DUO for...

cisco SECURE

Financial Services Regulations

All financial services organizations – insurance providers, banks, brokerage firms and others – must implement multi-factor authentication (MFA) to meet various state and federal regulations to ensure sensitive financial data is secure and protected.

THE CHALLENGE:

Satisfying State & Federal Regulations

New York and California were two of the first states that created new consumer data protection requirements. New York set the strictest state standard for financial services companies when the New York State Department of Financial Services (NYDFS) passed Cybersecurity Regulation 23 NYCRR 500 in 2019. Not only did the NYDFS expand the definition of financial services to include all companies that engage in financial transactions, it also spelled out cybersecurity requirements all companies operating in NY state must follow, including implementing multi-factor authentication (MFA) across the workforce.

While the states acted first, the federal government was not far behind. In 2021 the Federal Trade Commission announced a change to the Safeguards Rule, originally established by the 1999 Gramm-Leach-Bliley Act (GBLA). Beginning in 2022, the Safeguards Amendment, requires that all companies that "significantly engaged in financial activities" must also use MFA to protect financial data. The mixture of state and federal laws can create a confusing environment, but ultimately, strong secure access measures across the workforce will help companies not only comply, but also improve their security posture.

"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

Financial Services Regulations

THE SOLUTION:

Duo's Zero Trust

Thousands of financial services companies trust Duo. Duo's trusted access helps organizations meet state and federal regulations in three ways:

01

MFA for All Users

Financial services regulations mandate the use of MFA for any individual accessing the organization's sensitive data. Verify your users' identities with Duo's easy-to-use multifactor 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 most apps, regardless of where they reside, protecting hybrid environments, remote access VPNs, single sign-on and more. To support remote employees, contractors, and third parties, 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 employees 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. Duo can verify device health before granting access, to prevent exposing your applications to potential risk.

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

In order to ensure secure access to sensitive financial data, risk-based authentication can protect against unauthorized access to information systems. This can also allow organizations to limit access to users that really need it, a key tenet of a zero trust strategy.

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.