DUO for...

Duo Security is now part of Cisco.

Financial Services

All financial services organizations – insurance providers, banks, brokerage firms and others – must implement multi-factor authentication (MFA) to meet the NYDFS Cybersecurity Regulation and NAIC requirements for access controls and risk-based authentication.

THE CHALLENGE:

Satisfying NYDFS & NAIC

NYDFS CYBERSECURITY REGULATION

All financial service companies operating or conducting transactions in New York must meet specific cybersecurity regulations by March 1, 2019. The New York State Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR 500) requires risk assessments, access privilege controls, multi-factor authentication (MFA) and more. **Any financial institution with an NYDFS license must meet the cybersecurity regulations or potentially be subject to penalties.** Compliance costs financial institutions $70 billion annually, according to the American Banker.

NAIC INSURANCE DATA REGULATIONS

Insurance organizations must also comply with National Association of Insurance Commissioners (NAIC) regulations to protect insurance data, including implementing access controls to limit access to only authorized individuals. South Carolina and Ohio adopted NAIC regulations on Jan. 1, 2019, and many other states are following suit.

“

We loved Duo’s speed to security, the experience working with their subject matter experts, the time and money we save with the ease of integration, and the overall end-user experience.”

John Bryant

Chief Technology Officer, Options Technology (managed services provider for financial institutions

Duo for Financial Services

THE SOLUTION:

Duo's Zero Trust

Over 2,000 financial services companies trust Duo. Duo ensures trusted access to help organizations meet NYDFS and NAIC regulations in three ways:

01

MFA for All Users

NYDFS mandates the use of MFA for any individual accessing a financial organization's internal networks from an external network. Verify your users' identities with Duo's easy-to-use multi-factor authentication (MFA). With one tap, users can approve a Duo Push notification sent to their smartphones. Duo offers several other authentication methods, including OTP-based hard/soft tokens, YubiKeys and more.

To meet compliance and pass audits, you need to protect your mix of cloud, older on-premises and custom apps. Duo integrates with more apps, regardless of where they reside, protecting hybrid environments, remote access VPNs, single sign-on and more. To support remote employees (insurance agents and financial planners), Duo offers easy self-enrollment and automated enrollment options to ensure successful deployments at scale and reduce help desk tickets.

02

Visibility Into Devices

To support insurance agents and contractors using their own personal devices, Duo provides greater device insight without an intrusive agent. Get visibility into all user devices, including corporate or personally-owned laptops, smartphones, desktops and PCs. Detect whether devices are running out-of-date software, and identify endpoints that are jailbroken, rooted, tampered with, unencrypted and more.

Useful for daily, weekly or monthly compliance audits, Duo's reports give you detailed insight into user and device risks that can easily be exported or integrated with a SIEM (security information and event management) system.

03

Adaptive Authentication

Based on a risk assessment, NYDFS requires financial institutions use effective controls such as risk-based authentication to protect against unauthorized access to their information systems.

Duo's solution lets you set policies to block access attempts based on an individual or group, geolocation, network type and device security. Enforce stricter login controls for unmanaged, personally-owned devices used by third-party service providers. Require encryption or enabled passcodes, and block access by devices without enabled security controls.