

# Alert

## Cybersecurity Risks and Considerations for Plan Sponsors to Protect Employee Benefit Plans

December 19, 2017

Recent massive and highly publicized data breaches should cause employee benefit plan sponsors to reexamine their security protocols. A security breach could jeopardize employee benefit plan assets and information. Plan data, for example, may include personally identifiable information such as social security numbers, addresses, dates of birth, bank accounts and other financial information. Plan sponsors should be proactive and implement (or improve existing) cybersecurity measures to comply with their fiduciary responsibilities under the Employee Retirement Income Security Act (ERISA).

### Call to Action

Plan sponsors should consider developing a cybersecurity risk management strategy and take into account the following steps:

- Identify risks and assess current cybersecurity measures;
- Establish enhanced written security policies and procedures (e.g., email/text alerts for account activity and multi-step authentication protocol and procedures to handle a data breach);
- Communicate security tips to plan participants including use of strong and unique passwords;
- Review service providers' contracts to:
  - ensure adequacy of security protocols and use of best in class systems and software
  - negotiate indemnification provisions for losses incurred by the plan and its participants and beneficiaries
  - require reporting of cybersecurity breaches;
- Document cybersecurity measures including any change due to a service provider's recommendation;
- Review fiduciary liability insurance coverage for data breach events;
- Consider purchase of cybersecurity insurance; and
- In the event of a breach, be active in the investigation, notice and response.

As plan sponsors seek to maintain retirement plan compliance, they should make sure cybersecurity protection measures are in place to safeguard the personal information contained in qualified plan records.

*Authored by [Mark E. Brossman](#), [Holly H. Weiss](#), [Susan E. Bernstein](#) and [Aaron S. Farovitch](#).*

If you have any questions concerning this *Alert*, please contact your attorney at Schulte Roth & Zabel or the authors.

This information has been prepared by Schulte Roth & Zabel LLP (“SRZ”) for general informational purposes only. It does not constitute legal advice, and is presented without any representation or warranty as to its accuracy, completeness or timeliness. Transmission or receipt of this information does not create an attorney-client relationship with SRZ. Electronic mail or other communications with SRZ cannot be guaranteed to be confidential and will not (without SRZ agreement) create an attorney-client relationship with SRZ. Parties seeking advice should consult with legal counsel familiar with their particular circumstances. The contents of these materials may constitute attorney advertising under the regulations of various jurisdictions.

## **Schulte Roth&Zabel**

New York | Washington DC | London

[www.srz.com](http://www.srz.com)