SCHNEIDER DOWNS
Wealth Management

Where Cybersecurity and Fiduciary Responsibility Meet

It's rare to go a day without seeing a headline about a data breach, fraud, ID theft, or some other cybersecurity issue occurring. It's a constant battle that businesses and organizations have to wage to stay ahead of hackers and fraudsters who want to steal their data and take control of their systems.

Certain attacks constitute a specific form of identity theft known as account takeover fraud. Account takeovers typically leverage personally identifiable information (PII) and website credentials compromised in data breaches and avoid triggering credit monitoring alerts since they are not associated with the opening of a new account.

As a plan sponsor, you need to make sure the vendors and providers that have access to your employees' personal data and workplace accounts are safeguarded against data breaches and hackers. It's your obligation to vet your providers and ensure that they have strict controls in place to protect employees.

Schneider Downs Implements and Recommends these Best Practices

Account Creation

In many cases, setting up an online account for an existing retirement account requires knowledge of certain personally identifiable information, such as a mailing address, Social Security number, or account number. Because this type of data is regularly compromised via data breaches, Schneider Downs recommends that additional verification steps be added to online account creation processes.

Additional verification steps may include:

- A one-time code sent to the email address or mobile phone number on file for the account
- Integration of a third-party identity verification service into the online account creation process
- Allowing account owners to "lock" their account to prevent the creation of an online account without going through a separate unlocking procedure

Schneider Downs Retirement Solutions works with partner firms and their employees to set up retirement accounts as employees become eligible to participate in the company's retirement program. System-generated eligibility reports are based on completed census data provided by the plan sponsor immediately following the end of each payroll period. Participants may enroll online through the participant website or by completing and executing a hard copy enrollment form.

Participants may access the participant website by entering a default username and password, which must be changed upon initial login. Participants logging in for the first time will be directed through a series of election options, including personal information, contribution amounts, investment elections, etc. The final step presents a summary of all elections for approval by the participant. Once approved, the participant is provided with a transaction confirmation number and a confirmation email is sent to the email address of record.

Session Management

Attackers often attempt to compromise accounts by using password dumps from one of the various data breaches that have occurred in recent years. These attacks typically follow one of two strategies:

Continued on back

1. Attempting to reuse compromised passwords with the original username/email address (in the hopes that individuals have reused a password across multiple online accounts)
2. Password spraying, or attempting to use a compromised password across many target accounts with the goal of evading account lockout thresholds

In order to reduce the risk of these types of attacks, Schneider Downs recommends the following baseline settings:

- Multi-factor authentication (MFA) be implemented either as a required or optional configuration for all plan participants
- Device trust settings should default to untrusted; and the implications of trusting shared devices should be made clear
- Session timeouts should be configured to 30 minutes or less
- Account lockouts should be configured to occur when an incorrect password is entered five or more times in the span of no more than one hour

Advanced detective controls implemented by industry leaders include:

- Analysis of source IP addresses and other system information to identify non-typical geographic locations and potential password spraying attacks
- Behavioral analytics to establish a baseline of user behavior and alert on suspicious activity
- Blacklisting passwords that are known to have been compromised

Schneider Downs Retirement Solutions utilizes multi-factor authentication (MFA) to enhance data security protection for our partner firms and their retirement plan participants. When MFA is enabled for a plan, participants will be required to enter a one-time PIN that is sent to their mobile phone number in order to login to their online retirement account.

We require that a participant's second form of contact come from the plan sponsor in order to safeguard the integrity of the information.

Further, Schneider Downs Retirement Solutions engages a third party to complete a System and Organization Controls for Service Organization (SOC 1® Type 2) report, which can be provided to prospects and clients upon reasonable request. This report details the suitability and design and operating effectiveness of various control objectives.

Transaction Monitoring

In order to evade detection, many criminals will make small adjustments to account settings over the span of days or weeks. This activity will typically culminate in the distribution of funds to a throwaway bank account. To aid in detection of fraudulent activity, Schneider Downs and account owners have the ability to configure a variety of alerts to be sent to their email address of choice.

Actions that may trigger alerts include:

- Online account creation
- Account distributions
- Loan distributions
- Loan payments
- Changes to investment elections
- Investment rebalancing
- Changes to beneficiaries

Schneider Downs implements by default all of the alerts noted above, which are sent to the email on file as provided by the employer sponsoring the retirement program. Further, before a distribution may be processed, our team will request information to confirm the identity of the requestor.

Data Handling Procedures

Some procedures, such as back office activities and phone conversations, can sometimes be manipulated by scammers.

For example, scam artists often pose as an account owner on the phone and employ various social engineering tactics to gather information they can later use to compromise an account. Additionally, sensitive account information may be stolen intentionally via "dumpster diving" or as a crime of
opportunity by individuals passing through an area where sensitive information is left in plain sight.

Schneider Downs recommends the following:

- A clean desk policy
- Secure document disposal policies
- A documented procedure for establishing identity over the phone
- Regular training for all staff on data handling procedures
- Vet and understand data sharing policies of third-party providers

Schneider Downs Retirement Solutions' control environment reflects the philosophy of senior management concerning the importance of securing financial data and information. The importance of security is emphasized through the establishment and communication of policies and procedures and is supported by investment in resources and personnel to carry out the policies.

Schneider Downs has a dedicated information security team consisting of a chief information security officer (CISO) and senior security specialist responsible for management of information security throughout the organization. Specifically, the information security team and CISO are responsible for developing, maintaining and enforcing Schneider Downs Retirement Solutions' Information Security Policy (ISP). The ISP is reviewed annually by the CISO and is approved by the firm's Security Steering Committee. These standards and policies address the management and implementation of security controls, ranging from the physical security of facilities and equipment to the logical security at the data element layer.

Our heightened level of diligence around data and privacy security is especially important given some of the litigation issues that have been raised recently. Two recent cases have brought into question how participant data collected by a plan's third party recordkeeper can and should be used for non-plan purposes. For example, certain recordkeepers have shared the investment data and financial asset information that they acquire through the normal course of business with affiliated companies to solicit plan participants to sell other non-plan related products like an IRA accounts, life insurance, credit cards, and brokerage accounts. The underlying issue at hand regarding this dynamic and whether or not it constitutes a break of fiduciary duty boils down to whether participant data is considered to be a "Plan Asset" under the Employee Retirement Income Security Act of 1974, as amended (ERISA), which is not currently spelled out in the legislation.

For this reason, it is increasingly important that plan sponsors stay abreast of developing litigation and review service agreements with third-party recordkeepers and administrators to understand what types of data are collected and retained by such vendors, and what those vendors are able to do with such data. At Schneider Downs Retirement Solutions, we do not share participant level data with third-parties without plan sponsor approval, to mitigate the possibility of it being used for unintended purposes.

If you have questions related to our retirement services, please contact our offices at sdretirement@schneiderdowns.com or visit our website, www.sdretirementsolutions.com.