Could This Be Your Retirement Plan?

Prepared by:
Joseph J. Lazzarotti
Jackson Lewis P.C.

LORMAN®
Published on www.lorman.com - July 2019

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 1300 available
- ☑ **Slide Decks -** More than 2300 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

Could This Be Your Retirement Plan?

By Joseph J. Lazzarotti on April 8, 2019

As reported by CBC, B.C. Pension Corporation announced a data breach involving pension plan records after discovering a box containing microfiche could not be found following a recent office move. The box contained personal information (names, social insurance numbers and dates of birth) on approximately 8,000 pension plan participants. The company employed those participants during the period 1982 to 1997. Learning of this incident, persons responsible for pension plan administration might be wondering how secure are their facilities (or their service provider's facilities) for remote storage. And, pension plan participants might be wondering why do plans need this information and for so long.

In the U.S., the Employee Retirement Income Security Act (ERISA) governs the administration of pension plans, and the law includes specific record retention requirements. For example, persons who are responsible for filing plan reports must "maintain records to provide sufficient detail to verify, explain, clarify and check for accuracy and completeness." ERISA Section 107. In addition, ERISA requires employers to maintain sufficient records to determine benefits due to employees. ERISA Section 209. Because employees may not retire for many years after

accruing benefits under the pension plan, plans need to maintain records until plan participants retire and the records must be sufficient to determine benefits under the plan.

These record retention requirements present important issues for employers, plan administrators, and pension plan service providers. We have written about pension plans experiencing data breaches caused by malicious attackers. But, relatively straightforward administrative recordkeeping activities also can result personal information being compromised. In late 2016, the ERISA Advisory Council, a 15-member body appointed by the Secretary of Labor to provide guidance on employee benefit plans, shared with the federal Department of Labor some considerations concerning cybersecurity. To date, the DOL has not issued any formal guidance on these recommendations, however, employers, plan administrators, and pension plan service providers should revisit their procedures for handling sensitive personal information maintained in their pension plan records.

According to the Council's recommendations, there are four major areas for effective practices and policies: (i) data management; (ii) technology management; (iii) service provider management; and (iv) people issues. This is a good list to work from. However, while not an exhaustive list, the following action items may help to avoid incidents like the one discussed above:

- Retain only the data that is needed; if certain data elements can be redacted, removed them;

- Maintain an inventory of records that are retained regardless of format, and where to find them;
- Outline a clear process for moving records, and track location and inventory during the move; and
- Delete records that are no longer needed; confirm service providers have done so, as applicable.

Of course, no set of safeguards for protecting personal information will prevent all kinds of compromises to it. Mistakes happen, so employers and plan administrators should be prepared by developing and maintaining incident response plans and practice them.