CYBERSECURITY

ARE PUBLIC DEFINED CONTRIBUTION PLANS AT RISK?

HOW REAL IS THE THREAT?

Defined contribution plan participants face an ever-evolving, ever-changing landscape of cyber related threats due to the multiple layers of personally identifiable information (PII) being shared between plan sponsors, recordkeepers, and other third-party service providers.

CHALLENGES FACED BY GOVERNMENTAL DEFINED CONTRIBUTION PLAN SPONSORS

One major challenge faced by many public sector defined contribution plan sponsors is internal, sometimes antiquated, IT systems (often payroll and human resource administration systems) and the heavy reliance on third party data recordkeeping systems. An additional hurdle faced by public defined contribution plan sponsors is that there is no comprehensive federal regulatory scheme that governs cybersecurity for retirement plans and their associated service providers.

While the Department of Labor (DOL) has in the past attempted to impose obligations on private defined contribution plan sponsors in an attempt to protect the confidentiality of an employee's personal information[1], and some states have enacted laws to address cybersecurity breaches[2], public defined contribution plan sponsors generally may not feel they have clarity with respect to their duties and obligations. Nevertheless, while governmental defined contribution plans are not subject to the Employee Retirement Income Security Act (ERISA), the ERISA fiduciary and the DOL's cybersecurity rules can serve as best practices for governmental defined contribution plan sponsors.

TYPES OF DATA AT RISK IN DEFINED CONTRIBUTION PLANS

The PII that is most at risk for a cybersecurity attack under defined contribution plans include:

- Social Security Numbers
- Dates of Birth
- Addresses

[1] DOL Reg. § 2520.104b-1(c); DOL Technical Release No. 2011-03.

[2] A.B. 1841 (California); H.B. 1453 (Colorado); S.B. 258 (Delaware); H.B. 1025, 1033, S.B. 624 (Florida); S.R. 360 412 (Georgia); S.B. 7601 (New York); S.B. 1538 (Oregon); H.B. 241 (Utah); H.B. 817 (Virginia); H.B. 2375 (Washington); North Carolina and Wyoming have also enacted legislation related to cybersecurity breaches.

- Email Addresses
- Bank Account Information
- Employee Compensation Data
- Account Balances
- Assets of the Plan

The vulnerability of passwords and the ability of hackers to guess the entry information to participant accounts on recordkeeper websites pose the greatest cybersecurity threat to defined contribution plans. To alleviate this risk, some recordkeepers are adopting a layered identification approach that includes requiring dual IDs, with passwords provided by both the service provider and the plan participant, and fingerprint identification. Many cybersecurity experts say fingerprint identification is far better than using passwords.

Another area that should be of particular concern to defined contribution plan sponsors is the evolving use of the SSN in forms as a method of identifying plan participants or plan participants identifying themselves. Specifically, it is important to identify whom within a service provider's organization has access to participant SSNs and how that access can be limited. This further relates to the distribution of plan materials (e.g. quarterly statements) to participants that include SSNs. Materials which contain participant names, addresses and account numbers are a major source for obtaining data for cybersecurity attacks. Government defined contribution plans that enroll employees using paper forms that request the employee's SSN, particularly at new hire orientations or benefits fairs, can also raise the risk level.

THREATS TO GOVERNMENTAL DEFINED CONTRIBUTION PLANS

The ways in which hackers penetrate defined contribution plans has continued to become more complex. Examples of common cyber threats include:

- **Ransomware** – criminals encrypt and seize an entire hard drive and will only release it for a high ransom.
- **Phishing** – fraudulent emails are sent with the objective of enticing the user to interact and inadvertently provide an avenue for a cybercriminal to infiltrate a computer network.
- **Wire transfer email fraud** – cybercriminals pretend to be senior executives asking employees to transfer funds.
- **Malware** – intrusive and harmful software is stored on an external drive that is inserted into and executed on a network computer.

CURRENT ENVIRONMENT – WHAT IS BEING DONE

Defined contribution plans possess the type of personal information subject to privacy and data security laws. However, a comprehensive system for regulating privacy and cybersecurity does not currently exist. Instead, privacy and data security rules are scattered in a number of federal and state-specific statutes and can apply to retirement plans either directly or indirectly. As a result, it can often be difficult to identify the privacy and data security rules applicable to retirement plans or know with certainty how to comply with them.

It is important to monitor changes in this area as regulations are rapidly evolving to meet the increased risk associated with cyberattacks. Because of the types of personal information held and transmitted by retirement plans, they are currently subject to regulation and oversight from the following areas:

- **Gramm-Leach-Bliley Act ("GLB Act").** The GLB Act requires several federal agencies to establish regulations requiring financial institutions to provide customers with a notice of privacy policies and practices, and must not disclose nonpublic personal information about a consumer to nonaffiliated third parties unless the institution provides certain information to the consumer and the consumer has not elected to opt out of the disclosure. The Act also requires the Commission to establish for financial institutions appropriate standards to protect customer information.

Some of the largest data breaches over the last few years may have resulted from the hacking of third party vendor platforms, so it is important for plan fiduciaries to ensure its vendors have the proper policies and procedures in place to minimize the risk of these breaches and to have a plan of action in place in the event of such breaches. One way to do that is for plan fiduciaries to inquire about these policies when selecting vendors and to continue to monitor compliance throughout the service relationship. Many of the following federal regulations were a result of the GLB Act.

- **Securities and Exchange Commission (SEC).** Regulation S-P requires financial institutions registered with the SEC to adopt written policies and procedures reasonably designed to ensure the security and confidentiality of customer information and records. Regulation S-P covers applies to broker-dealers, investment companies, and investment advisers, etc.
- **Federal Trade Commission (FTC).** The FTC has the authority to develop rules that regulate specific areas of consumer privacy and security. The FTC established the following two bodies of law that at least indirectly affect retirement plans:
  - FTC's "Red Flag Rules" rules require financial institutions to have identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft. The Red Flag Rule was created to help prevent identity theft. The Red Flag Rule applies to state or national banks, state or federal savings and loan associations, mutual savings banks or any other entity that holds a transaction account belonging to a consumer.
  - The FTC has also created the "Gram Leach Bliley Safeguards Rule" which requires financial institutions over which the FTC has jurisdiction to develop, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards. The definition of "financial institution" is broad and a retirement plan's consultants, investment advisors and investment platforms are typically subject to these requirements.

Both the SEC and FTC have created detailed rules related to structure and operation of the required written policies. These rules apply to the financial institutions holding plan assets, investment advisors and other vendors who handle plan assets. In order to ensure plan fiduciaries are meeting their duties to the plan, it is important to ask vendors about their privacy and security policies and operational compliance with the applicable laws.

There are a number of tools available to defined contribution plan sponsors to monitor a vendor's compliance with applicable privacy and security standards. For example, the Report on Controls SOC II provides detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems. These

reports can play an important role in oversight of a vendor's management programs, internal corporate governance and risk management processes, and regulatory oversight.

- **State Law.** State Attorneys General all over the United States are enforcing the privacy laws instituted by their states. There have been a number of regulatory developments at the state level in the last few years. Most recently, New York instituted new cybersecurity rules for the financial services industry during business in the state and California issued several privacy and data security-related resources.
  - **New York.** The New York Department of Financial Services implemented new cybersecurity regulations effective March 1, 2017 (using a two-year transition period). Under these new rules, banks and other financial service organizations must establish and maintain written cybersecurity programs, perform periodic risk assessments, designate a chief information security officer and comply with additional requirements like conducting annual testing of its cybersecurity program and training personnel and notifying regulators of breaches.
  - **California.** California's extensive privacy and data security laws are among the most protective in the United States. The California Attorney General issued several new resources that include detailed discussion of California's data security laws. The California Attorney General Data Breach Report for 2016 sets the baseline for reasonable security measures under California law. The California AG's report indicates that employers/plan sponsors who do not use the 20 controls identified in the Internet Security's Critical Security Controls may not comply with California's privacy and data security laws.

Those in the financial industry such as banks, registered broker-dealers, record keepers etc. have responded to the increased enforcement activity in the cybersecurity area in a number of ways. One such response was by the Society of Professional Asset-Managers and Record keepers (SPARK) Institute which has formed the Data Security Oversight Board to establish uniform data management standards and create a certification program so that providers can assure defined contribution plan clients that a baseline level of data security is being provided.

In May of 2016, the SPARK Institute announced the creation of an Industry Data Security Oversight Board. With industries and government entities facing unprecedented threats from cybercrime, SPARK unveiled its plan to establish uniform data-management standards for the defined contribution market that will be overseen by this Data Security Oversight Board (DSOB).

Over the last year, SPARK's DSOB has met with cybersecurity experts, presented to governmental and regulatory agencies, and is narrowing its focus to develop collaborative and uniform criteria for record keepers to use as a baseline level of security across retirement plan clients. Common Criteria Certification, as it is known, ensures that services purchased by organizations perform and are secure at the desired level of performance. It has emerged as a standard by which all industries can evaluate the security of IT and data systems. With Common Certification Criteria, plan sponsors and their consultants will have an extra measure of confidence that a record keeper's data security is at a level that meets established guidelines.

Other industries, including healthcare providers, government agencies and other financial institutions have benefited from achieving a Common Certification Criteria. However, the program's success is yet to be determined and will be contingent on a number of factors. For example, it is unknown if SPARK's program will set baseline criteria high enough to meet the minimum requirements of the most stringent state privacy and security laws.

FINANCIAL LIABILITY AND PROTECTIONS FOR BREACHES

With the vast majority of states now having privacy laws that apply to sensitive PII, a government defined contribution plan could face significant remediation-related expenses should a breach occur. On average, direct costs amount to approximately $6 per breached record[3].

Because these costs can be significant, cybersecurity insurance exists to help cover these direct costs. More importantly, it provides resources to help the plan sponsor manage the breach event. Cyber liability insurance is not new, but has gained import in recent years because it helps mitigate the liability associated with a data breach. Liabilities include administrative, technological, and legal costs. Cyber liability insurance policies are intended to cover both a sponsor's first-party breach costs as well as protection from third-party liabilities that might result from the breach event.

The direct first-party breach costs that these insurance contracts generally cover include:

- Legally required notification expenses, including mailings to inform participants of the breach,
- Free credit monitoring for each affected participant,
- Identity-protection services,
- Forensic investigative costs to identify what information was taken and how it occurred,
- Audit and legal services related to compliance, and
- Communication and public relations services.

One of the benefits of cyber insurance is that, subject to the limits of liability purchase, insurers typically provide the insured plan with experienced professionals who help handle the fallout from a breach event. Attorneys who specialize in privacy compliance are typically assigned and forensic experts may also be engaged to stop an ongoing breach, fix the damaged network, restore data, and attempt to prevent future similar breaches from occurring. Public relations firms are often provided to help in communication and can provide call centers to help manage the deluge of calls that may follow notice mailings.

This team of experts can be supplemented by funds provided by the carrier to cover not only the cost of the experienced professionals, but also the ancillary costs of providing legally required notification expenses, credit monitoring and the other first-party costs noted above. Given the sensitivity of, and the potential damage created by, the breach, these policies are unique in that they will often be triggered, meaning the carrier will respond with assistance while the data breach is still occurring instead of simply reimbursing incurred costs after the event which is typical of most insurance coverage payments.

The other advantage is that these policies provide protection from third-party liability that may result from a breach event. Third-party liabilities are those claimed by individuals who allege that they have been harmed by the breach (for example, a participant who, through identify theft, might seek financial redress. Some policies also include limited regulatory proceeding coverage (coverage for lawsuits or

[3] Ponemon Institute, June 2016. 2016 Cost of Data Breach Study: United States

investigations by federal state or municipal regulators in relation to privacy laws) and extend the policy to cover certain fines and penalties that may also be assessed.

Government defined contribution plan sponsors considering insurance protection should be prepared to answer the following questions:

- Does the plan have an information security policy that stipulates that sensitive information is protected whether in written or electronic form?
- Does the plan sponsor store or have direct access to sensitive information?
- Does the plan sponsor use third parties to process or store sensitive information?
- Does the plan sponsor and its third parties have an incident-response plan and when was it last tested?
- Has the plan experienced a breach in the past?

CONCLUSION

Given the continuing need for plans to adopt ever-greater levels of technology for administrative efficiency, the risk of inadvertent disclosure of personal information is escalating. Regardless of the investment made in protecting systems and data transmissions, plans remain vulnerable to human error and malicious or criminal actions. The latter are a particular cause for concern because of their prevalence and the fact that they are the most expensive to handle.