TIAA CREF

Financial Services

Department of Labor Comments

Addressing Scope Statements - “Model Notices and Disclosures for Pension Risk Transfers” and “Model Notices and Plan Sponsor Education on Lifetime Plan Participation”

May 29, 2015

to be addressed

1. What security and privacy risks must retirement plans in the U.S. address with the procedural prudence required of them under ERISA, particularly as it relates to the electronic maintenance, storage and transmission of information necessary for Plan participants to make informed decisions with respect to risk transfer transactions or lifetime plan participation?

2. How would you suggest Plan administrators and fiduciaries protect the Plan and the Plan participants from those risks?

3. Vulnerability and what questions sponsors should ask – what should be disclosed to customers

Landscape

A. Most Americans now use of **personally identifiable information (PII) –** including name, social security number, driver license number, address and email address – in conducting their daily business. Consequently, financial services providers, third-party administrators, and others deal with and possess retirement plan participants' PII as part of daily business.

B. Due to a rising number of data breaches, identity theft has accelerated. Cross-industry fraudsters are able to assemble and socially engineer information to **make financial service data a primary target for fraudsters**.

C. Privacy of information and maintaining security of the privacy have become an **enterprise-critical priority** for retirement services providers.

Threats and Data Security Risks

- Some service providers may fail to identify aspects of data security or potential risks to plan sponsors and participants. Some providers may also fail to educate their staff members on data security awareness.
- There is often limited focus on procedures, controls, data handling, and due diligence as well as pure IT controls. Coordination of approaches needs to involve multiple areas such as IT, human resources, financial crimes, physical security, compliance, legal and operations, and becomes difficult & complex.
- Vetting of vendors and third parties has been underestimated in the context of data handling.
- Understanding the “chain” of handling data as it moves through a transaction is weak due to complexity and degree of difficulty & variability.
- Risk assessments of firms’ exposure can be weak – and some firms make no risk assessments at all. Smaller firms may not have an understanding of the risks or the mitigating controls.

Social Engineering

- ✓ The art of manipulating people and systems into performing actions or divulging confidential information.
- ✓ Social Engineering and phishing attacks gain access to critical data components
- ✓ What begins as a data theft of seemingly less important data can be foundational to data combinations.
- ✓ Data gathered from a variety of sources can be combined with available information, to be pieced together forming key facts, figures, and keys to take over the financial activities – and ultimately disrupt an individual's financial well being.
- ✓ There are long term impacts of massive data breaches, including those at high-profile retail stores.
- ✓ Data combinations and or / full sets of data are available on the "Dark Web" and other places in easily consumable manner.

Events increase Risk

There are business-to-business events that require large dataset transfers – and that ultimately increase the risk to the individual.

- Data formats are complex and vary at a transactional level
- Data communication and transport / transmission mechanisms do not have safeguards
- Business-to-business controls vary greater with the size and maturity of companies engaged – no standards exist for how much information to divulge and at what point in time
- The chain of privacy and safeguards is only as strong as the weakest link

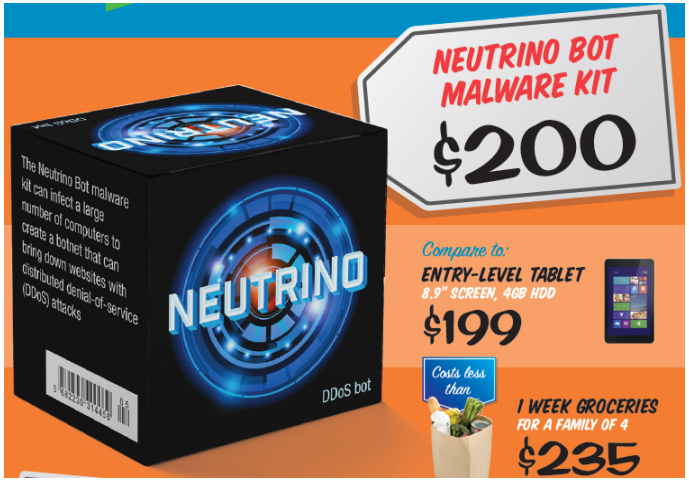
Listen and Learn

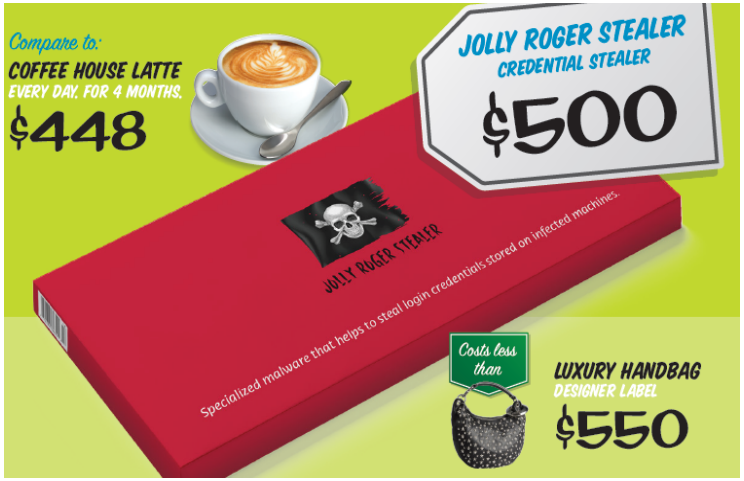
1. “You are going to be hacked.” Joseph Demarest, Assistant Director of FBI Cyber Division, “Have a Plan”
2. “About 110 Million Americans – equivalent to a large percentage of US Adults – have had their personal data exposed in some form in the past year “ Tim Pawlenty, President of Financial Services Roundtable and former Governor of Minnesota.
3. About 80% of hacking victims in the business community didn’t realize they had been hacked until told by government investigators, vendors or customers according to a recent Verizon study cited by Pawlenty.
4. “Two kinds of big companies exist in the United States. There are those who’ve been hacked… and those who don’t know they have been hacked…” James Comey, FBI Director in a CBS 60 Minutes interview

Industry Context

Serious financial fraud is conducted as a business and the barriers to entry continue to decline.

The low cost of stealing credentials, hacking accounts, and defrauding accounts presents a very low barrier to entry. The risk to financial institutions, however, is exponentially higher and increasing rapidly.





Criminals can acquire access to customer accounts very cheaply via the internet:

- 2011 – $0.50 to buy a PayPal ID
- 2011 - $700 for a bank account with a guaranteed balance over $82,000
- 2013 - $300 for a bank account password with balance between $70k-$150k

Safeguard & Protections

Standards might help provide protection to all parties

Financial services firms' operational nature requires them to have more stringent data security standards. But these are not uniformly applied and both large firms but especially small firms dealing with complexity of multiple providers and data exchanges have few incentives other than lawsuits to keeping pace with privacy and security protocols.

Standards for information exchange and the manner it can be transported / transmitted – which do not exist today, would safeguard privacy. Standards are important; as multiple industries have shown it difficult to legislate in a technical and highly dynamic area.

Formats for the data to be included in the information sets of large scale transactions – which do not exist today, would safeguard privacy

Firms must balance of use of confidential customer information while maintaining privacy. This work has limited or self-imposed guidance. To capitalize on emerging opportunities many fraudsters are introduced into a transaction chain such as affiliated and non-affiliated partners, third-party and outsourcing firms, each with new risks and a new potential weak link in the data chain.