GREENLEAF TRUST

Perspectives

OCTOBER 2018
VOLUME 27, ISSUE 10

Retirement Account Cybercrime on the Rise

Lisa A. Hojnacki
Participant Services Coordinato

Identity theft and the presence of cybercriminals is on the rise and can have devastating effects on individuals and businesses alike. More recently some of these criminals have turned their attention to employer sponsored retirement accounts, such as 401(k)s. While it is generally far easier and faster for thieves to abuse credit card and bank accounts, some perpetrators are drawn to the bigger potential payout of retirement accounts. In light of the recent large security breaches of companies like Equifax and Target, the fire alarm has been sounded and retirement plan administrators are taking notice, intensely focusing on the issue of cybersecurity.

As plan fiduciaries there is a broad duty under the Employee Retirement Income Security Act (ERISA) to act solely in the interest of the plan participants and beneficiaries. This requires plan fiduciaries to take action to serve and protect plan participants and beneficiaries and Greenleaf Trust is doing just that.

In an effort to prevent fraudulent online account access for our participants, we are implementing Multi-Factor Authentication (MFA) for personal web account access. This is a method of confirming the account user's identity through multiple account verification steps, such as a known password and an unknown one-time PIN generated by the authentication system.

At the same time the multi-factor authentication system is released, we will also be adding an additional security step, which will require a copy of a government issued photo ID for large distributions for those submitting a hardcopy paper form.

While it is essential that plan administrators take swift measures to protect plan assets and individual plan participants themselves, there are also things that you as an individual can do to protect yourself. Following are three easy tips for protecting your retirement savings account from cybercrime.

> "While it is generally far easier and faster for thieves to abuse credit card and bank accounts, some perpetrators are drawn to the bigger potential payout of retirement accounts."

Tip No. 1

Apply some of the following best practices when accessing your online accounts. Use passwords and storiethem safely. Don't access retirement accounts using shared computers or open WiFi networks. Add email alerts to your account that notify you when important changes are made. Be sure to have updated phone numbers and emails on file for multi-factor authentication and in the event you need to be notified of a security breach.

Tip No. 2

Be on the lookout for phishing emails in which cyber criminals try to gain personal information via deceptive means such as legitimate looking emails with fake web links or harmful attachments. Only open emails from trusted, legitimate sources. A useful slogan to keep top of mind is, "If you see a link, stop and think!"

Tip No. 3

Consolidate your retirement plans from former employers. Many of us wind up with multiple employer sponsored retirement savings accounts, and believing it's a hassle to move the money, we leave it behind in a former employer

account. This can increase exposure and risk to your account security by simply allowing for more access points to your sensitive account data. Work with the company HR department to find out if you can roll over former employer sponsored retirement accounts, which avoids taxes and penalties.

In today's world, most of us rely on the convenience of online tools and yet these tools are the very thing that can make us susceptible to cybercrime. At Greenleaf Trust our Business Information Services team works with the Retirement Plan Division to continue our impeccable history of protecting our participants' sensitive account information. We are pleased to be implementing these new security processes to thwart the rising attempts of cybercriminals now and in the future.

"...our Business Information Services team works with the Retirement Plan Division to continue our impeccable history of protecting our participants' sensitive account information. "