GREENLEAF TRUST

Perspectives

APRIL 2019
VOLUME 28, ISSUE 4

Introducing Multi-Factor Authentication to Your Retirement Plan Account

Michelle M. Gray
Participant Services Specialis

If you're like most people, you've either personally been a victim of identity theft, or you know someone who has. In fact, in 2017, 16.7 million Americans were victims of identity theft and $16.8 billion dollars were stolen, which was an increase of 12% from 2016. In 2017, 14% of all fraud complaints were related to identity theft and were the third most reported complaints to the Federal Trade Commission.

When thinking about what accounts or assets might be at risk of identity theft or cybercriminal attacks, you may not immediately think of your retirement plan. Perhaps the first thing that comes to mind is your bank accounts or credit cards. Unfortunately, employer sponsored retirement plans are not exempt from cyberattacks and have experienced a substantial increase in cyberattacks over the past few years.

> "... employer sponsored retirement plans are not exempt from cyberattacks and have experienced a substantial increase in cyberattacks over the past few years."

Greenleaf Trust works hard to ensure your retirement plan assets and personal information are protected. As part of this process, effective this month, we are implementing a multi-factor authentication system. While it may perhaps be a bit of an inconvenience to add an additional step to your login process, we feel that it's a vital part of keeping your information and your assets safe.

Multi-factor authentication (MFA) grants a user access only after they provide two or more pieces of evidence (factors): knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is).

Once we implement MFA, you will need to have either an e-mail address or cell phone number in your account in order to receive a one-time PIN. When you attempt to login with your user ID and password, the system will ask you where you'd like your PIN sent. It can either be e-mailed to you or texted to you. Once the PIN is sent to you, you will have 5 minutes to enter the PIN. After 5 minutes, the PIN will expire and you will be required to request a new PIN. The PIN will contain both letters and numbers and is case sensitive, so it's very important to enter it exactly as it is sent to you. If you are logging in from a personal device (your personal computer, tablet or cell phone), you may request that the system remember the device, which means it will remember the device for 180 days. During that 180 days, you will not be required to enter a PIN during subsequent login attempts. With a remembered device, you will only need to repeat the multi-factor authentication process every 180 days (approximately 6 months).

If you attempt to log in and do not have an e-mail or cell phone number on file, you'll be instructed to call our participant call center to provide an e-mail address or cell phone number to us.

Although we realize this new process may be a slight inconvenience, we feel that it's an important part of keeping your personal information and plan assets safe. If you have any questions on multi-factor authentication, or if you need to provide us with an e-mail address or cell phone number, please call our participant call center at (866) 553-8400.