Expert Q&A on Retirement Plans and Cybersecurity

PRACTICAL LAW EMPLOYEE BENEFITS & EXECUTIVE COMPENSATION

Search the Resource ID numbers in blue on Westlaw for more.

An Expert Q&A with Todd Larson of Sentinel Benefits & Financial Group discussing cybersecurity and retirement plans.

Who are the targets for cyber predators and how is the current environment conducive to attacking those parties?

Cyber predators determine the most vulnerable parties and act on them. In the retirement plan arena, this includes both individual retirement plan participants, plan sponsors, and recordkeepers. There are a number of factors that lead cyber predators to attack retirement plan participant accounts:

- **Retirement plan account balances.** The average 401(k) plan balance is relatively large. This provides for an enticing reward for cyber predators to act.
- **Frequency with which participants check account balances.** Most participants do not routinely check their account balances and probably check their accounts between a few times a year and annually. Because of this, cyber predators' access to accounts can remain undetected by participants for long periods of time.
- **Authentication.** In the age of internet transactions, account authentication is the key to opening doors (and closing them) for cyber predators. At a minimum, accounts are required to be authenticated with a user name and password. Other personal information is also handy to add layers of authentication, such as an email address and cell phone number. Since most participants do not routinely access their accounts, the personal information can be incomplete or stale. Recent hacks of large US firms has caused the need for retirement plan recordkeepers to stay ahead of the curve and enhance their authentication process by using multifactor methods. Additional capabilities to monitor transaction activities is also necessary for these recordkeepers.
- **Technical acumen.** Many participants, especially some of those with large account balances, are older and tend not to be the most technically savvy participants. These individuals can be better targets for cyber predators. Some of these individuals have very public profiles like senior managers and "C" level executives. Collecting information on them is easier than other lower profile participants and can be done using the web and email phishing tactics.

If plan sponsors or recordkeepers are required to authenticate participant accounts, why are cyber predators still able to gain access to those accounts?

The typical plan sponsor or recordkeeper processes payroll related data from their clients, including:

- Social security numbers.
- Addresses.
- Account balances.
- Other employee information.

Most recordkeepers do not have a lot of payroll related data to work with unless users add their own personal data. Hackers always look for ways to infiltrate accounts with recordkeepers that do not have strong authentication strategies and operating procedures to defend themselves. These strategies include frequent password resets and account information changes.

What strategies can be used by plan sponsors or recordkeepers for more effective authentication and overall security?

For more effective authentication, plan sponsors and recordkeepers can:

- **Require participants to use more diverse data.** There are currently services that require participants to utilize more advanced authentication information. For example, some third-party services require information on mortgages and car loans for authentication. This information adds another layer of protection because it may not be readily available on the dark web or through other hacking means. An example of this type of authentication question is, "Approximately how much was your first mortgage?"
- **Make the authentication process more complex.** In addition to more diverse data, plan sponsors and recordkeepers can use other advanced methods of identification, including multifactor and biometric identification. Instead of merely signing on with a username and password a fingerprint or code texted to the cell phone on record makes the login more secure.

Plan sponsors and recordkeepers can also implement a combination of both requiring participants to use more diverse data and making the authentication process more complex.

There are also other simpler strategies that can be implemented. Plan sponsors or recordkeepers can encourage participants to provide innocuous answers to security questions. For example, a more secure answer to the questions "What is your mother's maiden name" or "What is your high school team's mascot?" might be "pickles" or a random word that cannot be guessed by looking at the participant's Facebook page or through Google searches. Since the point of attack can also be over the phone, requiring more data from participants may also be a viable solution for plan sponsors and recordkeepers. For example, personal cell phone numbers and email addresses (outside work) may help. It is important to realize that this solution is still not hack proof as phone numbers and email addresses change.

Plan sponsors and third-party administrators should also examine how they approve bank transfers, distributions, and loan approvals. Existing workflows need added checks and more review even if transaction and service levels are affected.

Besides changes to authentication, what else should plan sponsors and recordkeepers be doing to prevent cyber predators from gaining access to participant accounts?

There are numerous other steps plan sponsors and third-party vendors can take to ensure that cyber predators do not gain access to participant accounts, including:

- **Know your risks and threats.** Businesses should conduct risk assessments from a technology perspective. This is done through technical leaders working with business leaders in creating and testing hacking scenarios. Businesses should also have disaster recovery and business continuity plans that take cybersecurity into account.
- **Create Additional Internal Controls**. Businesses should be prepared to work to improve the security associated with retirement plan transactions, including partnering between plan sponsors and recordkeepers. This should include analyzing patterns of transaction behavior, account changes, and access frequency.
- **Know your data.** The accidental email of a spreadsheet can often cause more damage than an external hack or internal data theft. For a better handle on data, businesses should be able to answer the following questions:
  - where do your "spreadmarts" or legacy spreadsheets with sensitive data reside?
  - do the spreadmarts have client information on them?
  - are there access controls to ensure the wrong employees cannot access data?
  - are there scanning tools to look for and prevent accidental data loss and intentional loss?
- **Educate and promote awareness.** All employees of the plan sponsor or recordkeeper should think of client data as a precious valued asset each time they interface with it. As such, they need to partner and work with IT and clients to keep it secure. Training and security screening reviews are best practices.
- As cyber predators evolve, businesses need to also actively evolve their defensive strategies, which starts with awareness. Awareness includes examining what other companies are doing within your industry and keeping tabs on these best practices.
- **Know your vendors.** In an age where systems are hosted and cloud technologies and IT support strategies allow for distributed computing, companies need to do their homework. Companies also need to make sure that vendors are secure. This includes ensuring vendors contracts are in place and conducting active due diligence as part of regular policy and procedure. These are key elements for basic vendor management.
- **Gather the right security tools.** Technology is constantly evolving with tools to defend against data loss, and attacks are becoming more sophisticated. Companies need to dedicate resources to monitor evolving technology in the marketplace. The use of these tools is becoming more and more a business responsibility where traditionally IT has controlled this function.

Why should plan sponsors be pay attention to all of this?

Plan sponsors should pay attention to cybersecurity and work together with recordkeepers to keep participant data and retirement plans safe. Plan sponsors should be especially concerned with cybersecurity because:

- **Plan sponsors approve disbursement transactions**. Plan sponsors typically must approve disbursement transactions and have the final say in the disbursement.
- **Potential fiduciary liability.** It is not always clear where fiduciary responsibility lies in the event people, processes, or systems fail and funds are stolen. Each situation can vary on a case by case basis.

Plan sponsors should ensure that recordkeepers have systems and processes to support participants and that they can execute secure transactions and account maintenance. All parties need to work together to enact best practices and proper checks and balances.