DUNBAR BENDER & ZAPF
retirement plan actuaries and consultants

Fraud Attempts Targeting Participant Distributions: How You Can Protect Your Plan - November 2018

Fraudulent distribution request from participant 401(k) accounts is a fast growing trend in identity theft. Individuals claiming to be a plan participant will contact a customer service center pretending to be a plan participant in order to request a retirement plan distribution.

These criminals have done their research and have excessive amounts of personal information, such as social security number, dates of birth, pet names, etc. Identity thieves can use a variety of methods to steal your information, from phishing scams to buying personal data online. They also take advantage of company data breaches to gain sensitive information that can be used for fraud.

Recordkeeping platforms, investment companies and TPA firms are taking measures to protect participants' online information with security programs, online information monitoring, and other internet safety measures to help ensure data is protected from hackers. They have employed various techniques; these techniques range from simple verifying that the account name and bank information match participant data, to complex voice recognition and background noise authenticity.

What Can Participants Do To Help Keep Their Accounts Secure?

- Create their own online access to their retirement account with a user profile.
- Check their retirement account often for any discrepancies in your account information or balance.
- If available, set email alerts to notify when changes are made to the account or request a two-step verification where a one-time use access code is sent to the participant via text or email.
- Pay attention to any notices from about account changes, such as email or password.
- Don't use security questions that hackers could find the answers to online or on social media.
- Employers should have a plan in place for securely handling and protecting sensitive information.