Bloomberg Law®

Privacy and Security Law Report®

Workplace Issues

Many employers were only concerned with privacy and security for health plans covered by HIPAA and state laws, but protecting participant information in ERISA and other employee information that shouldn't be overlooked, the authors write.

Cybersecurity Risks and Liabilities for Employers, Retirement Plan Sponsors and Fiduciaries



By Greta E. Cowart, Marcus D. Brown and Theanna Sedlock

Introduction

Many employers historically were only concerned with privacy and security for health plans under the privacy regulations issued under the Health Insurance Portability and Accountability Act of 1996 (''HIPAA'') and State laws; however, there are other references to protecting participant information in ERISA and employee information that should not be overlooked. Data security experts consistently state that it is not ''if'' a breach will occur, but ''when.'' Employers send employee data to vendors for many purposes—payroll, leave management, disability management and retirement plan administration and record keeping.

While there are cybersecurity insurance policies, they are expensive and the terms and coverage must be carefully reviewed to determine what is covered because not every loss may be covered. A breach may trigger costs including state law penalties, costs related to breach notifications, post-breach employee protection, regulatory compliance and fines, public/employee relations/crisis communications, attorneys' fees and litigation costs, cybersecurity improvement costs, technical investigations, increased insurance premiums, increased financing costs due to the impact on profits, public relations image costs, operational disruption, impact on and losses in employee relations, devaluation of business reputation and loss of intellectual property.

Some plan fiduciaries commonly use electronic disclosure to fulfill responsibilities and may place the plan fiduciaries at risk for ERISA non-compliance, potential penalties and ERISA fiduciary exposure. Electronic distribution of plan information to participants and beneficiaries is utilized by many plan administrators to save the cost of copying and distribution. The requirements applicable for electronic distribution must be satisfied to utilize it.

ERISA, Electronic Delivery and Cybersecurity

The information an employer provides to a record keeper for a retirement plan may not be subject to HIPAA privacy and security, but it is still prudent to

 ISSN 1538-3423

protect that participant personal information as it often contains sufficient information for someone to steal a participant's identity. The data and information provided to a retirement plan record keeper or to a vendor for payroll or leave management often includes name, date of birth, address, Social Security number, information about compensation and other information.

While there is no regulatory scheme protecting the personal data provided to retirement plans, such as in the European Union or under HIPAA privacy and security for health plans, under federal law, that does not mean there is no obligation to keep the personal information secure. There is a protection requirement under ERISA, if a Plan Sponsor utilizes electronic methods of distribution of plan information. If a plan wants to disclose information through electronic media under the DoL regulation § 2520.104b-1(c), it must ensure that the electronic system used for furnishing the documents results in (i) actual receipt of the transmitted information, (ii) *it protects the confidentiality of personal information relating to the individual's accounts and benefits (e.g., incorporating into the system measures designed to preclude unauthorized receipt of or access to such information by individual other than the individual for whom the information is intended)*. . .

While this is in reference to the system used to furnish the documents electronically, in some circumstances this may apply to the outside retirement plan record keeper and also to the employer's own information system. The extent that such requirement imposes an obligation to protect the personal data of the participants and beneficiaries of a retirement plan has not been defined in regulations or other guidance issued by the U.S. Department of Labor (''DoL''). It does not require much creativity to see how failure to ensure adequate security of the participants' personal data might be used to claim a failure to provide a required disclosure and then the plan fiduciary may face an issue.

Potential Consequences—Participant Directed Investments

However, in EBSA Technical Release No. 2011-03 dealing with a secure continuously available website used to communicate the information about the participant-directed investment alternatives under the retirement plan, the DoL explicitly included as one of the conditions for utilizing the electronic media disclosure that ''The plan administrator takes appropriate and necessary measures reasonably calculated to ensure that the electronic delivery system protects the confidentiality of personal information.''

In order for a plan to be an ERISA 404(c) participant-directed investment plan, the plan must provide an opportunity for a participant or beneficiary to exercise control over assets in her account, and must provide the participant or beneficiary an opportunity to choose, from a broad range of investment alternatives, the manner in which to invest the assets of his account. A participant has the opportunity to exercise control only if: (i) under the terms of the plan the participant or beneficiary has a reasonable opportunity to give investment instructions. . ., and (2) the participant or beneficiary is *provided or has the opportunity to obtain sufficient information to make an informed decision* among the available investment alternatives. Thus, it is important that the investment information is provided in compliance with the electronic distribution requirements in order for the plan to provide sufficient information to meet the regulatory definition to be an ERISA § 404(c) plan.

For a plan that provides for participant direction of investments, it must meet certain disclosure requirements. The information disclosed must include general plan rights, information on administrative expenses, individual expenses (including disclosures on quarterly benefit statements) and certain disclosures made on or before the first investment. There also must be significant disclosures related to the investment alternatives, performance data, fees, expenses and restrictions and there must be a website providing information on investments and information must be presented in a comparative format.

However, if there is a failure to keep participant information protected and secure that results in a failure to comply with the electronic disclosure requirements, this may impact a number of DoL required disclosures. If the electronic disclosure requirements are not met and the participants do not receive the plan investment information in another manner, then the participants have not been provided the investment alternative information necessary for the plan fiduciaries to obtain the Fiduciary Relief potentially available to an ERISA § 404(c) plan. While merely failing to disclose the information required to qualify carries no civil monetary penalty consequences; it does have consequences as to whether the plan fiduciary obtains the ERISA § 404(c) relief. The plan fiduciaries could lose the ERISA § 404(c) protection if the information is provided solely via electronic disclosure and the participants' information is disclosed via a breach or hack. The participants may have received the information, but they would still have an argument that the plan sponsor's delivery of the plan or investment information was not correctly disclosed under ERISA because the electronic disclosure failed to comply with all of the requirements because it failed to protect the confidentiality of the participants' private information. This means the plan fiduciary may be potentially liable for participants' investment decisions.

Consequences—SOX—Blackout Notices

If the plan was required to provide blackout notices under ERISA § 101(i) or the mandatory notice of the right to diversify employer stock under ERISA § 101(m), the failure to provide these notices is subject to a civil monetary penalty of $131 per participant per day.

More ERISA Regulations to Come?

The 2016 ERISA Advisory Council report, issued in January 2017, on cybersecurity was focused on providing useful information to plan sponsors, fiduciaries and plan service providers. Plan sponsors and fiduciaries are told in the report that they should consider cybersecurity in safe-guarding benefit plan data and assets and when making decisions to select or retain a service provider. It is a report; so it is not a regulation or law, but merely recommendations based on the hearings held by the ERISA Advisory Council.

  PVLR ISSN 1538-3423

In administration of payroll, leave management, disability management, and in retirement plan administration, there are often multiple service providers receiving personally identifiable information (''PII'') for the employer or its plan and while some financial service organizations are subject to extensive regulation, there may be many service points for a retirement plan or an employer that are not regulated, resulting in a retirement plan's PII being vulnerable. Employers as well as plan fiduciaries deal with PII and should be equally concerned with having an appropriate cybersecurity management program.

The report concludes that based on the type of plan, its resources and to the extent the plan is bearing some or all of the costs of developing and implementing a cybersecurity risk management program, plan fiduciaries will need to determine the balance of preventive measures relative to the probability of the threat, the loss exposure, and the cost of protective action. This challenge suggests that a scalable, individualized cyber risk assessment strategy is the prudent starting point.

A cybersecurity risk management program would include prioritizing the program and its scope within the entity, orienting the scope within the entity, developing a current profile of the entity's current cybersecurity status, conduct a risk assessment, analyze gaps and implement an action plan that would include training personnel on cybersecurity policies and procedures, as frequently the greatest risk to cybersecurity is the human element.

Accounting Requirements

The AICPA issued in its Employee Benefit Plan Audit Quality Alert #365 that the plan sponsors are responsible for implementing processes and controls for a plan's systems, including mandating third-party service providers to secure and to restrict access to the plan's data. When plan administration services are outsourced, the plan administrator responsibility is to protect the security of the plan's records extended to the service provider's systems in order for the audit requirements to be met to obtain a clean audit report.

Employers, when contracting for services, may want to inquire about how accountants view the processes of the potential vendor as audits were developed to review these processes. The AICPA assesses internal controls and can produce a Service Organization Control Report (''SOC'') at one of two levels. A SOC 1 report is a report on controls at a service organization relevant to user entities' internal control over financial reporting and is specifically intended to meet the needs of the entities that use the service organizations and the CPAs that audit the user entities' financial statements by evaluating the effect of the internal controls. A SOC 2 report is a report on controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy and this is the report on the security of the systems and the ability of the service provider's systems to protect the data and confidentiality of the parties who utilize the service provider, such as a plan utilizing a record keeper.

Employers and plan fiduciaries considering vendors may want to inquire whether the vendor has a SOC 2 report, as this is a more extensive report on the vendor's system and its security protections. Another type of report is an ISAE 3402 report generated from an International Standard on Assurance Engagement. This is an international accounting standard audit and reports on the audit of an entity that provides services to user entities and such services are likely to be relevant to user entities' internal control as it relates to financial reporting. This type of engagement and report looks at whether the service organization's controls operate as described or whether its controls with respect to its services to other entities that are relevant to such other entities' financial reporting provide appropriate controls. The audit reviews the system, its design and controls, the effectiveness of such controls in protecting the integrity of the process and data, and its internal audit function.

Potential Labor and Employment Law Issues

The loss of sensitive personal information belonging to employees should be of significant concern to employers. While protection of personal information has lagged behind technology, employers should take precautions to protect their employees and avoid potential enforcement actions by governmental agencies, or civil claims brought under common law or various state statutes.

Recently, seven complaints were filed against Sony and consolidated into a single class action related to the hack Sony suffered in 2015 exposing its emails and personally-identifiable information of its employees including Social Security numbers, birthdates, home addresses, salaries, and medical records. Anthem also faced a class-action lawsuit after it suffered a hack into its own employees' information. Given these examples of common law claims brought against employers, it would be prudent to ensure that adequate security measures are in place to protect confidential employee information.

However, the Pennsylvania Supreme Court recently found that an employer did not have a duty to manage its computer systems to safeguard sensitive personal information collected from its employees. The data had been maintained on an internet-accessible computer system and in a data breach, the names, birth dates, Social Security numbers, tax information, addresses, salaries and bank information of approximately 62,000 current and former employees was accessed and stolen. The court held, ''[w]e find it unnecessary to require employers to incur potentially significant costs to increase security measures when there is no true way to prevent data breaches altogether.'' While this is one state court's position, it is not consistent with other legal trends.

Social Security numbers are commonly part of the data provided to a retirement plan record keeper or to other human resources vendors. Several states impose a statutory duty on employers to protect the privacy of employees' Social Security numbers. These statutes affect how employers process and use pay-related documents and reporting to record keepers for retirement plans. In Texas, for example, employers are generally prohibited from printing Social Security numbers on any materials sent by mail, including paychecks sent by mail. The law provides a ''safe harbor'' if certain conditions are met.

In addition, various states require employers to notify employees of any data breach that compromises personal information. For example, Texas Business &

Commerce Code § 521.053 requires a business that loses sensitive personal information through hacking or other means of unauthorized acquisition to promptly notify victims of the security breach. The Texas Workforce Commission, noting the dangers associated with the loss of sensitive personal information of employees, has taken the position that the statute applies to the employer-employee relationship.

Many state laws include private rights of action for disclosure of personal or private information. In addition to state privacy laws, we operate in a global economy and employees frequently transfer and work in different countries. Inbound employees' (inpats) personal information is frequently subject to the protection of laws in their country of origin and their personal information has other legal protections and potential violations of the privacy of such information may trigger other consequences and rights. With an increasingly global and mobile workforce, employers may need to consider whether there may be data transferred internationally with respect to certain employees and whether there may be laws beyond the U.S. laws that apply. Employers need to be mindful of the potential application of the laws of other jurisdictions if they have employees and vendors transferring data in and out of jurisdictions that are part of the EU or other jurisdictions with similar laws.

Other Regulation

The Federal Trade Commission has been regulating cybersecurity under Section 5 of the Federal Trade Commission Act, which prohibits deceptive business practices in commerce. The Federal Trade Commission is charged with protecting consumers, including protecting individual consumers from identity theft. The FTC may file lawsuits against businesses to enforce privacy- and security-related promises and to challenge business practices that cause substantial consumer harm as part of its enforcement of the statutory prohibition on unfair and deceptive trade practices.

Cybersecurity Insurance

As the cyber world and markets evolve, new insurance developed to protect against new risks in the e-world. Employers should inquire about vendor cybersecurity efforts and cybersecurity insurance and what it covers.

Summary

Security should be a consideration for every employer and retirement plan fiduciary.

If those are not sufficient reasons, the National Security Agency's list of software flaws that might permit hacks was mysteriously released in mid-August 2016 and reportedly places many large companies' IT systems at risk. So a new road map for hackers is out. Are you ready?

Cybersecurity Considerations in Selecting Service Providers—Due Diligence

1. Does the service provider have a comprehensive and understandable cybersecurity program?
2. Does the service provider have a SOC 2 report? Or an ISAE 3402 report?
3. What are the elements of the vendor's cybersecurity program?
4. How will the data be maintained and protected?
5. Will the data be encrypted when it is at rest? In transit? On devices?
6. Will the service provider assume liability for breaches? What are its breach procedures?
7. Is the encryption of data automated or manual?
8. Will the vendor assume liability for breaches?
9. Is there a limitation on the vendor's liability?
10. Will the vendor stipulate to permitted uses and restrictions on data use? Will it educate its personnel on such limits?
11. What are the vendor's procedures for notifying the employer of a breach of vendor's system? Are these procedures satisfactory?
12. Will the vendor provide regular reports on its security risk analysis results?
13. Will the vendor provide reports on its security monitoring?
14. When does the vendor train its personnel and contractors on security and how frequently is the training required?
15. If the vendor does not have a SOC2 report, does it subject itself to other external reviews or does it have an external certification?
16. What level or type of cybersecurity coverage does the vendor maintain?
17. Does the cybersecurity insurance provide ''first party'' or ''third party'' coverage?
18. What level of financial and fraud coverage is provided?
19. Does the vendor use subcontractors? Will the vendor require the subcontractor to comply with all of the specifications of this agreement? If not, what security protections are provided in the subcontractor agreements?
20. What controls does the vendor have over its assets, including after assets are retired or taken out of service? (e.g., are hard drives of laptops wiped clean of all contents when retired?)
21. What are the vendor's hiring practices, e.g. background checks?

  PVLR ISSN 1538-3423

PVLR ISSN 1538-3423