

## 2011 ERISA Advisory Council

### Privacy and Security Issues Affecting Employee Benefit Plans

The impact of changes in technology on ERISA requirements for retirement plans and non-health welfare plans

**Issue Chair:** Anna Rappaport  
**Vice Chair:** Karen Kay Barnes  
**Drafting Team:** Denise Clark, Portia Wu

#### **Description**

When ERISA was enacted in 1974, state of the art technology consisted of a fax machine, communications regarding benefit plans were mailed, and plan distributions were made by check. Today administration includes a mixture of computer solutions, internet transactions, outsourcing, call centers, paper mail and more. As technology has improved, there are increasing concerns about privacy, security and fraud as many financial transactions are conducted on-line, and plan participants increasingly are required to use technology to interface with their plans which has produced increasing concerns about privacy, security, and fraud as well as opportunities for greater control. Privacy, security and fraud issues are not isolated to benefit plans as identity theft is a major issue in our society.

The Council is interested in learning how the changes in technology affect plan participants and sponsors, how ERISA requirements protect participants in the current environment, and what guidance is offered in related matters. The study will cover defined contribution, defined benefit, and welfare plans but exclude health care benefit plans because these plans are subject to extensive privacy regulations. In addition, the provision of health benefits in the United States is in a state of transition. The Council's focus will be on privacy and security for data and distributions, rather than on the form or method of disclosures to plan participants, which is the focus of the Department of Labor's RFI on Electronic Disclosure issued April 7, 2011.

The Council will assemble empirical information from multiple sources to help Department of Labor (DOL) establish a baseline for how issues of privacy and security are linked to plans providing employee benefits, and to learn how the DOL can improve means to protect participants, and offer additional guidance to plan sponsors, and providers of support services.

#### **Objective and Scope**

The Council is examining this topic and intends to draft recommendations for the Secretary of the DOL to consider. The report will focus on:

1. Identifying the issues related to privacy and security (the identified issues);
2. Examining the current role of the DOL in addressing the identified issues, and in influencing stakeholders;
3. Identifying benefit plan administrative structures and/or designs that can positively impact the identified issues;
4. Identifying the stakeholders who can influence recommendations;

5. Formulating recommended guidance to plan sponsors regarding effective practices on protection for participants, and the identification of additional educational opportunities for plan sponsors, service providers and individuals;
6. Identifying current cross-over of DOL current and potential efforts with Federal consumer protection laws and other applicable efforts such as financial literacy educational programs;
7. Identifying special issues relating to particular groups such as the unbanked in the workforce, disabled individuals, and those with low literacy skills;
8. Identifying lessons learned from regulations in other settings including, for example, internationally and the area of health benefits.

### **Questions for Potential Witnesses**

#### **Identifying the problem**

1. What is the nature of the privacy and security problems and challenges facing participants and plan beneficiaries? What are the perceptions of the DOL, employers, plan administrators, recordkeepers, and others about these challenges?
2. With respect to privacy and security, are there special issues for particular groups of participants or beneficiaries, such as individuals who are unbanked, those with low or no access to technology, those with low literacy skills, disabled persons, agents who have power of attorney, retirees, people with diminished cognitive skills, or spouses?
3. What information on fraud and technology has been identified from SAS 70 audits? Do technology solutions increase or decrease the opportunities for fraud?
4. Are there special privacy and security issues to be examined at time of distributions from defined benefit and defined contribution plans? How similar/different are these issues under these plans?
5. Are there special issues that are tied to events such as enrollment and termination of employment?
6. Does fraud create liability problems for plan sponsors and administrators?
7. Are the likely sources of fraud different and are there special issues for small employers?

#### **Understanding Context/Environment**

1. What is the role of the DOL in dealing with privacy and security matters?
2. How does ERISA currently deal with matters related to privacy and security?
3. What common practices are used by plan sponsors and service providers to deal with privacy and security matters today? How should they be modified?
4. What is the interplay of federal and state privacy laws that affect benefit issues?
5. What types of specialized professionals are used in privacy and security, and what, if any, is their typical role with regard to personal financial data, and pension data? What should it be? Are there government reports, creditable research and relevant litigation available that can help the Council better understand the issues?
6. What technologies are important in understanding these issues? Is security better in fully automated transactions, when service centers are used, or when transactions are partly conducted by mail? What issues are raised by these alternatives?
7. What is the role of auditors and of SAS 70 audits of service providers in understanding controls?

**Defining solutions: Effective practices/desirable/education/standards**

1. Have effective practices been identified for plan sponsors and plan administrators?
2. What lessons can be learned from international experience? Are there practices or policies in other countries that could serve as a model for benefits in the United States?
3. Are there any lessons that can be learned from the privacy and electronic data transmission laws that currently govern health care plans and the delivery of health benefits?
4. Should an employer's right to use retirement or other employee benefits data be limited to de-identified data?
5. How can employers respond to the needs of special groups?
6. What information, if any, should individuals with powers of attorney or family members have access to and under what circumstances? Who should be included in the definition of family member for this purpose?

**Possible Recommendations within the Jurisdiction of the DOL**

1. What actions should the ERISA Advisory Council recommend to the DOL regarding privacy and security?
2. Are there additional educational and outreach opportunities that should be implemented or enhanced to address this issue?
3. Are there strategies that will address small business issues?
4. Are there any steps that DOL can take to address the needs of special groups?