John Ludlum

Partner
801.799.5953
Salt Lake City
jeludlum@hollandhart.com

Dean Bennett

Partner
208.383.3993
Boise
adbennett@hollandhart.com

Bret Busacker

Partner
208.383.3922
Boise
bfbusacker@hollandhart.com

New Concerns for Employers and HR Departments post-Equifax Cyber Breach

Publication — 09/18/2017

Background

Equifax, a consumer credit reporting company, recently announced that computer hackers exposed the personal information of 143 million Americans stored on the company's data base. Information exposed by the breach included names, Social Security numbers, addresses, birthdays, phone numbers, driver's license numbers, among additional data. Although cyber-attacks have become commonplace in recent years, the monumental size of the Equifax breach, which impacts approximately 44% of U.S. residents, raises significant concerns for employers.

Retirement Plan Concerns

Plan sponsors have a fiduciary duty to protect and preserve the assets of employee benefit plans. Although the fiduciary implications arising from cyber-attacks are still relatively unknown, plan fiduciaries must act reasonably and prudently to protect plan participants and beneficiaries from such attacks. Recent high-profile breaches, including the Equifax hack, have placed plan fiduciaries on notice that the risk of a cyber-attack is real. To combat this risk, we recommend plan fiduciaries take the following steps to protect plan assets from cyber-attacks:

- Evaluate the data security measures currently implemented by the plan sponsor;
- Coordinate with internal IT departments or outside IT consultants on data security initiatives;
- Know and understand the plan's service providers' security procedures;
- Consider implementing additional security measures offered by the plan's service providers (for example, some service providers now offer voice verification processes, two-step authentication, email alerts on all account activity, restricted account access for only recognized devices, etc.); and
- Review the plan's service provider contracts to ensure they fully address data security and provide appropriate indemnities to the plan, plan participants, and plan beneficiaries in the event of loss due to a security breach.

Plan fiduciaries should document any measures taken to improve data security, including all interactions with service providers and any changes implemented as a result of such interactions.

Plan sponsors should also consider communicating security tips to plan participants. Plan participants can further safeguard their retirement plan

Nicole Snyder

Director of Finance and Operations
208.383.3939
Boise
ncsnyder@hollandhart.com

accounts using the following techniques:

- Create a unique username, rather than using a Social Security number;
- Create a strong and unique password – i.e., at least 9 characters, including uppercase and lowercase letters, numbers, and punctuation marks;
- Keep username and passwords private – i.e., do not “save” them in a browser;
- Ensure that all contact information is accurate and up-to-date;
- Update security questions and answers; and
- Regularly monitor account activity and promptly report any concerns.

Hiring Practices

Under Equal Employment Opportunity Commission rules, employers can use credit checks only when the information is relevant to the position. However, background check companies sell packages that include information that is not relevant to every position, and employers will occasionally request too much information.

In light of the Equifax breach, employers should consider the relevancy of the information they are requesting for background checks and subsequently storing on company computers. The less information employers request and keep, the more they reduce the potential threat of sensitive personal information becoming compromised.

Employers should also protect the information they gather. Access to personal information should be restricted on a “need to know” basis, and should not be stored in locations that are generally accessible to company personnel. In addition, employers should consider using background checks for employees who will have access to this data as part of their job responsibilities.

Employers that use Equifax's Workforce Solutions

Equifax's product portfolio includes wage and employment verification services, which store sensitive employee data on behalf of many employers. This information can be intermingled with Equifax's consumer credit reporting products and sold to debt collectors or other agencies. Although the extent of the breach is still unknown, employers that use Equifax's Workforce Solutions should be wary.

Until more information is known, affected employers can instruct concerned employees to contact Equifax about placing a block on their employment records. Employers can also direct employees to the website Equifax created in response to the breach where individuals can determine whether their information has been compromised.