Staying Vigilant With MFA

cyber security risk management MFA

Summary: Multi-factor authentication has become more widely used by organizations with ongoing data breaches proving costly. Even community financial institutions have been hit. It may feel overwhelming to know how to start. So, we give you three considerations when deliberating on multi-factor authentication as well as a few options that are available.

In honor of Labor Day on Monday, we found some trivia you might find interesting. Labor Day was first celebrated as a parade of 10K Central Labor Union workers in NYC on September 5, 1882. It became a federal holiday in 1894. Labor Day is considered the end of summer (when it used to be tradition to stop wearing white) and is the “unofficial NFL season kickoff” with 99% of all first games happening the Thursday after Labor Day. Get your finger food ready for those football gatherings!

While finger food is yummy, make sure to keep those fingers clean and ready for fingerprint authentication. This is one of the ways that organizations are keeping their data secure using multi-factor authentication (MFA). MFA use is on the rise, as it provides superior protection over passwords alone. While it may take some time to get MFA in place, it is the best way to prevent data breaches, which have become very costly — to the tune of $18.3MM per year per company in the banking industry alone.
Here are three things to consider with MFA in the ongoing battle to shore up your institution’s security.

1. MFA is a layered security approach

MFA requires two or more methods for successful authentication. One example would be a combination of something you know (like a password), what you have (debit or credit card), and something unique to you (such as a face or fingerprint scan). This approach is not unlike the two-factor approach bank customers use to access the ATM — with a card and a PIN. Yet, it is clear that incorporating a third option, such as a fingerprint scan, makes things more difficult for cyber thieves.

Does this layered approach of authentication make sense for community financial institutions (CFIs)? Absolutely, according to securities experts who see the added layers of security MFA offers as more of a must than a nice-to-have. Consider this: The pandemic is a leading reason for a flood of cyberattacks directed at financial institutions. A massive 238% uptick occurred between February and April of last year, according to research from VMware Carbon Black.

2. Customers accept MFA

With many smartphones using MFA these days, many bank customers are used to it. They use a fingerprint or face ID to get into their phones. So, why not use it for a bank account? According to PYMNTS.com research, 52% of large city dwellers are “very interested” or “extremely interested” in using MFA. Yet, it is not only the urban areas that have a preference. Nationally, 75% of consumers are logging into digital banking with usernames and passwords, yet only 42% want to. The rest prefer more advanced measures of authentication. This increasingly widespread use and preference make it easier for CFIs to put MFA into practice.

3. Employees and third parties need it too

Employees and third parties should also use MFA to access data. In a survey of senior and mid-level security professionals, 83% believe that employees have made customer or confidential business data accessible by mistake. That's why branch staff needs to be reminded often about the importance of MFA and how to use it properly — on personal devices as well. This is especially important as some branch staff may still be working remotely. Requiring employees to use long, complex passwords is a start. But you'll want to go a step further.

While employees may falter at times, third parties can also unwillingly or willingly find unauthorized access to customer and financial data. According to a 2021 Ponemon report, over half of respondents gave third parties access to confidential data without checking their security and privacy practices. MFA should be a requirement organization-wide for all systems that contain sensitive information and where user control is necessary, including third-party access. This would remove additional measures needed to validate and verify authorized third-party users.

Consider the options

The number and type of offerings have increased, so you may be surprised at what you find when you do your research for the right MFA solution. One potential option is to choose an authenticator app, such as Google Authenticator, that generates codes. It's considered more secure than SMS/text authentication. However, if an authenticator app isn't an option, then SMS/text authentication can work. Biometric data like fingerprints or facial recognition technology could be good alternatives where devices are used, such as with branch check-in tablets. There are other options beyond authenticator apps and biometrics too. A physical security key may also be a viable option for logging into certain websites. Or a key fob with a code to access certain files.

As Jonah Force Hill, senior cyber policy advisor said, "*Every organization — providers of financial services, in particular — must remain vigilant in the face of these evolving threats.*" MFA is one way to remain vigilant.

Choosing the right MFA solutions can be daunting for CFIs, especially given the need to balance top-notch security with ease of use. But with so much at stake, CFIs can't afford to bypass these important security measures.

CECL: THREE TIERS TO FIT YOUR NEEDS

CECL is one of the biggest challenges these days. CECL FIT gives you options to get started simply with a web-based solution that fits your portfolio needs. It includes as much expert assistance you need at no extra cost. Learn more about our CECL FIT® today.

ECONOMY & RATES

Rates As Of: 09/03/2021 05:46AM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	0.05	0.01	-0.04
6M	0.06	0.00	-0.03
1Y	0.07	0.00	-0.03
2Y	0.21	0.00	0.09
5Y	0.78	0.01	0.42
10Y	1.32	0.01	0.41
30Y	1.94	0.01	0.30
FF Market		**FF Disc**	**IORB**

0.08	0.25	0.15
SOFR	**Prime**	**OBFR**
0.05	3.25	0.07