2FA is on the Way!

Wait, what? 2FA? That's "two-factor authentication," which is an identity and access management security method that requires two forms of identification to access resources and data.

2FA gives businesses the ability to monitor and help safeguard their most vulnerable information and networks.

In the latter part of this year, Fidelity will be making 2FA mandatory for all participants. So, it will be important to have your phone number and personal email addresses on file with AHRP ahead of that roll-out to make sure you will be able to successfully complete the authentication process without having to call AHRP at 800-730-2477. Go online and update your profile with your personal cell phone number at AHRP.com.

How does 2FA benefit you?

Businesses use 2FA to help protect their employees' personal and business assets. They do this by preventing cybercriminals from stealing, destroying, or accessing your internal data records for their own use.

The advantages of 2FA are endless. For example, with 2FA, there's no need for users to carry or download a token generator, or an app associated with one. The websites of most businesses use your mobile device to text, call, or use a personalized 2FA to verify your identity.

How it will be used at AHRP?

- **Two-factor authentication** at log-in and for high-risk transactions
- **Real-time security text alerts** for transactions
- **Customer Protection Guarantee** automatically enabled for clients who provide personal contact information – and rest assured neither Fidelity nor AHRP will ever sell or use your personal contact information for marketing purposes

What are the various authentication methods?

There are a number of methods used to verify your identity through 2FA. Here are some of the most popular options:

Hardware tokens

Businesses can give their employees hardware tokens in the form of a key fob that produces codes from every few seconds to a minute. This is one of the oldest forms of two-factor authentication.

Push notifications

Push two-factor authentication methods require no password. This type of 2FA sends a signal to your phone to either approve/deny or accept/decline access to a website or app to verify your identity.
~Like PING ID

SMS verification

SMS, or text messaging, can be used as a form of two-factor authentication when a message is sent to a trusted phone number. The user is prompted to either interact with the text or use a one-time code to verify their identity on a site or app. (This option will be coming soon to AHRP, so get ready!)

Voice-based authentication

Voice authentication works in a similar way to push notifications, except that your identity is confirmed through automation. The voice will ask you to press a key or state your name to identify yourself. (This option is available now on the Fidelity 800.)