Employee Relations LAW JOURNAL
Electronically reprinted from Vol. 43, No. 4 Spring 2018

Employee Benefits

Cybersecurity for Retirement Plans

Mark E. Bokert and Alan Hahn

Many cybersecurity breaches have been reported over the last few years. The most notable of these is the recent Equifax breach. These types of breaches pose a threat to plan assets and personal data of participants in employee benefit plans. The main areas of concern include the unauthorized exposure of participants' personal information, the theft of money from retirement accounts, and the infiltration of service provider systems. The cost to a plan sponsor of dealing with a cybersecurity breach can be astronomical. Therefore, plan sponsors and fiduciaries should take steps now to address the risks posed by a cybersecurity attack and develop a strategy for managing those risks.

The Environment

Earlier this year, Equifax, one of the largest credit reporting agencies, disclosed that personal and financial information for around 143 million consumers was compromised in a cybersecurity breach that began in late spring. According to the company, the breach started in May of this year and continued until it was discovered in late July. The information that was hacked includes Social Security numbers, birth dates, driver's license numbers, and addresses. The breach also included credit card numbers for more than 200,000 customers and documentation related to disputes for some 180,000 customers. Unfortunately, this enormous data breach is not unprecedented. In 2013, personal information of approximately one billion Yahoo! users was compromised and, in 2014, the personal information of some 145 million Ebay users was also exposed.

Breaches also have occurred in the retirement plan area. In one case, a union pension plan's data was subject to a ransomware attack.

Mark E. Bokert is a partner and co-chairs the Benefits & Compensation Practice Group of Davis & Gilbert LLP. His practice encompasses nearly all aspects of executive compensation and employee benefits, including matters related to equity plans, deferred compensation plans, phantom equity plans, qualified retirement plans, and welfare plans. Mr. Bokert may be contacted at *mbokert@dglaw.com*.

Alan Hahn is a partner and co-chairs the Benefits & Compensation Practice Group of Davis & Gilbert LLP. His practice is devoted to advising clients of all sizes, including in the design and implementation of a wide variety of creative, unique, and tax-effective employee benefit plans and programs. Mr. Hahn may be contacted at *ahahn@dglaw.com*.

Ramsomware is a program that holds data hostage until the owner of the data pays a ransom (usually in bitcoin or actual dollars). Fortunately, the union pension plan had adequate backup of the data and was able to avoid paying the ransom. In another case, a hacker caused a government defined contribution plan to issue fraudulent loans from accounts of participants whose personal information had been stolen. Approximately 60 of these loans were issued to web profiles created by the hacker, costing participants over $2.5 million in plan assets. Other cases have occurred, but they have been largely underreported.

The expense of dealing with a cybersecurity breach can be substantial. These expenses may include the cost of notifying participants of the breach, investigating the breach, recovering data, restoring systems, hiring a public relations firm, reputational damage to the company, and the cost of restoring plan assets. There also may be legal costs; security breaches can trigger governmental investigations, penalties under federal or state law, and civil lawsuits.

The monumental size and high-profile nature of many of these breaches have placed fiduciaries of employee benefit plans on notice of the risk of cyberattacks. Fiduciaries should address these risks to avoid substantial cost and even personal liability.

The Legal Landscape

There are numerous state laws dealing with cybersecurity breaches in which personal information is stolen or otherwise comprised.[1] Generally, these laws provide that affected employees must be notified of the breach. They also may give affected employees a private right of action against the employer that failed to safeguard their personal information. Some states even require the employer to provide affected employees with identity theft and credit monitoring protection for a period of time following the breach.

In the area of employee benefit plans, federal regulation governing cybersecurity is not comprehensive. While the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA), governs the protection of health information used or generated by certain health, dental, and vision plans, there is no federal statute or regulation that applies comprehensively to cybersecurity for retirement plans. Many retirement plans are covered by the Employee Retirement Income Security Act of 1974, as amended (ERISA). However, ERISA's application to cybersecurity breaches is unclear. It is possible that ERISA would pre-empt state laws governing cyberbreaches. It is also possible that the fiduciary duty provisions of ERISA would apply to the protection of participants' personal information and data. Personal information may be "plan assets" under ERISA. To the extent the fiduciary provisions apply, then plan fiduciaries would be required to discharge their duties with the care, skill, prudence, and diligence under the circumstances

then prevailing that a prudent man acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims.[2] Plan fiduciaries also would be required to discharge their duties with respect to a plan solely in the interest of plan participants and beneficiaries.[3]

Several pronouncements issued by the U.S. Department of Labor (DOL) relate to protecting personal information in ERISA-covered plans. For example, in DOL Technical Release No. 2011-03, the DOL stated that in order for a plan administrator to use electronic media (e.g., a web site) for purposes of disclosing information about plan investments, the plan administrator must take "appropriate and necessary measures reasonably calculated to ensure that the electronic delivery system protects the confidentiality of personal information."[4] In addition, in DOL Regulation Section 2520.104b-1, the DOL stated that if a plan administrator discloses information about the plan electronically, it must protect the confidentiality of personal information relating to the individual's accounts and benefits.[5] Failure to follow either the technical advice release or the DOL regulation could result in civil penalties against the offending plan administrator.

Next Steps for Plan Fiduciaries and Sponsors

The growing trend is for plan fiduciaries to establish prudent procedures to protect plan participants' personal information and plan assets from cyberattacks.

Plan fiduciaries should engage their ERISA counsel to develop a reasonable yet comprehensive approach to dealing with cybersecurity issues for their employee benefit plans. Broadly, the approach should include a review of the plan sponsor's security systems and procedures, a review of the security systems and procedures of third-party service providers (such as the plan's third-party administrator), and communicating with plan participants to help maximize security efforts. Ideally, the strategy for dealing with cybersecurity issues for employee benefit plans should be integrated with the company's overall cybersecurity strategy.

The initial step for implementing a strategy is to identify who is responsible for implementing the strategy. Typically, this would fall upon the administrative and/or investment committee that oversees the plan. A discrete subset of committee members also could be tasked with the responsibility. An important consideration in selecting the committee or members who oversee the strategy is their ability to understand the data and the processes for storing the data.

The first thing the responsible fiduciary should do is evaluate the data security measures currently implemented by the plan sponsor. Coordinating this undertaking with internal IT departments is likely essential. The responsible fiduciary should seek to understand what data

is being used, where it is stored, and how it is accessed. Key components of the review will be to determine whether the data is encrypted and whether access to the data is adequately controlled and protected. The responsible fiduciary also should seek to understand when data is retained and when it is discarded. The responsible fiduciary also should evaluate backup and recovery plans and determine how frequently the plan sponsor's systems are tested.

Next, the responsible fiduciary should identify all service providers with access to plan data, and request and evaluate their cybersecurity programs and controls, including transmission and encryption protocols and procedures. If a service provider has additional security measures that it can offer the plan sponsor, the responsible fiduciary should consider implementing such additional security measures (examples include email alerts, restricting web site access for only recognized devices, and voice verification software). The plan sponsor's ERISA counsel should review the plan's service provider contracts to ensure they address data security, provide appropriate indemnities to the plan sponsor, and otherwise adequately protect the plan sponsor in the event of any loss due to a cybersecurity breach. Generally, service provider agreements should contain appropriate contractual obligations for data protection and a fair apportionment of risk between the parties to the contract. The contract should address compliance with applicable data privacy laws, adherence to relevant industry standards, and obligations of the parties in the event of a cybersecurity breach. The agreement also should address the level and type of insurance coverage the service provider maintains and whether third-party losses are covered.

Finally, the responsible fiduciary should consider communicating security tips to plan participants in order to bolster security efforts. Such tips could include creating strong passwords. Emails and Social Security numbers should not be used for either user names or passwords. The plan sponsor should require stronger passwords, such as those with at least nine characters, including at least one upper case letter, number, and punctuation mark. Plan sponsors also should require participants to frequently update their passwords and security Q&As. Participants should be reminded to keep their user names and passwords private and not to "save" them on their computer's browser. Participants also should be reminded to regularly access their accounts to ensure there has been no tampering or unauthorized access. If there has been unauthorized access of tampering, participants should be told where to report the breach.

Plan fiduciaries should document the steps they have taken to review and improve their employee benefit plans' data security, including communications with service providers and participants, and any changes implemented as a result of such review. To further manage the risk of a cybersecurity breach, plan fiduciaries should consider reviewing applicable insurance coverage. Traditional insurance coverage (fiduciary liability, errors and omissions, directors and officers, and ERISA bonds)

may not cover a cybersecurity breach or only provide limited coverage, so additional coverage may be desirable. Any insurance policy covering cybersecurity breaches should be reviewed carefully by someone who is familiar with such policies.

Conclusion

The Equifax breach and other high-profile breaches have put plan sponsors and fiduciaries on notice that the threat of cybersecurity attack is very real. Plan sponsors and fiduciaries need to do all they can in order to protect the personal information of participants and plan assets. Failure to act could be very costly. Plan sponsors and fiduciaries, along with their ERISA counsel, should develop a strategy for addressing and managing the risks of a cybersecurity attack. Such a strategy should include evaluating the plan sponsor's security systems and protocols, evaluating the security systems and protocols of the plan's service providers, and communicating with plan participants in order to maximize security efforts. Undertaking such a strategy is consistent with the standard of prudence by which all ERISA fiduciaries are required to abide, and will serve to protect the plan, plan sponsors, and participants to the maximum extent possible.

Notes

1. *See, e.g.,* Cal. Civ. Code §§ 1798.29, 1798.82*;* N.Y. Gen. Bus. Law § 899-AA, N.Y. State Tech. Law 208.

2. ERISA § 404(a)(1)(B).

3. ERISA § 404(a)(1).

4. DOL Technical Release 2011-3, Interim Policy on Electronic Disclosure Under 29 CFR 2550.404a-5 (September 13, 2011).

5. 29 C.F.R. § 2520.104b-1(c)(1)(i)(B).