many directories or sources they are coming from.

As the foundation for secure connections between people and technology, Okta can uniquely help your organization meet the access and authentication requirement portions of 23 NYCRR 500. With Okta lifecycle management, financial services organizations have control of all user identities across various lifecycle states. IT teams can create and deactivate user accounts, provision user access to apps and manage entitlements from one place. These processes can also be automated via rules, policies, workflows, and APIs. With Okta's reporting and API Access Management solution, financial services organizations have complete visibility into authentication events as well as the ability to take decisive action. Okta's identity driven policy engine allows IT teams to easily configure access policies and authorization to API resources. They can define access based on a user's profile, group, network, client, and consent. User access can also be immediately revoked or user permissions updated based on their profile and status.

With 23 NYCRR 500 deadlines looming (and penalties for those who do not become compliant on time), impacted financial services firms simply cannot wait. Rather, they should use this regulation to re-examine how identity can play a larger role in their organization's overall security. As the threat landscape changes and cybersecurity laws and regulations adjust in response, organizations must also adapt their security policies to encompass identity concepts for the most visibility into, and protection against, rising threats.

okta