Liabilities and Risk from Failing to Address the Cybersecurity of Your Retirement Plan Data

09.12.16

In the current 114th session of Congress, there have been 204 bills, resolutions and amendments introduced addressing cybersecurity in their text, if you had any doubt about whether you should be concerned about cybersecurity of your retirement plan data, please read on. 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 and in other laws 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]

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, while there is no current overriding federal regulatory scheme dictating security or privacy standards, there are consequences for the plan administrator and employer if that data is not kept secure as described in part below.

Electronic Disclosure Requirements for Some Notices Include Security Concepts

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]

The data and information provided to a retirement plan record keeper or service provider records for a retirement plan often includes significant participant and beneficiary identifying information. Thus, the information, if in the wrong hands, could 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, and (ii) "*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)" among other requirements.

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 as both may be used to furnish documents and information electronically to participants. 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 issues by the U.S. Department of Labor ("DoL"). It does not require much creativity to see how failure to ensure adequate security with respect to the participants' personal data might be used to claim a failure to provide a required disclosure and the other claims that might be based on a failure to disclose and potentially result in a fiduciary issue.

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[7] and upon request. Failure to deliver such individual account statements can result in a civil monetary penalty of $110 per day per participant.[8] 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[9]. However, both of those Bulletins required the plan administrator to furnish the participant benefit statements in good faith compliance with the Internal Revenue 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 if the participant data is hacked because 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 clearly included this security requirement in this temporary enforcement policy and if remains in effect until the DoL issues further guidance in this area.[10] 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 indicate that the earlier good faith compliance FABs 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).[11] The Fiduciary Relief does not relieve the plan fiduciary from prudently selecting or monitoring the investments or service providers.[12]

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.[13] 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.[14] 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 so the plan fiduciaries may be able to claim the Fiduciary Relief.
For an individual account plan that provides for participant direction of investments, it must meet certain fiduciary requirements for disclosure.[15] The disclosure requirements include plan related information.[16] 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.[17] 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.[18]
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 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 electronic disclosure 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) due to a breach of its retirement plan participant personal information, 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.[19] 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 electronic disclosure 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.[20] 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 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 could be lost and the civil penalties could be assessed for failing to notify.

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[21] and it is addressed in some of the bills pending in Congress.

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 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 because as part of the audit review 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, those do not protect the plan administrator/fiduciary. A plan administrator/fiduciary must rely on imposing contractual responsibility on service providers to the plan to protect the plan's records by creating a contractual legal requirement binding the service provider as long as no regulatory or statutory requirement applies to such service provider and provides remedies for the plan administrator/fiduciary.

Not All Disclosures are Created Equal

ERISA electronic disclosure regulations govern many required disclosures such as qualified default investment alternative ("QDIA"),[22] SOX notices,[23] qualified change in investment alternative[24] participant benefit statements,[25] investment alternative information,[26] COBRA notices and suspension of benefits notices and these are governed by the Department of Labor's electronic disclosure requirements.[27] 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. Failure to disclose on each notice carries its own consequences.

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.[28] The Code also mandates a notice for Qualified Automatic Contribution Arrangements and Eligible Automatic Contribution Arrangements.[29] 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."[30] 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.

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,[31] but such rules do not apply to notices required under Titles I and IV of ERISA.[32]

Potential Labor and Employment Law Issues

When a laptop was stolen from the employer containing employee names and addresses and social security numbers that had not been misused, three of the employees had standing to sue as a class action on claims of negligence and breach of implied contract against the employer.[33] While those three employees had standing to sue in federal court because they had a credible threat of real and immediate harm from the theft of the laptop containing personal information, they failed to adequately allege the existence of an implied contract and the case was dismissed for failure to allege sufficiently all of the required elements of their claim.[34] While their claims ultimately did not proceed, it was due to procedural failure and thus it does not stop other potential claimants in similar situations. Some states recognize common law rights of privacy which may provide protection of participant rights in the event of a breach and prove costly for the employer. Privacy violation allegations were intertwined with claims allegedly under the collective bargaining agreement and under a duty of fair representation 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.[35]

While an employer must maintain this type of information secure, the NLRB has expressed qualms regarding overly broad policies applied to employees that could reasonably be interpreted as precluding employees from discussing wages, hours and working conditions. Thus, employers should carefully craft security policies in light of the NLRB's expressed concerns.

State Employment Law Statutory Privacy Mandates

Employees have the duty to protect the privacy of their employees' social security numbers under a number of states laws and since social security numbers are provided to record keepers for retirement plans for use in participant and beneficiary identification on reporting.[36] Some of these state laws limit how an employer may use its employees' social security numbers and may require the employer to notify the employees in the event of a breach.[37] Some states limit the number of digits of an employee's social security number that an employer can use.[38] The penalties for failing to protect the privacy of an employee's social security number varies by state. Social security numbers are commonly part of the data provided to a retirement plan record keeper. The statutes apply to employers and not to benefit plans, thus ERISA preemption is not likely to avoid the application of these statutes.

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.[39] Anthem also suffered a hack into its own employees' information.[40] The law in this area is just beginning its evolution and lags far behind the technology.

Other Regulation

The Federal Trade Commission is regulating cybersecurity under Section 5 of the Federal Trade Commission Act which prohibits deceptive business practices in commerce.[41] The Federal Trade Commission is charged with protecting consumers, including protecting individual consumers from identity theft. 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. 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 data security requirements, not all record keepers are affiliated with financial institutions. Even agreements with record keepers with legal security obligations should consider adding protections providing rights to the plan administrator/fiduciary because contractual language creating such obligations protects the plan administrator/fiduciary by providing rights it can enforce directly.

International Considerations

In a world with a global and mobile workforce, there may be other issues arising from the interaction with international laws. However, there seems to be sufficient legal concerns in the U.S. without expanding this further.

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. 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 the above reasons are not sufficient, 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.[42] So a new road map for hackers is out.

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.

2. Data Privacy Law Compliance identifying what laws must be complied with by the party providing services to the plan.
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 privacy law requirements applicable to the employer and the plan administrator's fiduciary obligations.
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.
8. Definitions related to cybersecurity terms, standards and tools or mechanisms.

Contact:
Greta Cowart
214.745.5275
gcowart@winstead.com

---

[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 Cyber-attack; 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
[6] DoL Reg. §2520.104b-1(c)
[7] ERISA §105
[8] ERISA §502(c)(1)
[9] P.L. 109-280.
[10] U.S. Department of Labor, Employee Benefits Security Administration, Technical Release No. 2011-03 (Sept. 13, 2011).
[11] See DoL Reg. §2550.404c-1(b) and §2550.404c-5(b)
[12] *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)
[13] See DoL Reg. §2550.404c-1(b)(1)
[14] See DoL Reg. §2550.404c-1(b)(2)
[15] See DoL Reg. §2550.404a-5(a) and (b)
[16] See DoL Reg. §2550.404a-5(c)
[17] See DoL Reg. §2550.404a-5(c)
[18] See DoL Reg. §2550.404a-5(d)
[19] DoL Reg. §2520.104b-1(c)(1)(i)(B)
[20] DoL Reg. §2520.104b-1(c)
[21] 81 Fed. Reg. 60389 (Sept 1, 2016)
[22] ERISA § 404(c)(5); DoL Reg. § 2550.404c-7
[23] ERISA § 101(i)
[24] ERISA § 404(c)(4)

[25] ERISA § 105
[26] ERISA § 404(c)
[27] DoL Reg. § 2520.104b-1(c)
[28] Code § 401(k)(12)(D), § 401(k)(13)(E) and §401(m)(11)
[29] Code § 401(k)(12)(B) and 414(w)(4)
[30] DoL Reg. § 2520.104b-1(c)(1)(i)(B); Treas. Reg. § 1.401(a)-2
[31] Treas. Reg. §1.401(a)-21(a)(2)
[32] Treas. Reg. §1.401(a)-21(a)(3)
[33] *Krottner v. Starbucks Corp.*. 628 F. 3d 1139 (9th Cir. 2010).
[34] *Krottner v. Starbucks Corp.*, 406 Fed. Appx. 129 (9th Cir. 2010).
[35] *Saenz v. Kaiser Permanente International*, 2010 BL 35550 (N.D. Cal. 2010).
[36] 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.
[37] E.g., Alaska, Delaware, Florida, Texas and Oregon.
[38] E.g., California, Michigan, Nebraska and South Carolina.
[39] *Corona v. Sony Pictures Entertainment, Inc.*, U.S. Dis. Ct., Central Dis. California, No. 2-14-CV-09600-RGK-SH.
[40] Thomson Reuters “Employment Alert” Vol. 32, No. 5 (March 6, 2015).
[41] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d. 236 (3d Cir. 2015)
[42] “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.