Multi-Factor Authentication for Independent Agencies:
A Gathering Storm

Key Issue

MFA implementation is a top issue for carriers and their partner agencies. ID Federation believes carrier security teams are quickly implementing their version or interpretation of MFA while not fully understanding the impact on their agents, especially if every carrier has a different solution.

How Can SignOn Once Help?

SignOn Once implementation can streamline the process to meet regulatory requirements for incorporating MFA. When the agency administrator adds a new user to their system and they check the MFA box, a flag is sent to all participating carriers. This indicates the user went through MFA as they logged into their management system. Also, users only need to remember their login credentials for their management system, not for all their participating carrier partners.

This is a huge benefit. If an agency management system user connects to 10 carriers and all them have implemented SignOn Once, those users only need to manage MFA at the beginning, one time, when they log into the system, not for every participating carrier. The time saving is enormous.

Furthermore, identity providers (technology vendors) go through a thorough assessment process to ensure they meet the requirements defined in the ID Federation Trust Framework. The process ensures they are service organization control, or SOC, compliant for practices that guarantee security oversight across the organization. The Trust Framework is likely more in depth than what carriers go through before allowing third parties to connect to their systems.

ID Federation's goal is to raise awareness and provide information to carriers to help them ensure success in implementing MFA with their agents. Agencies will be on the receiving end of different MFA implementations and could get frustrated and confused, unable to write business as normal.

Like many new technology or workflow implementations, it's all about smart and timely communications to key stakeholders.

What is Multi-Factor Authentication?

Multi-factor authentication (MFA) is an electronic authentication method where a user is granted access to a website or application only after accurately presenting two or more pieces of evidence to an authentication mechanism. Also called "two-step authentication," MFA is an additional component beyond ID and password to create a more secure connection.

A website or application can add this additional factor the first time a user logs into a website from a new device, every time, or on some periodic schedule. There are various methods: Sometimes you are required to have a key, a biometric such as a fingerprint, or the answer to a security question like, "What school did you attend?" A security question is the most common today.

Regulatory bodies, such as New York Department of Financial Services and the National Association of Insurance Commissioners, have released rules in recent months on when MFA should be used in conducting business. The insurance industry is expected to see enhanced scrutiny around MFA practices.

SignOn Once
BY ID FEDERATION

What Does ID Federation Recommend?

For Carriers

- Do not implement MFA without advance notice (months, not weeks) to appointed agencies and a regularly communicated process. For example, add a pop-up on the agency portal login screen reminding users that MFA will be implemented in (X # of) days.
- Begin with a pilot program with some agencies vs. turning on MFA all at once for all users. Some carriers have begun testing first with employees, then agencies. One carrier reports that many of its larger agencies needed weeks or months to adjust to MFA implementation.
- For MFA, ask questions about something the user knows, such as "What school did you attend?" Send MFA requests to email addresses, not cell phones. Carriers likely will lack most cell phone numbers in appointed agency profiles. Also, agency owners are concerned about security and E&O liability. Some do not permit personal, private devices for business use.
- If you don't have separate credentials for all of your agency users, include this in your implementation plans. This improves both clarity and security. Perhaps consider awards for agencies that set up separate IDs.
- SignOn Once Identity Providers, which are agency management system solution providers, will send an attribute in the security token to indicate the user went through an MFA process when they connected to their systems.

For Agency Leadership

- Educate the agency staff about MFA and required workflow changes.
- Don't wait; proactively contact carriers to inquire about their plans for MFA.
- Create separate IDs for each associate. Shared IDs can create security problems.

ID FEDERATION IS AVAILABLE TO DISCUSS HOW SIGNON ONCE CAN HELP SOLUTION PROVIDERS AND CARRIERS ADDRESS IMPLEMENTATION.

- One password for all insurance logins
- Maximum security with minimum pain
- A cooperative effort among insurance colleagues

About ID Federation

ID Federation is a nonprofit group of volunteer leaders committed to working for the common good of the insurance industry. They include representatives from carriers, technology providers, industry associations and agencies. These volunteers collaborate on critical issues facing our industry related to customer experience, workflow efficiency and data security. These experts in technology and business — with legal input as needed — seek to eliminate the legacy processes that have hindered the industry for decades, replacing them with modern technology for ID and password management.