Bloomberg BNA

Tax Management
Compensation Planning Journal™

What Retirement Plan Sponsors and Employers Need to Know About Cybersecurity Risk and Liabilities

By Greta E. Cowart, Esq.
Marcus D. Brown, Esq.
and
Theanna Sedlock, Esq.[*]
Winstead PC
Dallas, Texas

INTRODUCTION

Many employers historically were only concerned with privacy and security for health plans under the Health Insurance Portability and Accountability Act (HIPAA)[1] and state laws; however, there are other references to protecting participant information in the Employee Retirement Income Security Act (ERISA) 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 all of the potential expenses or losses 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 cost to due to the impact on profits, public relations image costs, operational disruption, impact on and losses in employee relations (including impact on relations with affected collective bargaining units), devaluation of business reputation and loss of intellectual property. The total loss calculated for one company for one breach was $1.679 million.[2] In addition, there are also other laws protecting private information that should be considered.

Retirement plan sponsors and plan fiduciaries should consider cybersecurity with respect to their own systems and those of their retirement plan service providers. While there is no overriding federal law dictating security or privacy standards directed at retirement plans or the service providers to such plan, the retirement plan's data may remain largely unprotected unless the plan administrator requires that the plan's data be protected. Failure to take proactive steps to protect a retirement plan and its participants' data, may have undesirable consequences for the plan administrator and employer, as discussed below.

Some of the protections plan fiduciaries expect, as well as commonly used cost-saving tools such as elec-

---

[*] Greta E. Cowart (*gcowart@winstead.com*) is a shareholder with Winstead PC in Dallas. She practices in the areas of employee benefits, tax and executive and deferred compensation with a focus on health and welfare benefits and health-care reform implementation.

Marcus Brown (*mbrown@winstead.com*) is a shareholder in Winstead's Labor, Employment & Immigration Practice Group. He counsels and represents clients in all areas of labor and employment law in federal and state court, as well as before administrative agencies and arbitration panels.

Theanna Sedlock (*tsedlock@winstead.com*) is a member of Winstead's Labor, Employment & Immigration Practice Group in Dallas.

[1] Pub. L. No. 104-191.

[2] ''A Deeper Look at Business Impact of a Cyberattack,'' CSO Online Article (Aug. 25, 2016), http://www.csoonline.com/article/3110756/data-breach/a-deeper-look-at-business-impact-of-a-cyberattack.html.

ISSN 0747-8607

tronic disclosure, may be effective to fulfill responsibilities but place 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 fulfill disclosure obligations and save the cost of copying and distributing summary plan descriptions, participant account statements, participant-directed investment disclosures and many of the health plan disclosures. The requirements applicable to each type of electronic distribution must be satisfied so that the distribution of information complies with DOL regulations under ERISA and Internal Revenue Service regulations under the Internal Revenue Code (I.R.C.).[3] These requirements may differ. For example, only the ERISA regulations require that the plan sponsor protect the confidentiality of personal information.[4]

RETIREMENT PLAN DATA SECURITY

It is important that employers and retirement plan sponsors consider taking steps to ensure the security of participant information provided to plan record keepers or vendors. In this age of what seems to be perpetual announcements of breaches and hacking, it is critical that the employer can document its due diligence with respect to protecting the information of the retirement plan and the participants' private information. It is not only good business practice, but such security is required under compliance with ERISA's requirement for electronic disclosure, avoidance of penalties and exercising its fiduciary obligations because it relates to complying with disclosure requirements. It is important for the plan administrator to request that service providers comply with data protection standards and contractually have a binding legal requirement the plan administrators can enforce and to avoid negative comments in the management letter on the audit of the plan.

The security of participants' personal information is even more significant as plan sponsors increasingly outsource HR functions and transfer additional data to third parties, especially where the third-party contracts focus on statements of work and processes, but do not address data retention and security. Additionally, the advent of applications providing smart device access to one's accounts, including individual participant retirement plan account information, may pose a cybersecurity risk.[5]

ERISA, ELECTRONIC DELIVERY AND CYBERSECURITY

The information an employer provides to a retirement plan record keeper may not be subject to HIPAA privacy and security, but it is still prudent and a good business practice to protect participants' personal information as it often contains sufficient information for someone to steal a participant's identities. The data and information provided to a retirement plan record keeper or service provider often includes name, date of birth, address, social security number, account information, compensation and other information such as the beneficiaries and the beneficiaries' identifying information, which can be enough for a hacker to create identity theft issues for participants and/or beneficiaries.

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 regulations for health plans, that does not mean there is no obligation to keep the personal information secure. ERISA contains a protection requirement if a plan sponsor electronically distributes plan information. If a plan wants to disclose information through electronic media under 29 C.F.R. §2520.104b-1(c), it must ensure, among other things, that the electronic system used for furnishing the documents 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 individuals other than the individual for whom the information is intended).

While this is in reference to the system used by the plan sponsor 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 DOL. Failure to ensure adequate protection of an individual's personal information relating to the individual's accounts and benefits may result in an argument that the electronic delivery requirements were not satisfied and if those requirements were not satisfied, there may be a fiduciary issue.

Under the DOL regulation, electronic distribution of plan information to participants can be used with either (1) a participant who has the ability to effec-

[3] 29 C.F.R. §2520.104b-1(c).

[4] *Compare* 29 C.F.R. §2520.104b-1(c) *with* Treas. Reg. §1.401(a)-21.

[5] Eric Basu, *Cybersecurity Trends to Watch in 2017*, Business 2 Community (Jan. 23, 2017), available at http://www.business2community.com/cybersecurity/cybersecurity-trends-watch-2017-017.

ISSN 0747-8607

tively access documents furnished in electronic format at any location where a participant is reasonably expected to perform his or her duties as an employee; *and* with respect to whom access to the employer's or plan sponsor's electronic information system is a normal part of their duties; or (2) any participant who consents affirmatively, in either electronic or nonelectronic form, to receiving the documents through the electronic media and has not withdrawn such consent and has received certain notices with certain content.[6] While some guidance has considered providing information through continuously available websites,[7] none has eased the above two requirements, nor has any guidance explained what is covered by the requirement that the electronic system ''protect the confidentiality of personal information relating to the individual's accounts and benefits.''[8] However, a prudent plan administrator should ensure that participants' personal information is protected and its confidentiality preserved to protect the plan fiduciaries from claims arising out of failure to satisfy disclosure requirements, as at least a starting point and to avoid some of the enumerated consequences of a breach above.

NOT ALL DISCLOSURES ARE CREATED EQUAL

ERISA electronic disclosure regulations govern many required disclosures such as qualified default investment alternatives (QDIAs),[9] SOX notices,[10] qualified change in investment alternatives,[11] participant benefit statements,[12] investment alternative information,[13] COBRA notices and suspension of benefits notices.[14] It is important to remember which electronic standard applies to each type of disclosure and remember that the requirements for electronic disclosures were only loosened for participant benefit statements.

IRS Disclosures

There are also a number of disclosures, notices and distributions of information provided under the I.R.C., such as safe harbor notices for safe harbor §401(k) and §401(m) plans.[15] The I.R.C. also mandates a notice for qualified automatic contribution arrangements and eligible automatic contribution arrangements.[16]

However, for a plan administrator to fulfill the IRS required notice obligations for electronic delivery of notices, there are separate IRS requirements that are different from the DOL requirements for electronic disclosures. The regulations under the I.R.C. governing electronic disclosures do not include any reference to electronic security or maintaining the safety, confidentiality or integrity of the data in the manner that the DOL's regulation refer to ''protection of the confidentiality of personal information relating to the individual's accounts and benefits.''[17] This means that a vendor who fails to protect the privacy of participant information in a strictly U.S.-participant-only plan might not jeopardize the safe harbor nature of a §401(k) plan, but would jeopardize the protection of the plan administrator and plan fiduciaries related to certain disclosure required under ERISA and protection from liability for participant investment elections.

The IRS notice rules apply to participant elections, notices or elections under I.R.C. §104(a)(3), §105, §125, §127, §132, §220 and §223, as well as for any notice or election under a qualified plan under I.R.C. §401(a) and §403(a), SEP, SIMPLE and §457(b) plans.[18] However, such rules do not apply to notices required under Titles I and IV of ERISA.[19] The Treasury Regulations also do not apply to a suspension of benefits notice under I.R.C. §411(a)(3)(B) or to COBRA notices.[20]

Potential Consequences Under ERISA Individual Account Statements

So what consequences might flow from failing to comply with all of the requirements for electronically delivering plan information? The answer depends upon which disclosure requirement is not satisfied and which disclosure is impacted. Different disclosure failures trigger different penalties.

Individual account statements in a defined contribution retirement plan must be delivered both quarterly and annually[21] as well as upon request. Failure to deliver these individual account statements can re-

---

[6] 29 C.F.R. §2520.104b-1(c).

[7] Technical Release 2011-03.

[8] 29 C.F.R. §2520.104b-1(c)(1)(i)(B).

[9] ERISA §404(c)(5); 29 C.F.R. §2550.404c-7.

[10] ERISA §101(i). SOX is short for the Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204.

[11] ERISA §404(c)(4).

[12] ERISA §105.

[13] ERISA §404(c).

[14] 29 C.F.R. §2520.104b-1(c).

[15] I.R.C. §401(k)(12)(D), §401(k)(13)(E), §401(m)(11).

[16] I.R.C. §401(k)(12)(B), §414(w)(4).

[17] 29 C.F.R. §2520.104b-1(c)(1)(i)(B); Treas. Reg. §1.401(a)-21.

[18] Treas. Reg. §1.401(a)-21(a)(2).

[19] Treas. Reg. §1.401(a)-21(a)(3).

[20] Treas. Reg. §1.401(a)-21(a)(3)(i).

[21] ERISA §105.

ISSN 0747-8607

sult in a civil monetary penalty of $110 per day per participant.[22]

Participant benefit statements also can be delivered electronically pursuant to Field Assistant Bulletin (FAB) 2006-03, as modified by FAB 2007-03. The electronic delivery of individual account plan and benefit statements pursuant to the FABs must be executed in compliance with the I.R.C. requirements set forth thereunder.

Both of these FABs require the plan administrator to furnish benefit statements to participants in good faith compliance with applicable IRS requirements. Compliance with DOL's regulatory requirement is not the same as IRS requirements. However the IRS's requirements set forth under Treas. Reg. §1.401(a)-21 do not include any language providing for the protection of participants' personal information. Therefore, when IRS standards are used for electronic disclosure, protection of personal information is not required for the electronic delivery to be considered effective. It is curious that individual participant benefit statements with participant name and account information were allowed to be distributed using rules that did not require the plan administrator to ensure protection of the private information. Thus, there is at least an argument that the penalty should not apply to the participant statements because the confidentiality requirement does not apply when the IRS standards are used.

Potential Consequences — Participant Directed Investments

In Technical Release 2011-03, which discusses a secure website used to communicate information about participant-directed investment alternatives under a retirement plan, the DOL explicitly included as one of the conditions for utilizing electronic media disclosure a requirement that ''[t]he plan administrator takes appropriate and necessary measures reasonably calculated to ensure that the electronic delivery system protects the confidentiality of personal information.'' The Technical Release does not distinguish whose electronic delivery system must provide the protection of confidentiality, but it clearly included this security requirement in its temporary enforcement policy, and it remains in effect until the DOL issues further guidance in this area.[23]

Technical Release 2011-03 also does not define what it takes for a website to be ''secure'' so that the requirements for using this method of delivery of individual benefit statements and participant directed investment alternatives applies. This seems to indicate that the earlier good faith compliance using the IRS guidelines for electronic delivery are not sufficient, at least not with respect to disclosures related to participant-directed investments, because the Technical Release adds the requirement for protection of confidential information and does not incorporate the use of the IRS standards.

Distribution of information is also critical for participant-directed investments and for plan fiduciaries to obtain the provided limitation on the fiduciaries' liabilities with respect to participant investment decisions (Fiduciary Relief), to the extent it is available, under ERISA §404(c).[24] Fiduciary Relief does not relieve the plan fiduciary from prudently selecting or monitoring the investments or service providers.[25]

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.[26] A participant has the opportunity to exercise control only if: under the terms of the plan the participant or beneficiary has a reasonable opportunity to give investment instructions to an identified plan fiduciary who is obligated to follow such instructions; and the participant or beneficiary is *provided or has the opportunity to obtain sufficient information to make an informed decision* among the available investment alternatives.[27] Thus, it is important that the investment information is provided in compliance with the electronic distribution requirements in order for the plan to meet the regulatory definition of an ERISA §404(c) plan.

An individual account plan that provides for participant direction of investments must meet certain fiduciary requirements with respect to its disclosure of information.[28] The disclosure requirements include plan-related information, such as general plan rights and information on administrative expenses, individual expenses (including disclosures on quarterly benefit statements) and certain disclosures made on or before the first investment.[29] There also must be significant disclosures related to the investment alternatives, performance data, fees, expenses and restrictions; a website providing information on invest-

[22] ERISA §502(c)(1).

[23] Technical Release 2011-03.

[24] *See* 29 C.F.R. §2550.404c-1(b), §2550.404c-5(b).

[25] *Tibble v. Edison Int'l, Inc.*, 135 S. Ct. 1823 (2015) (*rehearing en banc* granted Aug. 5, 2016); *George v. Kraft Foods Global Inc.*, 641 F.3d 786 (7th Cir. 2011).

[26] *See* 29 C.F.R. §2550.404c-1(b)(1).

[27] *See* 29 C.F.R. §2550.404c-1(b)(2).

[28] *See* 29 C.F.R. §2550.404a-5(a), §2550.404a-5(b).

[29] *See* 29 C.F.R. §2550.404a-5(c).

ISSN 0747-8607

ments; and information presented in a comparative format.[30]

As mentioned above, Technical Release 2011-03 approves the utilization of a continuously available or accessible website for delivery of information regarding the investment options under a participant-directed investment plan under ERISA §404(c).[31] Under Technical Release 2011-03, the DOL set forth safe harbor conditions under which a plan administrator would be deemed to satisfy the requirement, set forth in 29 C.F.R. §2520.104b-1(b)(1), that disclosures under ERISA Title I must be furnished using measures reasonably calculated to ensure actual receipt of the material. In order to meet the terms of the safe harbor, the plan administrator must, among other things, take appropriate and necessary measures reasonably calculated to ensure that the electronic delivery system protects the confidentiality of personal information. Technical Release 2011-03 does not permit use of the IRS standards for electronic delivery, so all of the DOL requirements must be satisfied, including protection of a plan participant's or beneficiary's personal information. Thus, in order to utilize the electronic disclosure of investment alternative information via a continually accessible website, the plan administrator must take steps to protect the participant's personal information.

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 fiduciary with respect to participant-selected investments, assuming the plan had relied solely on electronic disclosure to meet the ERISA §404(c) disclosure requirements. While merely failing to disclose information for participant-directed investment accounts does not result in civil monetary penalties, it could affect the plan's qualification as an ERISA §404(c) plan. The plan fiduciaries could lose the ERISA §404(c) protection if the information is provided solely via electronic disclosure, and the individual participants' information is disclosed via a breach or hack. The participants may actually 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 protect the confidentiality of the participants' private information.

If a plan fiduciary relies solely on electronic delivery of the ERISA §404(c) information and loses protection under ERISA §404(c), it is no longer protected from being treated as a fiduciary with respect to individual participant investment elections. This means the plan fiduciary may be potentially liable for losses from participant investment decisions. This may just be another allegation added to ERISA litigation on plan fees and investments in participant-directed investment account plans.[32]

A far more significant risk is that the plan administrator and plan fiduciary might lose ERISA §404(c) protection because the failed electronic distribution caused it to fail to comply with the requirements for notice regarding the investment alternatives[33] due to loss of disseminating the appropriate information on the website. There are also additional potential issues under state laws and state private rights of action. A review of all of the state private rights of action is beyond the scope of this article.

Potential 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), and failed to do so, a civil monetary penalty of up to $133 per participant per day would apply.[34] There is no separate FAB or other guidance indicating that any standard other than the full DOL regulation's requirements would apply to delivery of these notices electronically. Therefore, when using electronic delivery with respect to a SOX or blackout notice, the mechanism also must consider the protection of the participants' information and comply with the full requirements published by the DOL in its regulation.[35]

This means that the protection of the confidentiality of personal information related to the individual accounts and benefits standard applies to the SOX notice provided electronically. The notices with respect to investment changes and blackout periods carry with them a civil penalty if the plan sponsor fails to provide a blackout notice or a notice to participants of their right to divest of employer securities under ERISA §502(c)(7) and, in most cases, each violation with respect to a single participant is a separate viola-

[30] *See* 29 C.F.R. §2550.404a-5(d).

[31] Technical Release 2011-03.

[32] 29 C.F.R. §2520.104b-1(c)(1)(i)(B).

[33] ERISA §404(a)(5), ERISA §404(c).

[34] 82 Fed. Reg. 5373 (Jan. 18, 2017).

[35] 29 C.F.R. §2520.104b-1(c).

ISSN 0747-8607

tion and results in a penalty of $131/day for penalties assessed after August 1, 2016 and $133 per day per participant on and after January 13, 2017.[36] Blackout notices are frequently delivered via electronic means and provide fiduciary protection if provided timely. If the electronic system does not protect the confidentiality of personal information, the fiduciary protection and compliance with the SOX notice requirement may be lost and the civil monetary penalties could be imposed.

Potential Consequences — SPDs

Failure to deliver a summary plan description upon request is subject to a civil monetary penalty of $147 per day prior to January 13, 2017, and $149 per day after such date, but not to exceed $1,472 per request prior to January 13, 2017, and $1,496 per request on and after January 13, 2017.[37] There is no separate FAB or other guidance indicating that any standard other than the full DOL regulation's requirements would apply to delivery of these notices electronically, so presumably if electronic delivery of SPDs is to be utilized it also must consider the protection of the participants' information.

ERISA ADVISORY COUNCIL ISSUES REPORT

The ERISA Advisory Council has been reviewing electronic securities and held a hearing on cybersecurity issues on August 24, 2016. In light of retirement plan security being a priority of the ERISA Advisory Council, plan sponsors and fiduciaries are on notice that their retirement plan data should be adequately secure.[38]

The 2016 ERISA Advisory Council report on cybersecurity, issued in January 2017,[39] focused on providing useful information to plan sponsors, fiduciaries and plan service providers. Plan sponsors and fiduciaries are instructed in the report that they should consider cybersecurity in safeguarding benefit plan data and assets and when making decisions to select or retain a service provider. The report is not a regulation or law, but merely contains recommendations based on the hearings held by the ERISA Advisory Council. The report recommends that the DOL should raise awareness about cybersecurity risks and the key elements for developing a cybersecurity strategy focused on benefit plans. The appendix to the report provides plan sponsors with materials to use in developing a cybersecurity program.[40]

In the report by the ERISA Advisory Council, it was noted that, in retirement plan administration, there are often multiple service providers who receive personally identifiable information (PII) for a plan. While some financial service organizations are subject to extensive regulation, there may be many retirement plan service providers that are not regulated and that result in a retirement plan's PII being vulnerable. The real world economic environment leaves small and mid-size employers without support or guidance with respect to the cybersecurity of their plan's PII. Larger organizations are more likely to have the resources to obtain guidance on management of PII. Third-party administrators and many service providers are not subject to security requirements.[41]

The report concludes that, based on the type of plan and its resources, and to the extent the plan bears 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, loss exposure and the cost of protective action. This challenge suggests that a scalable, individualized cyber-risk assessment strategy is the prudent starting point.[42]

Establishing a Cybersecurity Risk Management Program

The report emphasizes the need for a cybersecurity framework that follows a basic process for establishing a cybersecurity risk management program that must be also periodically updated. A cybersecurity risk management program would include prioritizing the program and its scope within the entity, orienting the scope within the entity, developing a profile of the entity's current cybersecurity status, conducting a risk assessment, identifying a target profile, analyzing gaps and implementing an action plan that includes training personnel on cybersecurity policies and procedures, as frequently the greatest risk to cybersecurity is the human element.

The Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (Safety Act)[43] provides risk management protections to firms that develop, sell or

---

[36] 82 Fed. Reg. 5373 (Jan. 18, 2017).

[37] ERISA §502(c)(7); 82 Fed. Reg. 5373 (Jan. 18, 2017).

[38] 81 Fed. Reg. 60,389 (Sept. 1, 2016).

[39] Cybersecurity Considerations for Benefit Plans, Advisory Council on Employee Welfare and Pension Benefit Plans, found at: https://www.dol.gov/sites/default/files/ebsa/about-ebsa/about-us/erisa-advisory-council/2016-cybersecurity-considerations-for-benefit-plans.pdf.

[40] *Id.*

[41] *Id.*

[42] *Id.* at p. 5.

[43] Pub. L. No. 107-296, Title VII, Subtitle G, §861–§865.

ISSN 0747-8607

deploy those technologies as well as to contractors and subcontractors and consumers downstream. These protections include limits on liability for claims arising out of, relating to, or resulting from an act of terrorism where Qualified Anti-Terrorism Technologies (QATTs) have been deployed.[44] The protections include capping liability at an approved level of insurance, exclusive federal court jurisdiction for claims against sellers from an act of terrorism, limits on noneconomic liability and exemption from punitive damages. While an act of terrorism that triggers Safety Act protections may not have originally contemplated financial harm from a cybersecurity attack within a benefit plan, some persons have argued that those protections might be applicable to a benefit plan. Benefit plan sponsors and fiduciaries may want to consider whether Safety Act certification might be part of the overall cybersecurity strategy. The report also says that each plan sponsor should evaluate its resources and tools and determine what may be the best use of plan assets before jumping into seeking certification.

While some initiatives are underway in the retirement plan industry by SPARK and in the health care industry by the Health Information Trust Alliance with their own cybersecurity and risk analysis frameworks, another option for plan sponsors is to see if their retirement plan vendors have Service Organization Control Report (SOC) 2 reporting, as this is a more extensive report on a vendor's system and its security protections. The American Institute of CPAs (AICPA) assesses internal controls and can produce a SOC at one of two levels. A SOC 1 report is on controls at a service organization relevant to user entities' internal controls over financial reporting. The SOC 1 report 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 internal controls. A SOC 2 report is on controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy. 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.[45]

The AICPA said in its Employee Benefit Plan Audit Quality Alert #365 that plan sponsors are responsible for implementing processes and controls for a plan's systems, which includes mandating that third-party service providers secure and restrict access to plan data. When plan administration services are outsourced, the plan administrator's responsibility to protect the security of the plan's records extends to the service provider's systems. The plan administrators must take this into consideration if their plans are required to be audited as part of the plan's management controls or expect to receive management comments from the auditors. While service providers may issue SOC 1 reports on their internal controls, absent statutory requirements, plan administrators must rely on imposing contractual responsibility to protect the plan's records and the plan administrator fiduciary by creating a contractual legal requirement binding the service provider.

The ISAE 3402 international security and process report is generated from an International Standard on Assurance Engagement. This is an international accounting standard audit that reports on the audit of an entity that provides services to user entities that is likely to be relevant to user entities' internal controls as they relate to financial reporting.[46] This type of engagement and report examines 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 is appropriate.[47] The audit looks at the service provider's systems and its ability to maintain the integrity of transactions. Although there are different types of service audits, they are commonly due on an annual basis. The audit considers the service organization and threats to its control objective involved in its provision of services. The audit reviews the system, its design and controls, the effectiveness of such controls and its internal audit function. The report includes the opinion of the auditor, can be in a variety of forms, and needs to be reviewed to determine its scope and nature.

Proposed Cybersecurity Measures for Financial Institutions

The Federal Trade Commission (FTC) has been regulating cybersecurity under §5 of the Federal Trade Commission Act, which prohibits deceptive business practices in commerce.[48] The FTC is charged with protecting consumers, including protecting individual consumers from identity theft. Such regulation has been upheld. The FTC also is involved in the enforcement of the Gramm-Leach-Bliley Act (GLBA) privacy requirements, which primarily impact financial institutions and do not impose security require-

[44] Cybersecurity Considerations for Benefit Plans, Advisory Council on Employee Welfare and Pension Benefit Plans at p. 10.

[45] *Id.* at p. 6.

[46] International Standard on Assurance Engagements (ISAE) No. 3402, *Assurance Reports on Controls at a Service Organization*, at p. 323.

[47] *Id.*

[48] *E.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d. 236 (3d Cir. 2015).

ISSN 0747-8607

ments.[49] 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.

The GLBA left the regulation and privacy requirements to the federal bank regulators — the National Credit Union Association, Treasury, Securities Exchange Commission and the FTC — after they consulted with the representatives of state insurance authorities designated by the National Association of Insurance Commissioners. Although many record keepers are affiliated with financial institutions subject to the GLBA and other laws regulating financial institutions, and likely already comply with other personal data security requirements, not all are. In addition, even those record keepers that are affiliated with financial institutions do not have security protection obligations that extend rights to the plan administrator, plan fiduciary or participant absent a contractual provision creating such obligations.

On October 19, 2016, the Federal Reserve, Office of Comptroller of the Currency and Federal Deposit Insurance Corporation released an advance notice of proposed rulemaking outlining cybersecurity standards meant to protect financial markets and consumers from online attacks against U.S. financial firms.[50] These rules will only be finalized after industry input. Comments were originally due on January 17, 2017, but were extended to February 17, 2017.[51] The proposal addresses cyber-risk governance, cyber-risk management, internal dependency management, external dependency management and incident response, cyber resilience, and situational awareness.[52] The rules are proposed to vary by the size of the bank and apply to banks and financial institutions with assets of $50 billion or more. Thus, once these new banking and financial institution security rules are final and in effect, as proposed, they will only apply to some of the larger financial institutions and will not reach all service providers to financial institutions that may be service providers to retirement plans. Because these rules will not apply to all financial institutions, retirement plan administrators and fiduciaries should take steps to protect plan participants' personal information.

The FBI established the Internet Crime Complaint Center (IC3) to field cybersecurity and internet crime complaints. The IC3 handles an average of 300,000 complaints per year.

The National Institute of Standards and Technology has developed a framework for Improving Critical Infrastructure Cybersecurity to which an update was recently proposed.[53]

ENFORCEMENT ACTION BY THE FEDERAL TRADE COMMISSION

In 2009, the Federal Trade Commission (FTC) issued a complaint against CVS Caremark Corporation (CVS), and concluded that CVS had disposed of documents containing confidential customer and employee information into unsecured dumpsters.[54] CVS was accused of engaging in deceptive trade practices under §5(a) of the Federal Trade Commission Act (15 U.S.C. §45(a)), which prohibits unfair or deceptive acts or practices in or affecting commerce. In particular, the FTC alleged that CVS had a privacy notice stating that appropriate data security measures were utilized that would have prevented the disposal of confidential information in such a manner. Ultimately, the FTC and CVS entered into a consent decree requiring, among other things, that CVS establish, implement and maintain a comprehensive information security program. Importantly, §5(a) is generally relied upon for the protection of consumers. However, the consent decree specifically states that the term ''consumer'' is defined to include an ''employee'' and ''an individual seeking to become an employee.'' This broad definition suggests that the FTC intends to take an aggressive approach in its interpretation of §5(a) and use it to protect sensitive employee information.

In October 2016, the FTC took another step in protection of personal health information when it issued a memorandum on its website reminding business associates and covered entities that use of protected health information (PHI) in a manner not disclosed in the HIPAA Privacy Notice may be pursued by the FTC as a deceptive or unfair trade practice prohibited by the FTC Act. The memorandum further reminds that all statements made to consumers will be considered, not just the form notice or authorization, to determine if such communications in total create a deceptive or misleading impression.[55]

The FTC recently entered a final order on one of its Administrative Law Judge's Initial Decisions on the

---

[49] Pub. L. No. 106-102.

[50] http://www.reuters.com/article/us-usa-cyber-banks-idUSKCN12J1Q00X. *See* Https://occ.gov/news-issuances/news-release/2016/nr-ia-2016-131.html. *See also* https://occ.gov/news-issuances/news-releases/2016/nr-ia-2016-131.html.

[51] RIN 3064-AE45, RIN 1557-AE06, 82 Fed. Reg. 8172 (Jan. 24, 2017).

[52] 81 Fed. Reg. 74,315 (Oct. 26, 2016).

[53] 82 Fed. Reg. 8408 (Jan. 25, 2017).

[54] *In re CVS Caremark Corp.*, Docket No. C-4259 (FTC 2009).

[55] *See* http://www.ftc.gov/tips-advice/business-center/guidance/sharing-consumer-health-information-look-hipaa-ftc-act.

ISSN 0747-8607

deficiencies in LabMD, Inc.'s data security practice, finding such practice to be unreasonable and an unfair trade practice in violation of §5 of the Federal Trade Commission Act. The order imposed a new information security program on the company and ongoing monitoring of the information security program and reporting to the FTC. Such order is now being reviewed by the Eleventh Circuit.[56]

POTENTIAL LABOR AND EMPLOYMENT LAW ISSUES

The loss of sensitive personal information belonging to employees should be of significant concern to employers. While this area of law has lagged behind technology (and the resourcefulness of hackers who would cause harm to unsuspecting employers and their employees), 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.

POTENTIAL COMMON LAW CLAIMS

The common law concerning an employer's obligation to protect the privacy of its employees' personal information is beginning to evolve.

In 2010, when a laptop was stolen from an employer containing employee names, addresses and social security numbers, three employees had standing to sue in a class action asserting claims of negligence and breach of implied contract against the employer.[57] While the claims ultimately were dismissed due to failure to state a claim, this case demonstrates that employers should be cautious about the security of sensitive employee information.

More 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.[58] 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.

STATE COURT CLAIMS

The Pennsylvania Supreme Court recently found that an employer did not have a duty to manage its computer systems to safeguard sensitive person 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.''[59] While this is one state court's position and it is consistent with the thought that there are those that have been hacked and those that know they have been hacked and it is not a matter of if, but when, the court's approach is clearly not consistent with the ERISA Advisory Council or other legal trends.

Claims Under a Collective Bargaining Agreement

Privacy violation allegations were intertwined with claims allegedly under a collective bargaining agreement and under a duty of fair representation claim when an employer provided the collective bargaining unit with the personal data of employees who were union members and the employees' personal data was stolen from the union. The claims, based on violation of the collective bargaining agreement and duty of fair representation, failed to be a basis for removing the claims to federal court. However, the state law claims related to the identity theft and resulting damages the union members incurred as the result of their identities being stolen were permitted to proceed outside of federal court.[60]

While employers must securely maintain personal information, they should use caution in developing overly broad security policies because the NLRB has expressed qualms regarding such policies applied to employees that could be reasonably interpreted as precluding employees from discussing wages, hours and working conditions.

CLAIMS BY FEDERAL EMPLOYEES

The Privacy Act of 1974 provides federal employees with a limited set of rights and protections.

---

[56] *LabMD, Inc. v. Fed. Trade Comm'n*, Docket No. 16-16270 (filed on appeal to the 11th Circuit, Sept. 29, 2016). Note that, in a related proceeding, the Eleventh Circuit approved LabMD's motion for a stay of the FTC's final order pending appeal. *LabMD, Inc. v. FTC*, No. 16-16270-D, 2016 BL 445002 (11th Cir. Nov. 10, 2016).

[57] *Krottner v. Starbucks Corp.* 628 F. 3d 1139 (9th Cir. 2010).

[58] *Corona v. Sony Pictures Entm't, Inc.*, No. 2-14-CV-09600-RGK-SH (C.D. Cal.) (*filed* Dec. 15, 2014, *settled* Apr. 6, 2016).

[59] *Dittman v. UPMC*, 2017 PA Super 8, 2017 ILRC 1023.

[60] *Saenz v. Kaiser Permanente Int'l*, No. C 09-5562 PJH, 2010 BL 35550 (N.D. Cal. Feb. 19, 2010).

ISSN 0747-8607

Federal employees' individual personal information is protected by the Privacy Act of 1974, which recognized that ''the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information,''[61] and that the Act was concerned with improper disclosure of such information. However, the Act did not entitle an employee to request destruction of his supervisor's records on the employee.[62]

STATE STATUTORY PRIVACY MANDATES AFFECTING EMPLOYERS

Social security numbers are commonly part of the data provided to retirement plan record keepers. Several states impose a statutory duty on employees to protect the privacy of employees' social security numbers.[63] 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.[64] The law provides a ''safe harbor'' if: (1) it was a practice prior to January 1, 2005, to print social security numbers on checks; and (2) the employer makes an annual disclosure to its employees that, upon written request, the employee's social security number will no longer be printed on the employee's paychecks.[65] It is important to note that these statutes normally apply to employers rather than benefit plans or the record keepers for such plans; thus, ERISA is not likely to preempt the application of these statutes to the employer.

In addition, various states require employers to notify employees of any data breach that compromises personal information.[66] 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.[67]

POTENTIAL STATE COMMON LAW AND FOREIGN PRIVATE RIGHTS OF ACTION

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. Potential violations of the privacy of such information may trigger other consequences and rights. Employers must consider foreign laws such as the European Global Data Protection Regulation when transferring employee data out of the countries comprising the EU. Additional regulations and laws protecting personal data should be expected, at a minimum from the U.K. following the Brexit vote.

INTERNATIONAL CONSIDERATIONS

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 privacy and security laws other than U.S. laws might apply. While many U.S. retirement plans may not cover citizens of EU member nations or may not receive protected personal information transferred from an entity governed by the EU rules, employers need to be mindful of the potential application of the laws of other jurisdictions if they have employees transferring data in and out of jurisdictions that are part of the EU or other jurisdictions with laws protecting personal information.

The FTC is involved in cybersecurity internationally with the European Union (EU). As we move more and more toward a global economy with workers moving across borders, employers must be aware of privacy directives protecting citizens of the EU member nations and data from EU affiliates that may require compliance with the EU requirements. Brexit will likely add nuances to protection of private per-

---

[61] 5 U.S.C. §552a.

[62] *In re Naval Avionics Ctr. & Am. Fed'n of Gov't Emps., Local 1744*, 78K/04659, 70 BNA LA 967 (May 16, 1978).

[63] *E.g.,* Alaska, California, Connecticut, Delaware, Florida, Hawaii, Illinois, Kansas, Maryland, Michigan, Minnesota, Missouri, Nebraska, New York, Oklahoma, Oregon, Pennsylvania, Puerto Rico, South Carolina, Texas and Utah.

[64] Tex. Bus. & Com. Code §501.001(a), §501.001(b).

[65] While other state laws are similar to the Texas statute, it is important to review the statute of each particular state to determine the specific requirements and penalties for failure to comply.

[66] *E.g.,* California (Cal. Civ. Code §1798.82); Colorado (Colo. Rev. Stat. §6-1-716); New York (N.Y. Gen. Bus. Law §899-aa); Nebraska (Neb. Rev. Stat. §87-801 et seq.); and Texas (Tex. Bus. & Com. Code §521.053).

[67] *See* http://www.twc.state.tx.us/news/efte/employee_privacy_rights_and_identity_theft.html.

ISSN 0747-8607

sonal data as the terms of the Brexit are worked out and new treaties addressing such issues are forged with the U.K. post-Brexit. New data privacy rules from the U.K. should be expected as Brexit is implemented and new agreements negotiated, but most reports indicate there will not be a change for two years.[68]

EU Citizen Protected Information

If a retirement plan sponsor is subject to regulation by the FTC and it receives personal information from an EU citizen or from an EU subsidiary or affiliate, then the plan sponsor will also need to consider the impact of the EU-U.S. Privacy Shield requirements (the Shield)[69] and the EU's General Data Protection Regulation (GDPR) beginning when those requirements become effective in 2018.

The Shield, effective on August 1, 2016, began requiring a plan sponsor to certify annually that it meets certain requirements in protecting the EU citizen employee's data and also requires the plan sponsor to obtain consent of the EU citizen before transferring any of the individual's private data to the United States. The Shield also requires the employer to enter into contracts that provide that the data may only be processed for limited and specified purposes consistent with the consent of the EU citizen and it must require the party receiving the information to comply with the same level of protection as under the EU principles of the Privacy Shield. A number of other requirements must also be met including requirements related to continued protection of the data if the organization leaves the Privacy Shield compliance, or it must return or destroy the data. There is also a mandated arbitral process for disputes, a required mechanism to respond to inquiries and complaints and individual rights to access and amend their information, among the other requirements. A one-year moratorium exists during which EU officials will not challenge the adequacy of an EU-U.S. Privacy Shield until after the summer of 2017.[70] Plan sponsors with operations in countries that are signatories to the TPP will need to monitor developments following the withdrawal.

Trans-Pacific Trade Pact Exit and Privacy

When President Trump removed the United States from the Trans-Pacific Partnership (TPP) trade pact via executive order on January 23, 2017,[71] it also implicated the data provisions that were intended to end data localization, and the requirement that companies store data within a country. The TPP was intended to engender general respect for the privacy laws of particular countries.[72] The full impact of the U.S. withdrawal from the TPP on data privacy and employers' ability to transfer data across country boundaries is yet to be determined.

CYBERSECURITY INSURANCE

As the cyber world and markets evolve, new insurance has been developed to protect against new risks in the e-world. Some have reported that defined contribution retirement plan service providers generally have cybersecurity insurance when they take on record keeping, but plan sponsors are more likely to be operating without cybersecurity insurance.[73] However, this article also states that while vendor management is a highly developed area, in the area of cybersecurity, most firms' coverage is inadequate. This means plan administrators, plan sponsors and fiduciaries should be inquiring about vendor cybersecurity efforts and cybersecurity insurance maintained by such vendors. In addition, plan sponsors should be reviewing their own system's data security program, policies and employee training as the human element is always a point of vulnerability. Cybersecurity and data security protections also need to start at home.

This article states that many larger defined contribution plans' record keepers maintain some cybersecurity insurance. The article also indicates that the level of coverage varies by the record keeper and coverage runs from $1 million to $100 million for larger record keepers.

Typical cybersecurity insurance covers the costs incurred from the theft of a participant's private information, restoration of assets, legal defense costs for the plan sponsor/plan administrator/plan fiduciary if sued, cost of regulatory agency investigations and penalties from a breach. However, there is no indication of coverage of the cost of corrective procedures that may be required to be implemented (under

---

[68] Marcus Hoy and Bryce Baschuk, *Brexit Won't Shift U.K. Privacy Law in Short Term*, 15 Bloomberg BNA Privacy and Security Law Rep., No. 34, 1690 (Aug. 22, 2016).

[69] The Annexes to the Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield. *See also* Aaron Simpson and Anna Pateraki, *The Privacy Shield Gets the Green Light from the European Union*, Bloomberg BNA World Data Protection Rep. (Aug. 25, 2016).

[70] Stephen Gardner, *Moratorium Set on EU-U.S. Data Transfer Pact Challenges*, 15 Bloomberg BNA Privacy and Security Law Rep., No. 31, 1547 (Aug. 1, 2016).

[71] 82 Fed. Reg. 8497 (Jan. 25, 2017).

[72] Daniel R. Stoller, *U.S. Pacific Trade Deal Exit Highlights Privacy Uncertainty*, Bloomberg BNA Privacy and Security Law Rep. (Jan. 23, 2017).

[73] Rick Baert, *Plans ask about cyber security insurance — but not for them*, Pension and Investments Online (Oct. 17, 2016), http://www.pionline.com/article/20161017/PRINT/310179997.

ISSN 0747-8607

HIPAA enforcement corrective procedures required have frequently been more costly than penalties). In addition, there is the cost of coverage for the breach resolution — from system restoration to forensic investigation of how the breach occurred — public relations and other reputational costs. Plan administrators/plan sponsors/plan fiduciaries inquiring about record keeper cybersecurity insurance should also ask about the insurer's rating and ask to have the opportunity to review how and whether the policy covers the clients of the record keeper.

SUMMARY

Cybersecurity should be a consideration for every retirement plan fiduciary. In order to preserve fiduciary protection while making required disclosures electronically, retirement plan fiduciaries should consider whether their duties of loyalty, prudence and to administer the plan for the exclusive benefit of the participants might require them to protect their participants' personal information.

As a practical matter, do you really want to explain to a C-suite member why you did not take steps to protect their personal information from identity theft or why the company needs to pay for identity theft protection for all of the employees because the retirement plan record keeper had a breach?

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.[74] 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 an SOC 2 report? Or an ISAE (International Standards on Assurance Engagements) 3402 report?
3. What are the elements of the vendor's cybersecurity program?
4. How will the plan(s) 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 for breaches?
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 plan administrator and fiduciaries of a breach of its system? Are these procedures satisfactory?
12. Will the vendor provide regular reports on its security risk analysis results and updates and management procedures?
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 SOC 2 report, does it subject itself to other external reviews or does it have an external certification?
16. Does the vendor have Safety Act certification?
17. What level or type of cybersecurity coverage does the vendor maintain?
18. Does the cybersecurity insurance provide ''first party'' insurance and provide coverage at the first sign of a breach, or does it provide ''third party'' coverage that only provides benefit coverage after someone makes a claim against the vendor?
19. What level of financial and fraud coverage is provided?
20. 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?
21. 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)?
22. What are the vendor's hiring practices (e.g., background checks)?

Provisions Plan Administrators Should Consider in Contracting to Protect Data Security

1. Confidentiality of information clauses identifying and defining whose data it is and what data is subject to protection and how the data can or cannot be used or mined.

[74] Ellen Nakashima and Andrea Peterson, *NSA's Use of Software Flaw to Hack Foreign Targets Posed Risks to Cybersecurity*, The Washington Post (Aug. 17, 2016).

ISSN 0747-8607

2. Data privacy law compliance representations that identify the laws the service provider must comply with and that include the service provider's covenant to continue to operate in compliance with such requirements.

3. Data protection protocols identifying the data security standards that must be satisfied and what security procedures must be implemented.

4. Security incident procedures and notification procedures considering state statutory and common law requirements applicable to the employer and the plan administrator's fiduciary obligations under ERISA.

5. Limitations of, and exclusions from, liability:
   a. Direct damages
   b. Indirect damages

6. Security audit provisions to permit the plan administrator to review compliance.

7. Customer-requested background checks of supplier personnel that are necessary to verify who has access. While some states have employment laws limiting an employer's ability to request such information prior to making a hiring decision, any personnel involved with participant personal information should be carefully reviewed prior to any access to such data that is provided by the record keeper.

8. Definitions related to cybersecurity terms, standards, tools or mechanisms.

9. Obligations to notify the plan sponsor of a breach and duty of vendor to promptly investigate suspicious facts.

10. Obligation to mitigate damage to participants and dependents affected by the breach.

11. Does the vendor maintain cybersecurity insurance, what limits apply, and will it protect the plan administrator/plan fiduciary and plan participants in the event of a breach? Who is the insurer? What is the insurer's rating? Can a copy of the policy be reviewed? Can the plan administrator or participants be listed as (an) additional insured(s)?

12. Is the vendor subject to federal cybersecurity regulations applicable to financial institutions or will it comply with other cybersecurity regulations in the United States or abroad that may apply to the plan data?

Cybersecurity Risk Management Using the Plan Sponsor as a Starting Point

1. Have the plan fiduciaries completed a risk analysis for the retirement plan after identifying the data elements used by the plan?

2. What are the plan sponsor's cybersecurity procedures and policies?

3. Have the plan sponsor's employees with access to retirement plan data and other employees with access to the plan sponsor's system been trained on cybersecurity policies and procedures for the retirement plan?

4. What are the consequences for the plan sponsor's employees who fail to follow the plan sponsor's security procedures?

5. Have all parties who have access to the retirement plan data been identified?

6. Has the plan sponsor identified all equipment on which personal identifiable information might be located? Is there a regular inventory process?

7. Does the plan sponsor have a cybersecurity management plan or policies?

8. Does the plan sponsor have procedures for contractors who have access to the plan sponsor's facilities or system?

9. Identify which retirement plan vendors need which data.

10. Identify the file/data transfer protocols used to transfer data to each retirement plan vendor and the security of each such process.

11. Should any certifications be obtained to try to limit liability?

12. What cybersecurity insurance does the plan sponsor maintain and what are the coverage limits?

13. Does the plan sponsor's employee disciplinary policy(ies) consider an employee's failure to follow cybersecurity protocols?

14. Review any collective bargaining agreements applicable to employees who have access to the employer's electronic system to determine if the addition of disciplinary measures for a violation of an employer's system security procedures is problematic, or if the addition of new work rules related to system security for such work group may raise any issues under the collective bargaining agreement.

ISSN 0747-8607