Potential Risk and Liabilities for Employers and Retirement Plan Sponsors and Fiduciaries

ALI-CLE Retirement Plan Update Webinar
November 3, 2016

Prepared by:

Greta E. Cowart, Esquire
Marcus D. Brown, Esquire
Theanna Sedlock, Esquire

Winstead PC
500 Winstead Building
2728 North Harwood Street
Dallas, TX 75201
214.745.5400

Updated October 31, 2016

Introduction

Many employers historically were only concerned with privacy and security for health plans under HIPAA[1] and State laws; however, there are other references to protecting participant information in ERISA that should not be overlooked. Data security experts consistently state that it is not "if" a breach will occur, but "when." Human resources and other custodians of social security numbers are frequent targets of cyber-attacks.[2]

While there are cyber security 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 raise debt, public relations image costs, operational disruption, impact on and losses in employee relations (including impact on relations with collective bargaining units impacted), devaluation of business reputation and loss of intellectual property. The total loss calculated for one company for one breach was $1.679 million.[3] In addition, there are also other laws protecting private information that should be considered. Retirement plan sponsors and plan fiduciaries should consider cyber security with respect to their own systems and at their retirement plan service providers because if the plan administrators do not require the plan's data be protected there is no overriding federal law dictating security or privacy standards, but there are consequences for the plan administrator and employer as discussed below.

Some of the protections plan fiduciaries expect and commonly used tools for cost saving such as electronic disclosure may be effective 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 fulfill disclosure obligations and save cost of copying and distributing the summary plan descriptions, participant account statements, participant-directed investment disclosures and many of the health plan disclosures. The requirements applicable for each type of electronic distribution must be satisfied to utilize electronic distribution of plan information to participants and beneficiaries.[4] Different requirements apply to different notices and disclosures. The electronic distribution requirements for the U.S. Department of Labor under ERISA and the electronic distribution of plan notices under the Internal Revenue Service requirements differ in several ways, one of which is that only the requirements under the regulations under ERISA require the plan sponsor to protect the confidentiality of personal information.[5]

[1] P.L. 104-191
[2] "Hackers are targeting tax professionals as October deadline approaches, IRS Warns" http://www.investmentnews.com/article/20160906/free/160909974/hackers-are-targeting
[3] "A Deeper Look at Business Impact of a Cyberattack; CSO Online Article August 25, 2016 http://www.csoonline.com/article/3110756/data-breach/a-deeper-look-at-business-impact-of-a-cyberattack.html
[4] DoL Reg. §2520.104b-1(c)
[5] DoL Reg. §2520.104b-1(c) compared with Treas. Reg. §1.401(a)-21

ERISA, Electronic Delivery and Cybersecurity

The security and privacy of 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 and a good business practice to protect that participant personal information as it often contains sufficient information for someone to steal a plan's participants' identities. The data and information provided to a retirement plan record keeper or service provider records for a retirement plan often includes name, date of birth, address, social security number, information about their account, compensation and other information such as beneficiaries and the beneficiaries' identifying information. Thus, the information provided to a retirement plan record keeper or some other service provider is sufficient for a hacker to create identity theft issues for a retirement plan's participants 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 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, as many do, utilizes the electronic methods of distribution of Plan information. If a Plan wants to disclose information through electronic media under the DoL regulation[6] §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's other than the individual for whom the information is intended),* (iii) the electronically delivered documents are prepared and furnished in a manner that is consistent with a style, format and content requirements applicable to the particular document; (iv) notice must be provided to each participant, beneficiary or other individual, in an electronic or non-electronic form at the time the document is furnished electronically, that apprises the individual of the significance of the document, when it is not otherwise reasonably evident as transmitted, (e.g., the attached document describes changes in the benefits provided for your Plan) and of the right to request and obtain a paper version of such document; and (v) upon request, the participant, beneficiary or other individual is furnished with a paper version of the electronic version of the currently furnished documents. Among the above requirements for a plan sponsor to be able to utilize electronic delivery of plan documents and information under ERISA is the following requirement:

> "Protect 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.);"[7]

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

[6] DoL Reg. §2520.104b-1(c)
[7] DoL Reg. §2520.104b-1(c)

protect the personal data of the participants' and beneficiaries' of a retirement plan has not been defined in regulations or other guidance issues 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. 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 effectively access documents furnished in electronic format at any location where 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 non-electronic form, to receiving the documents through the electronic media and has not withdrawn such consent and has received certain notices with certain content.[8] While some guidance has considered providing information through continuously available websites[9], 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." However, a prudent plan administrator should ensure that the participant personal information is protected and its confidentiality presented 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.

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[10] and upon request. Failure to deliver such individual account statements can result in a civil monetary penalty of $110 per day per participant.[11] Electronic delivery of participant benefit statements has also been permitted under DoL Field Assistant's Bulletin No. 2007-03 with respect to distribution of individual account plan and benefit statements and use of the Field Assistant's Bulletin ("FAB") No. 2006-03 with respect to the participant account statements quarterly for participant directed investment accounts and annually for pension statements implementing the changes under the Pension Protection Act of 2006[12]. However, both of those Bulletins required the plan administrator to furnish the participant benefit statements in good faith compliance with the Internal Revenue

[8] DoL Reg. §2520.104b-1(c)
[9] EBSA Technical Release 2011-03
[10] ERISA §105
[11] ERISA §502(c)(1)
[12] P.L. 109-280.

Service ("IRS") requirements and not by complying with the DoL's regulatory requirement and the IRS's requirements under Treasury Regulation§ 1.401(a)-21 does not include any language related to protection of the participants' personal information. The IRS regulation makes no mention of protecting the confidentiality of participants' personal information so when IRS standards are used for electronic disclosure, failure to protect personal information is not required for the electronic disclosure system to effectively deliver or disclose documents. 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 since the confidentiality requirement does not apply if the IRS standards are used.

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." The Technical Release does not distinguish whose electronic delivery system must provide the protection of confidentiality, but it is clearly included this security requirement in this temporary enforcement policy and if remains in effect until the DoL issues further guidance in this area.[13] The Technical Release 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 since the Technical Release adds the requirement for protection of confidential information as a requirement and does not use the appraisal of the FABs to use the IRS standards.

Distribution of information is also critical for participant directed investments and for plan fiduciary's to obtain the provided limitation on the fiduciary's liabilities with respect to participant investment decisions (the "Fiduciary Relief"), to the extent it is available, under ERISA §404(c).[14] The Fiduciary Relief does not relieve the plan fiduciary from prudently selecting or monitoring the investments or service providers.[15]

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

[13] U.S. Department of Labor, Employee Benefits Security Administration, Technical Release No. 2011-03 (Sept. 13, 2011).
[14] See DoL Reg. §2550.404c-1(b) and §2550.404c-5(b)
[15] *Tibble v. Edison Int'l, Inc.*, 135 S.Ct. 1823 (2015), *rehearing en banc* 9th Cir. *granted* August 5, 2016; *George v. Kraft Foods Global Incorporated*, 641 F.3d 786 (7th Cir. 2011)

range of investment alternatives, the manner in which to invest the assets of his account.[16] 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 to an identified plan fiduciary who is obligated to follow such instructions, and (2) the participant or beneficiary is provided or has the opportunity obtain sufficient information to make an informed decision among the available investment alternatives.[17] 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 to be an ERISA §404(c) plan.

For an individual account plan that provides for participant direction of investments, it must meet certain fiduciary requirements for disclosure.[18] The disclosure requirements include plan related information.[19] The plan related information includes 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.[20] 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.[21]

ERISA Technical Release No. 2011-03 approves the utilization of a continuously available or accessible website for delivery of information regarding the participant investment options under a participant directed investment plan under ERISA §404(c).[22] Under ERISA Technical Release 2011-03,the DoL helped facilitate the provision of the investment alternative information electronically; however, it comes with requirements as to the requirements under Department of Labor Regulation §2520.104b-1(c) which permits disclosure through electronic media, provided that the plan administrator has taken steps to protect the confidentiality of the participants' private information. ERISA 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 protecting the personal information of plan participants and beneficiaries. Thus, the plan administrator must take steps to protect the participant's personal information to be able to utilize the electronic disclosure of investment alternative information via a continually accessible website.

However, if there is a failure to keep participant information protected and secure which 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

[16] See DoL Reg. §2550.404c-1(b)(1)
[17] See DoL Reg. §2550.404c-1(b)(2)
[18] See DoL Reg. §2550.404a-5(a) and (b)
[19] See DoL Reg. §2550.404a-5(c)
[20] See DoL Reg. §2550.404a-5(c)
[21] See DoL Reg. §2550.404a-5(d)
[22] ERISA Technical Release 2011-03 Interim Policy on Electronic Disclosure for participant directed investment accounts.

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 account to qualify carries no civil monetary penalty consequences; it does have consequences as to whether the plan qualifies as an ERISA Section 404(c) plan. The plan fiduciaries could lose the ERISA §404(c) protection if the information is provided solely via electronic disclosure, but 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 the plan sponsor's delivery of the plan or investment information was not correctly disclosed under ERISA because the electronic disclosure may have failed to comply with the requirement because it 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 fiduciary with respect to individual participant investment elections. This means the plan fiduciary may be potentially liable for participant investment decisions. This may just be another allegation added to ERISA litigation on plan fees and investments in participant directed investment account plans.[23]

A far more significant risk is that the plan administrator and plan fiduciary might lose ERISA §404(c) protection because the failed electronic distribution may cause it to fail to comply with the requirements for notice regarding the investment alternatives[24] 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.

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 are subject to a civil monetary penalty of $131 per participant per day. There is no separate field assistance bulletin 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 to use 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.[25]

This means that the protection of the confidentiality of personal information related to the individual's accounts and benefits standard applies to the SOX notice provided electronically. The notices with respect to investments changes and black-out periods carry with it a civil penalty if you fail to provide a blackout notice or a notice to participant 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 violation and results in a penalty of $131/day for penalties assessed after August 1, 2016. Black-out notices are frequently delivered via electronic means

[23] DoL Reg. §2520.104b-1(c)(1)(i)(B)
[24] ERISA §404(a)(5) and §404(c)
[25] DoL Reg. §2520.104b-1(c)

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.

Consequences − SPDs

Failure to deliver a summary plan description upon request to the DoL is subject to a civil monetary penalty of $147 per day, but not to exceed $1,472 per request.[26] There is no separate field assistance bulletin 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.

Other ERISA Penalties

The loss of the ERISA §404(c) protection will not only result in loss of a fiduciary protection under ERISA §404(c) but it may impact compliance with other disclosure requirements, e.g., ERISA §104(b) such as distribution and summary plan description can only result in a civil monetary penalty of $100/day under ERISA §502(c)(1)(b) if it's a failure to furnish information required by Title I of ERISA to a participant or beneficiary who requested such information.

A plan administrator may choose to use electronic delivery of information to satisfy a number of disclosure requirements under ERISA. If the personal information of participants is not kept secure and protected, the plan administrator may not be able to use electronic delivery and may fail to satisfy its disclosure requirements under ERISA and incur other penalties or liabilities. The civil monetary penalty for failure to provide investment information upon request is not one of the failures escalated under the regulation for the Department of Labor Federal Civil Penalties Inflation Adjustment Act Catch-Up Adjustments Regulation.[27]

More ERISA Regulations to Come?

The ERISA Advisory Council has been reviewing electronic securities and held a hearing on cybersecurity issues on August 24, 2016. A follow-up teleconference is scheduled for September 27, 2016. So security of retirement plan data should be considered as it is clearly on the radar screen of the ERISA Advisory Council and may very well be at the Employee Benefits Security Administration.[28]

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 mandatory third party service providers to secure and to restrict access to the plan's data. When

[26] ERISA §502(c)(7)
[27] 81 Fed.Reg. 43430 (July 1, 2016)
[28] 81 Fed. Reg. 60389 (Sept 1, 2016)

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. So plan administrators need to consider this if their plans are required to be audited as part of the plan's management controls or expect to receive at management comments from the auditors. While service providers may issue SOC1 reports on their internal controls, absent statutory requirements plan administrator 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.

Retirement Plan Data Security

It is important for an employer and retirement plan sponsor to consider taking steps to insure the security of participant information provided to plan record keepers or vendors in taking steps to document their efforts to protect the security of the retirement plan information at a vendor when contracting with vendors. In this age of what seems to be perpetual announcements of breaches and hacking, it is critical that the employer can demonstrate 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 since it relates to complying with disclosure requirements. It is important for the plan administrator to request service providers to comply with data protection standards contractually to have a binding legal requirement the plan administrator can enforce and for the plan administrator to avoid negative comments in the management letter on the audit of the plan.

The security of a plan sponsor's participants' personal information is even more significant as more plan sponsors outsource more and more HR functions transferring more and more data to third parties where frequently contracts focus on statements of work and processes but may not address data retention or security.

Not All Disclosures are Created Equal

ERISA electronic disclosure regulations govern many required disclosures such as qualified default investment alternative ("QDIA"),[29] SOX notices,[30] qualified change in investment alternative[31] participant benefit statements,[32] investment alternative information,[33] COBRA notices and suspension of benefits notices and these are governed by the Department of Labor's electronic disclosure requirements.[34] 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.

[29] ERISA § 404(c)(5); DoL Reg. § 2550.404c-7
[30] ERISA § 101(i)
[31] ERISA § 404(c)(4)
[32] ERISA § 105
[33] ERISA § 404(c)
[34] DoL Reg. § 2520.104b-1(c)

However, there are also a number of disclosures, notices or distributions of information provided under the Internal Revenue Code of 1986, as amended (the "Code") such has safe harbor notices for safe harbor 401(k) and 401(m) plans.[35] The Code also mandates a notice for Qualified Automatic Contribution Arrangements and Eligible Automatic Contribution Arrangements.[36] 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 U.S. Department of Labor requirements for electronic disclosures. The regulations under the Internal Revenue Code (the "Code") governing electronic disclosures do not include any reference to electronic security or maintaining the safety or confidentiality or integrity of the data in the manner that the Department of Labor's regulation reference to "protection of the confidentiality of personal information relating to the individual's accounts and benefits."[37] This means that a vendor who fails to protect the privacy of participant information in a strictly U.S. participant only plan would 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 Code §§ 104(a)(3), 105, 125, 127, 132, 220 and 223 as well as for any notice or election under a qualified plan under 401(a) and 403(a), SEP, SIMPLE and 457(b) plans,[38] but such rules do not apply to notices required under Titles I and IV of ERISA.[39] The Treasury Regulations also do not apply to suspension of benefits notice under Code § 411(a)(3)(B) or to COBRA notices.[40]

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.

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.[41] CVS was accused of engaging in deceptive trade practices under Section 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

[35] Code § 401(k)(12)(D), § 401(k)(13)(E) and §401(m)(11)
[36] Code § 401(k)(12)(B) and 414(w)(4)
[37] DoL Reg. § 2520.104b-1(c)(1)(i)(B); Treas. Reg. § 1.401(a)-2
[38] Treas. Reg. §1.401(a)-21(a)(2)
[39] Treas. Reg. §1.401(a)-21(a)(3)
[40] Treas. Reg. §1.401(a)-21(a)(3)(i)
[41] *In re: CVS Caremark Corp.* Docket # C-4259 (Federal Trade Commission, 2009).

commerce. In particular, the FTC alleged that CVS had a privacy notice stating that appropriate data security measures were utilized which 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, the Section 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 and employee." This broad definition suggests that the FTC intends to take an aggressive approach in its interpretation of Section 5(a) and use it to protect sensitive employee information.

In October 2016, the FTC took its 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 in a manner not disclosed in the HIPAA Privacy Notice may be pursued by the FTC as a violation of the Federal Trade Commission Act 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.[42]

The FTC recently entered a final order on one of its Administrative Law Judge's Initial Decisions on the deficiencies in LabMD, Inc.'s data security practice, finding such practice to be unreasonable and an unfair trade practice in violation of Section 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.[43]

Potential Common Law Claims

For example, when a laptop was stolen from an employer containing employee names and 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.[44] While the claims ultimately did not proceed due to failure, 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.[45] Anthem also faced a class-action lawsuit after it suffered a hack into its own employees' information.[46] Given these examples of common law claims brought

[42] http://www.ftc.gov/tips-advice/business-center/guidance/sharing-consumer-health-information-look-hipaa-ftc-act.
[43] *LabMD, Inc. v. Federal Trade Commission*, Appeal to the Eleventh Circuit Court of Appeals at Appeal No: 16-16270-D, filed 9/29/2016, Case 16-16270.
[44] *Krottner v. Starbucks Corp.*. 628 F. 3d 1139 (9th Cir. 2010).
[45] *Corona v. Sony Pictures Entertainment, Inc.*, U.S. Dis. Ct., Central Dis. California, No. 2-14-CV-09600-RGK-SH.
[46] Thomson Reuters "Employment Alert" Vol. 32, No. 5 (March 6, 2015).

against employers, it would be prudent to ensure that adequate security measures are in place to protect confidential employee information.

Privacy violation allegations were intertwined with claims allegedly under the 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.[47]

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

While federal government employees have the protection of their individual personal information covered 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:"[48] and the act was concerned with improper disclosure of such information. Yet such act did not entitle an employee to request destruction of his supervisor's records on the employee.[49] So the Privacy Act of 1974 only provides federal employees with a limited set of rights and protections.

State Statutory Privacy Mandates Affecting Employers

Social security numbers are commonly part of the data provided to a retirement plan record-keeper. Several states impose a statutory duty on employees to protect the privacy of employees' social security numbers.[50] 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.[51] The law provides a "safe harbor" if: (i) it was a practice prior to January 1, 2005 to print social security numbers on checks; and (ii) the employer makes an annual disclosure to its employees that, upon written request, the employee's

[47] *Saenz v. Kaiser Permanente International*, 2010 BL 35550 (N.D. Cal. 2010).
[48] 5 U.S.C. §552a.
[49] *In re Naval Avionics Center and American Federation of Government Employees, Local 1744*, 78K/04659, 70 BNA LA 967 (May 16, 1978).
[50] 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.
[51] Tex. Bus. & Com. Code § 501.001(a), (b).

social security number will no longer be printed on the employee's paychecks.[52] 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.[53] For example, Texas Business & Commerce Code §521.053 requires a business that loses sensitive personal information through hacking or other means of unauthorized acquisition of 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.[54]

Potential State Common Law 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 and 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 regulation and laws protecting personal data should be expected, at a minimum from the UK following the Brexit vote.

Common Law Claims for Violation of Privacy Rights to Watch

The common law on an employer's obligation to protect the privacy of its employees' personal information is beginning its evolution. 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.[55] Anthem also suffered a hack into its own employees' information.[56] The law in this area is just beginning its evolution and lags far behind the technology.

[52] 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.
[53] 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)
[54] http://www.twc.state.tx.us/news/efte/employee_privacy_rights_and_identity_theft.html.
[55] *Corona v. Sony Pictures Entertainment, Inc.*, U.S. Dis. Ct., Central Dis. California, No. 2-14-CV-09600-RGK-SH.
[56] Thomson Reuters "Employment Alert" Vol. 32, No. 5 (March 6, 2015).

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.[57] The Federal Trade Commission 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 impacted financial institutions and did not impose security requirements.[58] 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.

Instead the GLBA left the regulation and privacy requirements to the federal bank regulators, to the National Credit Union Association, Treasury, Securities Exchange Commission and the Federal Trade Commission after they consulted with the representatives of state insurance authorities designated by the National Association of Insurance Commissioners. While many record keepers affiliates with financial institutions subject to the GLBA and other laws regulating financial institutions are likely to already be meeting other personal data security requirements, not all record keepers are affiliated with financial institutions and even those that are so affiliated do not have security protection obligations that provide rights to the plan administrator, plan fiduciary or to a participant absent a contractual provision creating such obligations to protect the plan administrator or plan fiduciary.

Reuters reported that on October 19, 2016, banking regulators outlined cyber security standards meant to protect financial markets and consumers from online attacks against U.S. financial firms and this was done in an advance notice of proposed rulemaking[59]. These rules will only be finalized after industry input. The proposal addresses cyber risk governance, cyber risk management, internal dependency management, external dependency management and incident response, cyber resilience, and situational awareness.[60] The rules are proposed to vary by the size of the bank and apply to banks and financial institutions with assets of $50 million or more according to the statements released by the Federal Reserve, Office of Comptroller of the Currency and Federal Deposit Insurance Corp. With this scope it is expected that roughly 40 banks and non-bank financial companies will be required to comply with these new security requirements.[61] Thus, once these new banking and financial institution security rules are final and in effect they will only apply to some of the larger financial institutions and will not reach all service providers to financial institutions who may be service providers to retirement plans. Since these rules will not apply to all financial institution, retirement plan administrators and fiduciaries should take steps to protect the plan participants' personal information as the current laws do not guarantee the protection to retirement plan data.

---

[57] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d. 236 (3d Cir. 2015)
[58] P.L. 106-102.
[59] http://www.reuters.com/article/us-usa-cyber-banks- idUSKCN12J1Q00X and see also Https://occ.gov/news-issuances/news-release/2016/nr-ia-2016-131.html. .
[60] 81 Fed. Reg. 74315 (October 26, 2016).
[61] http://www.reuters.com/article/ us-usa-cyber-banks- idUSKCN12J1Q00X .

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

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 there may be laws beyond the U.S. laws which 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 and out of jurisdictions which 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 personal data as the terms of the Brexit are worked out and new treaties addressing such issues are forged with the UK post Brexit. New data privacy rules from the UK should be expected as the Brexit is implemented and new agreements negotiated, but most reports indicate there will not be a change for two years.[62]

While the European Commission's Safe Harbor Decision[63] on data transfers was invalidated[64] and was struck down, the EU-US Privacy Shield effective August 1, 2016 became effective for companies to use by certifying their compliance with the Privacy Shield's principles.[65] Employers who transfer employee personal data to and from the EU should consider whether they can meet the requirements of the Privacy Shield and self-certify compliance requires the distribution of privacy notices, provide individuals a chance to opt out, comply with standards for transfers of such data, require compliance or destruction of data if they withdraw and a mechanism to address non-compliance concerns.

EU Citizen Protected Information

If a retirement plan sponsor is subject to regulation by the Federal Trade Commission 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

[62] "Brexit Won't Shift U.K. Privacy Law in Short Term" Bloomberg BNA Privacy and Security Law Report, Vol. 15, No. 34, p. 1690, August 22, 2016.
[63] (2000/520/EC).
[64] CaseC-362114 Maxmillian Schrems v. Data Protection Commissioner (Schrems).
[65] "The Privacy Shield Gets the Greenlight from the European Union" Bloomberg BNA World Data Report, August 23, 2016.

(the "Shield")[66] and the EU's General Data Protection Regulation ("GDPR") beginning when those requirements become effective in 2018. The Shield will require the plan sponsor to certify annually that it meets certain requirements in protecting the EU citizen employee's data and will also require it to obtain consent of the EU citizen before transferring any of the individual's private data to the U.S. The Shield will also require 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, 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-US Privacy Shield until after the summer of 2017.[67]

Cyber Security Insurance

As the cyber world and markets evolve, new insurance is 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 recordkeeping, but plan sponsors are more likely to be operating without cybersecurity insurance.[68] 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. 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 cost of corrective procedures that may be required to be implemented, (and under HIPAA enforcement corrective procedures required have frequently been more costly than penalties)), and 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 should be inquiring regarding record keeper cybersecurity insurance should also inquire regarding the insurer's rating and inquire regarding reviewing the insurance

[66] 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.
[67] "Privacy Regulations Set One Year Moratorium of Challenges to EU-US Data Transfer Pact," Bloomberg BNA Privacy and Security Law Report, Vol. 15 No. 31 p. 1547 (August 1. 2016).
[68] "Plans ask about cyber security insurance—but not for them" by Rick Baert, Oct. 17, 2016, Pension and Investments Online, http://www.pionline.com/specialreports/other/20161017 or at http://www.pionline.com/article/20161017/PRINT/31017997/plans_ask_about_cybersecurity .

contract/policy to have the opportunity to review how and whether the policy covers the clients of the record keeper.

Summary

Security should be a consideration for every retirement plan fiduciary to preserve the fiduciary protection available from making required disclosures electronically and the fiduciary protections that flow from such disclosures such as the QDIA, ERISA 404(c), and claims of violation of common law privacy rights, 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 the participants' personal information provided to vendors from hackers. 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 breech?

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.[69] So a new road map for hackers is out, are you ready?

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.
2. Data privacy law compliance representation which identifies with which laws the service provider must comply and their covenant to continue to operate in compliance with such requirements.
3. Data protection protocols identifying what data security standards 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 exclusion 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 are necessary to verify who has access and whether the plan fiduciary must be concerned and because many security incidents are due to the human element. While some states have employment laws limiting an employer's ability to request such information prior to the hiring decision, any personnel involved with participant personal information should be carefully reviewed prior to an access to such data is provided by the record keeper.
8. Definitions related to cybersecurity terms, standards and tools or mechanisms.

[69] "NSA's Use of Software Flaw to Hack Foreign Targets Posed Risks to Cybersecurity" by Ellen Nakashima and Andrea Peterson, The Washington Post, August 17, 2016.

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? May a copy of the policy be reviewed? May the plan administrator or participants be listed as an additional insured?
12. Is the vendor subject to federal cybersecurity regulation applicable to financial institutions or will it be subject to the new proposed cyber security regulation when it is final and effective?

4821-1079-5577v.3□999993-1□