

# Morgan Lewis

## OUTSIDE PUBLICATION

# CYBERSECURITY CONCERNS FOR ERISA FIDUCIARIES, *TODAY'S GENERAL COUNSEL*

April/May 2016

## AUTHORS AND CONTACTS

Patrick Rehfield, Saghi Fattahian

The F.B.I. now ranks cybercrime as one of its top law enforcement priorities, and President Obama's proposed budget would sharply increase spending on cyber security, to \$14 billion. Not only is personally identifiable information and data accessible with the click of a mouse, it's transportable via applications on smart phones, tablets and laptops. The more immediate and available personal data becomes, the greater the risk for a potential breach or unauthorized disclosure or access, as is evident from the cyber attacks on major retail operations, health care providers and the government.

## PLAN ASSETS AND PERSONAL DATA

Pension plans and welfare plan all store personal data on each participant and beneficiary, ranging from social security numbers and addresses to date of birth and health information. Not only does the plan sponsor have access to personal confidential data, but so do the participant and beneficiary, the third party service provider, and other vendors such as IT providers and data storage companies.

The technology platform where this personal data resides is increasingly complex, with more and more data being stored in the cloud and accessed remotely. While ERISA does not define the term "plan assets," the broadest definition contemplates something of value. What cyber attackers are seeking to steal is not just plan assets, but also personal data and an individual's identity, which may be of higher value than plan assets.

## THE ERISA ADVISORY COUNCIL

While cybercrime has made headlines over the last few years, this is not a new issue for ERISA fiduciaries. In 2011, the Department of Labor's (DOL) ERISA Advisory Council began looking at cybersecurity issues in the context of maintaining privacy and security around employee benefit plans. It identified identity theft and loss of plan assets as a major concern, caused in part by a lack of rigorous cybersecurity policies and procedures.

The ERISA Advisory Council recommended that the DOL provide guidance on the obligation of plan

fiduciaries to secure and keep private the personal identifiable information of participants and beneficiaries, and to develop educational materials and provide outreach for plan sponsors, participants and beneficiaries.

Notwithstanding the Advisory Council's recommendations, there currently is no comprehensive federal law governing cybersecurity. While there are federal laws that govern the collection and use of financial information, such as the Gramm-Leach-Bliley Act, Fair Credit Reporting Act and the Air and Accurate Credit Transactions, these laws govern transactions in the financial industry and do not apply to ERISA plans or the protection of personal identifiable information with respect to those plans.

In addition to these federal laws, most States have instituted privacy and security laws that address the protection of personal identifiable information, and also include notification requirements where there has been a breach or an unauthorized use or disclosure. These laws generally mirror the privacy and security requirements imposed on personal health information under the Health Insurance Portability and Accountability Act of 1996.

HIPAA, as amended, establishes privacy and security measures that group health plans must impose to protect individually identifiable health information (PHI), including a notification scheme when there has been a breach of PHI.

Under HIPAA, group health plans have been required to implement privacy and security measure on protected health information that they store for over a decade. HIPAA also contains a comprehensive breach notification structure in situations where there has been a cyberattack or impermissible use or disclosure of protected health information to impacted individuals, the Department of Health and Human Services and the media.

## **DOL GUIDANCE FOR FIDUCIARIES**

Guidance from the DOL will undoubtedly be driven first by a determination as to whether cyber security is deemed to be a fiduciary function. In the absence of such guidance plan fiduciaries may want to consider establishing prudent practices and procedures for handling and securing personal identifiable information, including securing personal identifiable information "at rest" (data stored on computers, on storage devices or being used by the data owner) and information in motion (data transmitted across a network, such as email ). These procedures may extend to third party service providers through administrative services agreements.

Plan fiduciaries should also review their record keeping processes to ensure they have proper procedures in case of any breach or investigation, possibly using the privacy and security rules under HIPAA as a benchmark.

When establishing cybersecurity procedures, plan fiduciaries and plan sponsors should consider the type of data they store along with plan assets, and impose privacy and security measures on all third party vendors that have access to or access the plan's data. They also should consider educating and training all personnel who access or have access to plan data.

Finally, it should be noted that if the DOL does not act in this area, ERISA plan fiduciaries may be required to implement cybersecurity initiatives as a result of SEC regulations on investment managers.

*This piece was originally published in Today's General Counsel's April/May 2016 issue.*

