

New MFA Mandates for FIs

Regulations Like FTC Guidelines and 23 NYCRR 500 Have Raised a High Bar on MFA

Financial institutions – whether systematically important banks (SIFIs), local and regional banks, savings and loan institutions, payment networks or insurance companies – have long been on the front lines of digital technology. They're of course security-conscious and highly regulated already, but that doesn't keep cybercriminals and other adversaries from making them their preferred target.

The cybersecurity industry has seen time and again how a specific defense method is implemented only to have criminals find a way to thwart it at scale. What follows is a rapid exploitation of existing protections and desperate scrambles for replacements. Only then do standard and audit bodies close off these gaps with updated tech and start auditing against revised requirements.

That's precisely where we're at with MFA today.

PROBLEMS WITH MFA

Multifactor authentication (MFA) has experienced a continual back-and-forth between "defender deployment" and "adversary compromise" since it was introduced in 2019. As widespread adoption began, two truths emerged:

- MFA is only as strong as you make it: there are many different factors to choose from in modern MFA architecture. While some are easy to deploy but may also be inherently weak (like all knowledge factors and one-time passwords) others are traditionally more difficult to manage, even though they're more robust (like possession factors and some types of biometrics).
- Adversaries will ruthlessly root out the weaker forms of MFA: Once an exploit has achieved success against any form of MFA – but especially weaker code-based or knowledge-based forms – they wither under an onslaught of ATO attempts.

Organizations who deploy MFA need to keep this in mind, from initial design to later refinement. Luckily, there's excellent guidance available on "what makes good MFA."

“STRONG MFA” ACCORDING TO CISA & NIST

No organization is perhaps more knowledgeable about what works and what’s prone to fail in cyber defense strategies than the U.S. Cybersecurity and Infrastructure Security Agency, or CISA. When it comes to MFA, CISA has gone to great pains to define and document the only options that are suitable to achieve phishing resistance: a) PKI-based solution like those that create and deliver TLS certificates; or b) FIDO2-based solutions that leverage WebAuthn, another form of PKI.





A screen shot from the official CISA website highlighting their guidance for robust (phishing-resistant) MFA.

RECOMMENDED IMPLEMENTATIONS

Table 1 lists forms of MFA from strongest to weakest based on their susceptibility to the above cyber threats:

Table 1: MFA Forms, Strongest to Weakest

Authentication Form	Overview	Threat
Phishing-resistant MFA:  FIDO/ WebAuthn authentication  Public key infrastructure (PKI)-based	Phishing-resistant MFA is the gold standard for MFA. See the Phishing-Resistant MFA Implementations section for more information. CISA strongly urges system administrators and other high-value targets to implement or plan their migration to phishing-resistant MFA.	Resistant to phishing. Push bombing, SS7, and SIM swap attacks are not applicable.

To achieve MFA that’s robust and more specifically phishing-resistant, no other form of authentication is advised.

Not only does CISA make this recommendation, but so does NIST, the National Institute of Standards and Technology. In their 2024 update to SP 800-63, which covers digital identities and lifecycles, they highlight the need for phishing resistance and clearly state:

“An authenticator is phishing-resistant if it is a cryptographic authenticator that binds its output to a communication channel (e.g., client-authenticated TLS) or a verifier name (e.g., FIDO2/WebAuthN).”

Despite the heavy “officialese” in this statement, it’s saying effectively the same thing that CISA said: TLS-based or FIDO-2-based PKI is the way to go.

MFA IN FINANCIAL REGULATIONS

While requirements for multifactor authentication were introduced into most financial-services oriented regulations around 2018, a series of damaging exploits made it clear there was much more to do in order to keep customers and financial data safe:

- First American Financial, 2019: 885 million records linked to real estate transactions exposed through website design error
- Capitol One, 2019: 100 million credit card applications intentionally exposed by an AWS engineer
- JP Morgan Chase, 2014: 83 million accounts exposed, not fully discovered until 2019
- Equifax, 2017: 147 million US customers impacted by exploited records
- Experian, 2020: 24 million financial customers compromised through phishing campaigns

Not all of these attacks were due to poorly managed or incompletely deployed MFA. To get more insight into the differences between “good” MFA and “bad” MFA, watch this short video on current MFA exploits. But the scope of these attacks (and many more like them) made it abundantly clear that financial institutions were still high on two lists:

- The targets that criminal and nation-state adversaries most wanted to compromise, and
- Organizations whose systems were most in need of continual upgrades.

While regulatory standards are slow to evolve (much slower than adversarial tactics) there has been a sea change in the last 24 months. Now a whole host of financial-oriented regulations and standards are not just requiring “MFA,” but are also declaring the need for “phishing resistant MFA” in the way CISA defines it.

Standard or Mandate	Requires Simple MFA	Requires Phishing Resistant MFA	Source
FTC Safeguards	✓	✓	Link
PCI DSS 4.0	✓	✓	Link
FFIEC	✓	⊗*	Link
CISA Guidance	✓	✓	Link
NIST 800-663 Digital Identity Guidelines	✓	✓	Link
23 NYCRR 500	✓	⊗	Link

*Highly recommended

PHISHING RESISTANCE NEEDS TO HAPPEN FAST

The regulations and standards above are asking for these changes fast: the FTC Safeguards guidance, for instance, requires immediate action. This regulation covers any organization that participates in commerce with financial institutions, has a broad span of control. Mortgage lenders, payday lenders, mortgage brokers, account servicers, check cashers, wire transferors, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, and many types of investment advisors must subject themselves to FTC Safeguards audits ... which now include the use of phishing-resistant MFA in almost all use cases for account access.

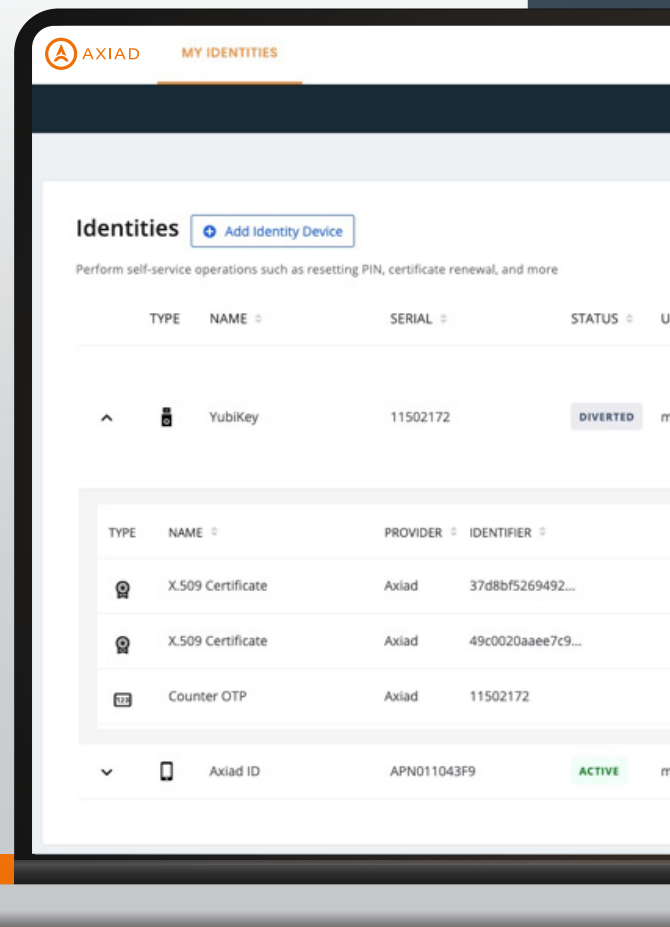
The FTC introduced these updated rules in fall of 2023, and they took effect in summer 2024. For other standards bodies and compliance regimes, similar changes are happening at a similar pace.

HOW AXIAD CAN HELP

A common refrain from financial services organizations is “But I already have an authentication system in place for MFA! Do I need to rip-and-replace this expensive system to achieve phishing resistance and meet these new requirements?”

Fortunately, the answer is “No.”

Most of these requirements assume that organizations already have, or are planning to install, a credential management system (CMS) to automate the delivery of FIDO2-based or TLS-based digital credentials into their authentication processes. The CMS doesn’t take over authentication: it simply manages the lifecycles of the increasingly critical credentials that make phishing-resistant MFA possible. The CMS injects the right credentials into the authentication process at the right time, wherever workflows or security requirements demand their presence.



Axiad Conductor lets identity teams manage multiple strong credentials—from FIDO to TLS certificates—across different operating systems, platforms and devices. This delivers audit-ready phishing resistance that doesn’t require new investments in MFA.

Best of all, the CMS that enables phishing resistance can be added to almost any existing MFA solution. Axiad Conductor doesn't need to be your authentication platform to add value. When paired with hardware-based authenticators, like those from Yubico, Idemia, Thales or Feitian, Conductor makes your systems phishing resistant on Day 1.

For more information on Axiad Conductor, the award-winning CMS that helps Financial Institutions become more secure and more nimble, visit our site at www.axiad.com for more details. You can download a product brief or calculate your savings over manually managed and admin-deployed MFA solutions.

And if on the off chance you look at the table above and say, "My most critical audit isn't asking for phishing resistance yet," count yourself lucky. But be prepared for imminent changes, too.

