Playing it safe: Cybersecurity risks to retirement plans

Technology, Privacy, and eCommerce

Companies are increasingly moving from paper records to electronic records, and retirement plan records are no exception. Employers transmit data to third-party recordkeepers electronically, and 401(k) plan participants typically rely on online platforms to access, monitor, and direct their plan accounts. Recent estimates place the dollar value of 401(k) and similar accounts at more than five trillion dollars, and these balances continue to grow as fewer and fewer companies offer traditional defined benefit pension plans.

Given the vast amounts of money held in these accounts and the increasing reliance on online platforms to manage them, 401(k) and similar plan accounts have become prime targets for two types of cyberattacks:

- Theft of sensitive participant data, which could ultimately lead to identity theft; and
- Theft of participant retirement funds, through fraudulent online transactions.

With the significant data breaches in recent years and the prevalence of increasingly sophisticated fraud schemes, a successful, large-scale attack on retirement plans appears almost inevitable. Even so, there is no comprehensive federal regulatory regime that governs retirement plans and their cybersecurity obligations, and case law offers limited guidance. Although there is a focus on cybersecurity and data privacy at the state, federal, and international levels, protection standards vary and their applicability to US retirement standards is unclear. This legal uncertainty makes it difficult to identify the exact protections plan fiduciaries must implement to avoid liability for failing to adequately preserve participant data or plan account balances. Given the potential dollar amounts at stake, plan fiduciaries should monitor evolving cybersecurity threats and industry standards for dealing with them, and take steps to avoid potential attacks on their own plans. This article evaluates the current legal landscape and highlights some best practices for plan fiduciaries to reduce the cybersecurity risks to their plans.

Current legal standards

Currently, there is no federal cybersecurity statute governing retirement plans. While the Health Insurance Portability and Accountability Act (HIPAA) contains comprehensive rules regulating the use and security of health plan data, there is no comparable law that covers retirement plans. The Employee Retirement Income Security Act of 1974, as amended (ERISA), is silent on data protection in the form of electronic records. Similarly, courts have not yet decided whether sensitive participant data is a plan asset subject to ERISA's fiduciary standards or whether managing cybersecurity risks is an ERISA fiduciary function. This is significant, because if protecting participant data and managing cybersecurity risks is a fiduciary obligation, and a fiduciary fails to meet this obligation, ERISA imposes substantial penalties, including a requirement that the fiduciary make the plan whole for any losses suffered as a result of its failures.

Although ERISA is silent on cybersecurity obligations, it does impose general standards of care on plan fiduciaries:

- Fiduciaries owe a duty of loyalty to plan participants, and must discharge their duties solely in the interest of plan participants and beneficiaries. Ignoring online threats could potentially violate this duty.
- Fiduciaries must act prudently, with the care, skill, and diligence that similarly situated fiduciaries might use. If various cybersecurity protections have become standard practices for plan fiduciaries, then a fiduciary risks breaching this duty if it fails to implement similar safeguards

The conservative approach is to treat ERISA as requiring plan fiduciaries to take at least some steps to guard electronic access to both monetary assets and sensitive participant data, and to periodically re-evaluate evolving threats and changing best practices.

> "Given the potential dollar amounts at stake, plan fiduciaries should monitor evolving cybersecurity threats and industry standards for dealing with them, and take steps to avoid potential attacks on their own plans."

Beyond ERISA's general fiduciary standards, recent legislative activity highlights the continued scrutiny on cybersecurity and data privacy, and underscores the need for plan fiduciaries to begin focusing on these issues:

- In February 2019, two legislators asked the Government Accountability Office (GAO) to examine data protections, processes, and procedures within the private retirement system. They requested that the GAO study issues such as the efforts that employers are taking to safeguard plan assets, the response required in the event of a data breach, the value of cybersecurity insurance, whether current laws and regulations adequately protect participants against cybersecurity risks, and what steps other countries are taking to protect their private retirement assets.
- States have begun to enact their own data privacy and data breach rules. Additionally, there are data privacy laws that apply to various industries (such as financial industries). While ERISA would arguably preempt many of the state rules and the sector-specific rules likely do not apply, it highlights an increasing desire to get companies to focus on preventing data breaches and act appropriately in the event of a breach.
- Other countries are responding to similar attacks and imposing various protections. Most

notably, the European Union passed the General Data Protection Regulation (GDPR), which took effect in May 2018. GDPR sets new, stricter standards of accountability for companies that collect, process, and use data gathered from European Union citizens, and imposes strict breach notification and data documentation requirements. It is viewed as one of the most comprehensive data protection regimes in the world. While it does not generally apply to US-based retirement plans, it is yet another statute that highlights the concerns over data privacy and could serve as a model for future US rules.

Retirement plans may not be subject to specific cybersecurity obligations, but there clearly is a heightened awareness and concern over these types of issues. These plans are vulnerable targets, and if participants lose their retirement savings, there likely will be litigation to hold someone accountable. Plan fiduciaries should therefore be evaluating their current practices and implementing additional protections as needed.

Evolving standards

As this area promises to be a focus for regulators, legislators, and cybercriminals, it is important to work closely with human resources representatives and plan service providers to proactively manage cybersecurity risks. In coming years, we expect a growing body of guidance, whether through statute, regulation, or the development of a body of case law.

> “It is important to remember that although employers may hire third-party service providers to administer and handle participant accounts, plan fiduciaries are still required to provide prudent oversight.”

Action items

Below are some proactive steps plan fiduciaries faced with protecting participant data and account balances can take:

Stay educated

Plan fiduciaries should educate themselves about the types of potential security threats, and what both third-party service providers and other employers are doing to prevent them. While plan fiduciaries do not have to understand the exact mechanics behind these threats, they should know enough to ask intelligent questions and understand market practices.

Monitor third-party service providers

It is important to remember that although employers may hire third-party service providers to administer and handle participant accounts, plan fiduciaries are still required to provide prudent oversight. This means that plan fiduciaries should:

- understand the steps their service providers are taking to protect participant data and account

balances. They should question service providers about their practices in handling sensitive plan data and what they are doing to prevent breaches. This can be done as part of the initial hiring process, but plan fiduciaries also should receive periodic updates or reports on these practices so that they can effectively monitor their service providers.
- review cybersecurity provisions in service agreements. Contractual provisions might address: (i) maintenance of a security program that meets accepted industry standards, (ii) obligations in the event of a breach, (iii) liability in the event of a breach, (iv) the plan fiduciary's right to audit the service provider's practices, and (v) the ability to renegotiate cybersecurity provisions as technology and threats evolve.

Understand internal risks

Cybersecurity is often viewed as a service provider issue rather than an employer obligation. However, plan fiduciaries should review the employer's own practices for exchanging participant data and account information. For example, the manner in which human resources personnel transmit information to the 401(k) plan recordkeeper or other service providers could leave the employer vulnerable to an attack. Additionally, if the employer's anti-virus software or firewall is out of date, sensitive information could be accessed.

Educate plan participants

Regardless of the protections third-party service providers or the employer put into place to prevent fraud and cyberattacks, individual participant behavior creates the most risk. Plan fiduciaries often educate participants about plan features and investment options, but rarely address basic account protection. Plan fiduciaries should consider drafting educational materials or hosting employee training sessions to:

- explain the dangers of sharing passwords, never changing passwords, or using passwords that are too simple.
- educate participants about the evolving security measures recordkeepers have available to help protect their accounts. These might include dual-factor authentication, automatic account lock features, or voice recognition software.
- recommend that participants periodically monitor their accounts (including the importance of receiving and reviewing account notifications), so that they are able to mitigate any damage in the event their account is compromised. Many participants set up their 401(k) plan accounts and forget about them, so they may not notice fraudulent transactions on their accounts for months. At that point, the window for taking any mitigating actions has often closed. This is particularly true for plans with large numbers of participants who have been auto-enrolled and may not even understand that they have an account balance.

Brenna Clark

Partner

Eversheds Sutherland

Brenna Clark, partner in the Atlanta office, focuses her practice on a range of employee benefits and compensation matters. She advises clients with respect to the design, implementation and compliance of qualified and nonqualified retirement plans, executive compensation arrangements, fringe benefits, and other benefit programs. She also provides employee benefits advice in corporate transactions.

Brittany Edwards-Franklin

Associate

Eversheds Sutherland

Brittany Edwards-Franklin, associate in the Atlanta office, counsels clients on a range of employee benefits matters, including qualified retirement plans, nonqualified deferred compensation, and executive compensation. She also advises on employee benefits aspects of mergers and acquisitions.