Advisory Council on Employee Welfare and Pension Benefit Plans

Report to the Honorable Hilda L. Solis,
United States Secretary of Labor

Privacy and Security Issues Affecting Employee Benefit Plans

November 2011

November 9, 2011

Dear Secretary Solis:

The 2011 Advisory Council on Employee Welfare and Pension Benefit Plans is pleased to present its Report on Privacy and Security Issues Affecting Employee Benefit Plans.

The Council has a diverse membership drawing from both profit and non-profit entities and representing various stakeholders in the provision of employee benefits to American workers and their families. We have a shared commitment to improving the provision of those benefits. This has enabled us to reach a consensus on a number of matters relevant to the issues we have examined.

The attached report was prepared after two days of testimony by 11 witnesses followed by discussion and deliberation by the Council.

We wish to gratefully acknowledge the assistance of all persons listed under "Acknowledgements" and, in particular, Larry Good and DiWeena Streater of the Employee Benefits Security Administration.

Respectfully submitted,

/s/

Theda R. Haber, Council Chair
Mildeen Worrell, Council Vice Chair, Drafting Team Member
Anna M. Rappaport, Issue Chair
Karen K. Barnes, Issue Vice Chair
Denise M. Clark, Drafting Team Member
Mary Ellen Signorille, Drafting Team Member
J.M. Towarnicky, Drafting Team Member
Theresa Atanasio
Sewin Chan
Karin S. Feldman
Marilee P. Lau
Michael A. Sasso
Gary A. Thayer
Michael F. Tomasek
Richard A. Turner

NOTICE

This report was produced by the Advisory Council on Employee Welfare and Pension Benefit Plans, usually referred to as the ERISA Advisory Council (the "Council"). The Council was established under Section 512 of ERISA to advise the Secretary of Labor. This report examines Privacy and Security Issues Affecting Employee Benefit Plans. The contents of this report do not represent the position of the Department of Labor (DOL).

ABSTRACT

The 2011 ERISA Advisory Council studied Privacy and Security Issues Affecting Employee Benefit Plans (other than health care benefit plans). The Council focused on the privacy and security of benefit data and personal information in light of the dramatic changes in technology and its use in the last decade in employee benefit plan management. The Council examined issues and concerns about potential breaches of the technological systems used in the employee benefit industry, the misuse of benefit data and personal information, and the impact on plan sponsors, service providers and participants and beneficiaries.

The Council recommended that Department of Labor (DOL): (1) provide guidance on the obligation of plan fiduciaries to secure and keep private the personal identifiable information ("PII") of participants and beneficiaries; (2) develop educational materials and outreach efforts for plan sponsors, participants, and beneficiaries to address the issues of privacy and security of PII; and (3) include in their outreach and educational materials information regarding elder abuse related to benefit plans.

II. ACKNOWLEDGEMENTS

The Council recognizes the following individuals and organizations who contributed greatly to the Council's deliberations and final report. The views and conclusions in this report are those of the Council alone.

July 20, 2011

Jeffrey Hinman, Department of Labor

Alan Brill, Kroll Inc.

Thomas J. Condron, Guided Choice

David L. Wray, Plan Sponsor Council of America (PSCA)
(formerly Profit Sharing/401(k) Council of America)

Kathleen M. Quinn, National Adult Protective Services Association

September 1, 2011

Seth Geftic, RSA, The Security Division of EMC

Ian McKay, American Institute of Certified Public Accountants

Chris Brecht, Carday Associates

John Barton, Health Services & Benefit Administrators, Inc. (HSBA)

Richard Carpenter, American Society of Pension Professionals & Actuaries

Anna Driggs, Investment Company Institute (written testimony only)

Larry Good, Employee Benefits Security Administration (EBSA)

DiWeena Streater, EBSA

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

II. RECOMMENDATIONS

III. BACKGROUND

A. Definition of the problem
B. Examples of actual problems involving pension and non-health benefit plans
C. Current environment for benefit plan administration
D. Current legal environment

IV. SUMMARY OF TESTIMONY AND COUNCIL DISCUSSION

A. Issues facing plan sponsors and administrators
   1. Points of vulnerability:
      i. Data management
      ii. Technology management
      iii. Service provider management
      iv. People issues
      v. Challenges for small business
      vi. Participants and beneficiaries
   2. Chart of practices useful to certain plan administrators to minimize security breaches
   3. Outreach to plan sponsors

B. Issues facing participants and beneficiaries
   1. Points of vulnerability
   2. Elder abuse and challenges for those with little or no technology skills
   3. Outreach and educational efforts

V. RATIONALE FOR RECOMMENDATIONS AND OBSERVATIONS

A. DOL guidance on fiduciary obligation to protect PII
B. DOL education and outreach to stakeholders on protection of PII
C. DOL education and outreach on elder abuse
D. Important observations
   1. New legislation
   2. Information sharing

VI. CONCLUSIONS

VII. APPENDICES

Appendix A
Information to support implementation of outreach recommendations

Appendix B
Resources and sources of information on matters under study

Appendix C
Witness summaries – Summary of testimony to the ERISA Advisory Council on privacy and security issues affecting employee benefit plans

I. EXECUTIVE SUMMARY

The 2011 ERISA Advisory Council examined the current state of benefit plan administration, and how technology has created opportunities and challenges for keeping personal identifiable information (PII) of plan participants and beneficiaries in retirement and certain welfare benefit plans private and secure.[1] This included an examination of the ways in which the security of plan data could be breached and the ways benefit plans can be subject to fraud. The study covered benefit plans that handle PII in a fully automated environment, as well as plans in which PII is also handled directly by plan personnel and with some manual processes. The study focused on understanding the growth and dependency on technology and its impact on the management of benefit plans.

The key points that were marshaled from the testimony (both oral and written) are: (1) administrative service providers are essential in any efforts to protect PII of plan participants and beneficiaries; (2) everyone who comes in contact with PII has a role to play in protecting such data; (3) many organizations, such as financial services organizations, are subject to extensive regulation or other legal requirements that result in multi-faceted efforts to protect PII of their customers; these efforts can provide some security of PII for plan participants and beneficiaries; (4) because of the multiple users and service providers in this area, and the resulting patch work regulatory system, security of the data may have some weak, and possibly, unprotected areas; and (5) large employers and organizations are more likely to have the resources (both in technology and personnel) to obtain guidance on the management of PII in benefit plans and to increase their due diligence efforts in this area; in contrast, small and some middle-size employers and organizations are less likely to have the resources to obtain this level of support and guidance; indeed, these employers and organizations often may not have the expertise to evaluate the security efforts, if any, of their service providers.

The Council's recommendations focus primarily upon the need for plan sponsors, plan administrators, participants and beneficiaries to be informed about their responsibilities and rights in the protection of PII in these retirement and welfare benefit plans. Specifically, the Council requests that the Department of Labor (DOL) provide guidance concerning the protection of PII as a fiduciary responsibility and the extent PII of benefit plan participants and beneficiaries should be protected in plan administration. In addition, the Council recommends that DOL provide updated outreach efforts and educational materials in this area for plan sponsors, service providers, plan participants and beneficiaries, as well as other individuals who come in contact with either PII held by the plan or the plan participants. The recommendations include some specific updates for outreach efforts and educational materials. These suggestions are intended to provide assistance and clarity for plan sponsors and administrators to manage plans more securely; to help fill current gaps for mid-size and smaller employers as they undertake the security of plan PII; to educate participants and beneficiaries on the importance of protecting their personal information, and to encourage them to do so; and to increase

[1] The scope of this study specifically excludes health care benefit plans subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

awareness in the employee benefits community of the special needs of the elderly and disadvantaged populations with respect to technology awareness, access and proficiency in security management.

Additionally, based on the testimony, the Council makes two observations. First, the Council observes that when legislation dealing with privacy and security information issues is proposed, the impact of rules, regulations and policies on employee benefit plans should be considered, given the vast amount of capital and PII they hold and maintain. Second, the Council suggests that plan sponsors could benefit from the establishment of a clearinghouse that would permit plan administrators and plan sponsors to share information resources and best practices utilized in this area.

II. RECOMMENDATIONS

1. The Council recommends that DOL issue guidance on the obligation of plan fiduciaries to secure and keep private the personal identifiable information (PII) of plan participants and beneficiaries, including the extent to which PII of benefit plan participants and beneficiaries should be protected in plan administration, and which guidance would also confirm that the plan assets may be used to cover reasonable costs to accomplish this result.

2. The Council recommends that DOL develop educational materials and outreach efforts (such as tip sheets or any other appropriate format that would serve as helpful resources) for plan sponsors, plan participants, and beneficiaries to address the issues of privacy and security of PII. The Council has identified the following publications that could be added or updated to accomplish this objective:

- <u>Plan Sponsors, Plan Administrators and Other Service Providers</u>

  - Update *Tips for Selecting and Monitoring Service Providers for Your Employee Benefit Plan* to address issues related to privacy and security of pension plans including a questionnaire that would focus on key areas in the selection and monitoring of plan administrators and other service providers.

  - Develop materials that would highlight the need for plan sponsors to address privacy and security in plan administration; outline factors to consider when developing and implementing privacy and security policy; address ways in which a plan sponsor can monitor plan administrators and other service providers with respect to privacy and security (e.g., appropriate certification, attention to other regulatory requirements that may apply such as HIPAA, an AICPA Service Organization Controls (SOC) report or similar assessments), and the need for additional layers of security (e.g., authentication) at vulnerable points such as plan loans, withdrawals, and distributions. Such materials would also include factors to be considered for remediation after a security breach has occurred.

- <u>Plan Participants and Beneficiaries</u>

  - Develop a publication for participants and beneficiaries addressing Privacy and Security of PII that is similar to *10 Warning Signs That Your 401(k) Contributions Are Being Misused*. The publication would assist participants and beneficiaries to understand the need for privacy and security of their plan information, including understanding who has access to such information, steps they should take to minimize such information being widely disseminated, and efforts they can take to monitor the plan's use and dissemination of PII.

  - Update *Taking the Mystery Out of Retirement Planning* to further underscore existing information on pension scams and to address steps plan participants and beneficiaries can take to protect their PII, including information to educate them

on the need to exercise security measures for purposes of conducting plan business, including obtaining plan loans, withdrawals and other plan distributions; measures to be exercised when a pass code is lost; and other risks (e.g., that inactive accounts may be more susceptible to fraudulent activity).

3**.** The Council recommends that DOL include in its outreach efforts and educational materials information from appropriate sources regarding elder abuse that is designed to increase awareness of elder abuse issues related to benefit plans. These efforts and materials should be targeted to plan sponsors, record keepers, and plan participants and beneficiaries (including reference to resources where additional information can be obtained).

III. BACKGROUND

A. Definition of the Problem

When ERISA was enacted in 1974, state of the art technology was a fax machine, communications were mailed and distributions were made by writing a check. As technology has improved and expanded to include various forms of electronic communications, there are increasing concerns about privacy, security and fraud in the benefits area as many financial transactions are conducted on-line and as plan participants are increasingly required to use technology to interface with their plans. Some of the possible and more common threats include:

- Theft of personal identities and other PII.
- Theft of money from bank accounts, investment funds and retirement accounts.

Benefit plans and their service providers face the same challenges that financial institutions do regarding access to individual assets and PII. The increased use of the internet to conduct financial transactions has increased the ability of financial institutions to quickly research and gather information relevant to financial transactions, thus permitting more efficient business transactions. However, it also allows new opportunities for fraud and other financial crimes. Technology also can enable sophisticated means to guard data and reduce risks.

The purpose of this study is to understand how these technological developments affect benefit plans subject to ERISA and to make recommendations to DOL about the kinds of guidance or education plan sponsors, fiduciaries, participants and beneficiaries may utilize to protect PII, remediate security breaches, and preserve the integrity of plan administration in this rapidly changing environment.

The Council has concluded that addressing these issues requires consideration of all stakeholders who share, access, store, maintain and use PII, including, but not limited to, participants, plan sponsors, plan administrators, third party administrators (TPAs), record keepers, investment advisors, other service providers, trustees and other fiduciaries. Issues to be considered include privacy policies which address who may have access to PII, procedures for disseminating information concerning PII security breaches, and remediation when breaches result in financial harm to plan participants and/or beneficiaries.

B. Examples of actual problems involving pension and other non-health benefits

DOL is aware of the vulnerability of ERISA plans. The Council received testimony from DOL representatives who provided examples of actual cases of theft of employee benefit money uncovered in their enforcement efforts. One of the cases involved a criminal ring penetrating a benefits administration system when a member of the criminal ring was unwittingly hired by a plan administrator. Targeted accounts were identified, addresses

were changed, and payments of requested distributions were directed to be sent to new addresses which were addresses for members of the criminal ring.

The American Institute of Certified Public Accountants (AICPA) also provided a list of data breaches that have occurred in pension plans (of which they are aware because of subsequent disclosures about the breach). The causes for the breaches were identified as follows:

- Unauthorized user hacking into the plan administrative system after gaining administrative privileges to the accounts and changing account information followed by a fraudulent distribution of funds from the participants' accounts to the unauthorized user. The hacker gained access to the system by planting a virus on the company's computer. It is believed that the virus was of a type that enabled the hacker to capture keystrokes when made by an authorized person, thereby enabling the hacker to capture login information and passwords of the plan participants;
- Unauthorized person logging into broker website, entering ID and password, and securing payment which was sent to a name different from the name on the account;
- Person hacking into database to gain access to more than 500,000 participants' PII due to failure of the plan (and administrators) to install security system updates;
- E-mail hoax (phishing attack) that directed participants to a look-alike website prompting participants to share personal data including Social Security numbers (SSNs);
- Employee downloading confidential information for more than 450,000 participants to a home computer;
- Several examples related to the ease with which PII was fraudulently obtained from laptops;
- Multiple examples involving SSNs on printed communications that were, in many cases, either mailed to wrong addresses or the information was made visible to others;
- Employee stealing electronic tapes that contained PII of plan participants and/or beneficiaries;
- Auditors who received CDs with PII of participants and beneficiaries in benefit plans they did not currently audit; and
- Payroll provider using the same password for all clients when the payroll system was established.

Because benefit plans maintained by governmental and other public entities are subject to greater disclosure rules, the examples provided by the AICPA were gathered mostly about public plans. However, this does not mean that fewer breaches occurred in private benefit plans, but rather, that private plans are less likely to disclose such information.

As part of the various examples where cyber theft of retirement funds can occur, the Council was shown a clip from an ABC-produced news segment on methods by which theft from 401(k) accounts can occur. The segment showed how business travelers who

were using hotel computers in the hotel's business centers or kiosks to access their personal financial information can be easily subjected to fraud. The clip showed how easy it was for someone to implant a device on these computers that will store the individual's information, thereby giving others (including those engaged in criminal activity) access to the information. It should be noted that some of the more sophisticated security systems and accompanying off-the-shelf software detect requests that are sent from a computer other than the computer that is registered with the system and usually used to communicate with the system. In such a case, additional prompts are used to solicit information that should be known only by the authorized person or owner of the account.

The Council heard testimony that confirmed the ease by which PII can be accessed by computer hackers where the information is managed carelessly, including the loss or mishandling of backup data tapes, PII left where it can be easily found, or openly shared by the individual. Data breaches can include the loss or theft of laptops and other portable devices that contain PII.

The Council also heard testimony on how individuals can contribute to security breaches by personal action, inattention or failure to act. Some scams are designed to trick individuals who have access to PII to disclose the information to another person who cannot be verified as the authorized user. These efforts are referred to as "social engineering." For example, people may call up a bank and say they are on vacation in another country, they have lost their wallet with all their information and they must have access to some money. They then talk the person on the phone into giving them the necessary information. Witness Alan Brill from Kroll Inc. provided an example of a small business that had a $9,000,000 wire transfer from its bank accounts to an account in another country. Investigations of call logs, call recordings and detailed information indicated that the bank had received a telephone call 30 minutes before the transfer took place. The investigation showed that the cyber criminals had convinced a bank employee to provide the log-in information needed to make the transfer.

Social networking can also contribute to the problem, as the Council learned that PII can often be found on these websites.

C. Current environment for benefit plan administration

Over the last decade, benefits administration, like many other functions, has become much more automated and efficient. Most financial businesses have migrated to automated platforms, and consumer self-service is commonly available in employee benefit administration. The technological experience of the consumers of these services is very diverse, ranging from people who are very savvy with technology and stay up-to-date to people who are moderate users of technology and communicate by e-mail, but who are not at all sophisticated, to those who do not use computers and never will. While direct deposit of retirement distributions, either periodic or single payments, is a common business practice, direct deposit is not an option in all situations as some participants do not have access to this service, some do not want to use it, and some are unbanked or

under banked. Plan sponsors in certain industries are likely to have a higher representation of employees with little or no technology access and skills. Today's retirees are more likely than the general population to have limited or no access to technology. While there are fewer people who are not connected to the internet today, there still remain segments of the population who do not use technology. Plan administrators must be prepared to deal with participants and beneficiaries who fall along this spectrum.

Managing security of personal data in a world of technology is an increasingly specialized business. Many organizations use specialized firms to test their security systems, and to provide special services or software to assist them. However this is more common for larger employers and larger TPAs.

Benefit plan administration is often outsourced and the administration of defined contribution plans is almost always outsourced. Generally, an increasing percentage of plan transactions can be conducted automatically through technological means such as the internet. In addition, payroll administration is generally automated, with benefit plan contribution information being electronically transmitted directly from the payroll processor to the record keeper. In the benefits area, plan funds are held by a trustee, which may be, in some circumstances, the same entity as the record keeper or investment service provider or one of their affiliates. Within this framework, plan sponsors very often look to TPAs and trustees to play major roles in providing security and privacy of plan data. It is not unusual for the plan sponsors to see protection of the security and privacy of plan data as part of the responsibility of external plan trustees, plan administrators and service providers. There is an expectation that these third parties will perform due diligence and execute effective security standards with regard to plan funds.

The question arises concerning the appropriate standard of due diligence to be used to evaluate controls over the security and privacy of the PII of plan participants and beneficiaries, especially since this information is such a critical part of the operation of the plan and its protection is so important to the welfare of plan participants.

Post-separation transactions, such as plan distributions, present a particular point of vulnerability. Particular attention is needed at the time of authorization of distributions to ensure that the PII of a participant or beneficiary has not been compromised. With the wide range of interaction in processing data, maintaining data for long periods of time, and vital information needed at the time of distribution to ensure correct authorization, the responsibility to ensure privacy and security of PII generally expands to include anyone who comes in contact with the data.

The Council heard testimony that service providers (like banks or those servicing banks, insurance company products and/or mutual funds) use a variety of techniques to enhance security at the time of payment including, for example:

- Offering participants the opportunity to lockdown their accounts so that distributions are not available until the participant unlocks the account.

- Multi-factor authentication, including:

    - Additional security questions for larger distributions and after an address change,
    - Computer software that identifies standard log-in location for the participant and imposes added security for non-standard locations,
    - Use of tokens for added security, and
    - Sending an e-mail or text message to confirm that distribution is being processed.

- Sign-offs on distributions by authorized parties.
- In defined contributions plans a spousal consent is required for a beneficiary payment to someone other than a spouse and in a pension plan the spouse must consent to an alternative form of distribution other than a joint and survivor annuity or alternative form of distribution. This spousal consent requirement does provide some additional security for such distributions because an additional signature is required.
- Mailing changes in PIN numbers and address change verifications to participants and then imposing a wait time for distributions.

Many TPAs are affiliated with mutual funds, banks or insurance companies which must comply with extensive regulation regarding privacy and security of data and PII in their normal course of business. These entities generally have extended these same security and privacy procedures to the third party administration portion of the business, even though it is not required. It is simply easier to run a business with one set of security protocols. In addition, TPAs that provide services to health plans must comply with, the Health Insurance Portability and Accountability Act of 1996 (HIPAA). However, some TPAs are independent and are not subject to any of these regulatory requirements. One of the witnesses who is responsible for administering both retirement and health care plans testified that when regulations apply in one area of the business, for example HIPAA regulating health care, it is very likely the standards of regulation will influence how other aspects of the business is conducted. For example, those TPAs who administer both HIPPA regulated health plans and retirement plans will often adopt similar security protections whenever practical. The Council also heard testimony that sometimes in a merger or acquisition of service providers for benefit plans (including TPAs that are exiting the business), older systems are acquired as part of the transaction. Often, these older systems could be points of vulnerability because the modern technology cannot be used to update the security measures on the acquired system.

From the testimony received, the Council learned that there is no comprehensive regulatory framework for TPAs or other service providers. More specifically, if there is a security breach, there is no uniform requirement to disclose the breach or the method to remediate the breach. The Council was not given any information regarding any method to determine the extent TPAs not linked to regulated business entities are securing PII, or to determine particular points of vulnerability. Because access to PII is important to the administration of benefits plans, even smaller TPAs who may provide administrative

support only (for example, TPAs conducting non-discrimination testing) will need to pay attention to protecting PII.

Access to plan information, PII and other financial information becomes necessary in cases where TPAs, plan sponsors, and other professionals provide advice to individuals in broader financial and retirement planning, especially with respect to the management of distributed funds. Broader financial planning requires consideration of all of the individual's financial resources, which can sometimes lead to tension between having access to a wide array of PII or a greater focus on privacy and security for the information, potentially resulting in a more limited amount of information being available.

The Council heard testimony from the multi-employer plan community indicating that these plans face different issues because a number of plan sponsors submit the necessary information to the TPA. In addition, the Council heard testimony that some of these plans are small and not automated. Multi-employer plans are often established in industries where the participants use different methods to communicate with plan administrators. In some, there are many individuals without regular computer access. For example, the Council was told that in one plan, the participants commonly pick up their distribution and other benefit payments in person.

D. Current Legal Environment

The Council heard testimony regarding the complex legal requirements governing mutual funds, banks, insurance companies, and health benefit plans with regard to securing and protecting PII. The laws and regulatory framework include:

Fair Credit Reporting Act (FCRA)

The FCRA regulates, among other things, the collection and dissemination by a consumer reporting agency of information about an individual's (consumer's) criminal, employment, and educational history, creditworthiness, and other personal characteristics. The FCRA's definition of "consumer reporting agency" encompasses, for example, credit bureaus and background check companies.

Fair and Accurate Credit Transactions Act (FACTA)

An amendment to the FCRA under FACTA requires the three nationwide consumer reporting agencies (i.e., Equifax, Experian, and TransUnion), as well as nationwide specialty consumer reporting agencies (i.e., agencies that report on a nationwide basis on medical payments; residential, check writing, or employment history; or insurance claims), to provide, upon request from the consumer and free of charge, one disclosure of the consumer's file during any 12-month period. FACTA also permits a consumer who is the victim of identity theft to place a fraud alert on the consumer's file with the nationwide consumer reporting agencies. For 90 days, an initial fraud alert tells creditors to follow certain

procedures, including contacting the consumer, before opening any new account or changing an existing account.

Gramm-Leach-Bliley Act (GLBA)

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLBA, protects consumers' non-public personal information maintained by a covered financial institution. Covered financial institutions include banks, mortgage brokers, credit unions, financial or investment advisory services providers, auto dealers that lease and/or finance, collection agencies, and other creditors.

While these laws touch on certain transactions within the financial industry, they do not require protection of PII in the transfer and sharing of PII throughout the administration of retirement plans. Consequently, there is a current patchwork of federal laws that impact the privacy and protection of PII in various transactions and at different stages of retirement plan administration, but not at the plan level.

In addition to these federal regulations, nearly all states have some type of privacy laws and these laws are not uniform. These laws have spill-over effects on benefit plans and their administration, but often do not directly apply. Some of those laws, as of October 2010, include:

State Identity Theft Legislation

Identity theft is a crime in every state. While the definition of identity theft varies among the states, the crime typically involves the use of the victim's personal information, such as SSNs, driver's license number, or credit/debit card number, to commit fraud or other crimes.

State Consumer Report Security Freeze Laws

47 states (Alabama, Michigan, and Missouri are the exceptions) have enacted laws that require the nationwide consumer reporting agencies (i.e., Equifax, Experian, and TransUnion) to place a security freeze (also known as a credit freeze) on a consumer's file, upon request from a consumer. A security freeze prohibits the consumer reporting agency, with limited exceptions, from releasing any information in the consumer's file without the consumer's authorization.

State Security Breach Notification Laws

46 states (Alabama, Kentucky, New Mexico, and South Dakota are the exceptions), as well as the District of Columbia, Puerto Rico, and the U.S. Virgin Islands, have enacted laws requiring organizations that have suffered a security breach to notify those individuals whose personal information has been compromised.

State Laws Protecting Social Security Numbers

More than 30 states have enacted legislation restricting certain uses and disclosures of SSNs. These laws generally prohibit (a) the public display of SSNs, (b) printing SSNs on any card, such as an insurance ID card, that an individual must show to obtain products or services, (c) requiring an individual to transmit his/her SSN over the internet unless the connection is encrypted, (d) requiring an individual to use his/her SSN to access a website unless a password or other authentication device is required to access the website, and (e) mailing documents that contain an individual's SSN to the individual unless the document by law is required to include the SSN, such as a Form W-2.

State Laws Requiring Proper Disposal of Personal Information

More than 25 states have enacted laws that require disposal of personal information in a secure manner (for example, by shredding paper documents or "cyberscrubbing" electronic storage media). The definition of "personal information" in these laws varies but generally includes first name or initial and last name in combination with a SSN, driver's license number, credit or debit card number, or financial account number with any required security code. Some states also include health information and other types of sensitive information in the law's definition of personal information.

ERISA does not directly address whether and how employee benefit plans should protect PII of participants (and beneficiaries) of retirement benefit plans. There has not been any jurisprudence concerning the potential of ERISA preemption of state laws concerning PII. ERISA's preemption provision may not reach many of these state laws. Consequently, plans have to comply with many of these state laws including SSN disclosure laws because there are no overall federal issued guidelines. Thus, the Council believes that as state laws are developed in the area of privacy of financial data and other PII, retirement plan administrators will need to be mindful of these laws and adjust their administrative practices accordingly. *See* discussion of proposed legislation at section VI.D.1. below.

IV. SUMMARY OF TESTIMONY AND COUNCIL DISCUSSION

A. Issues Facing Plan Sponsors and Administrators

1. Points of Vulnerability

The testimony heard by the Council, and follow-up research conducted by the drafting team, provided consistent information about sources of vulnerability and areas where it is critical that those with access to PII take appropriate action. The testimony also indicated that giving these matters organizational priority and enforcing company policies are important aspects of any effective security program. The Council, from testimony and submitted articles, identified four major areas for effective practices and policy as

follows: data management, technology management, service provider management and people issues. The Council heard testimony from service providers and security system experts that supported the conclusion that certain practices were effective in minimizing misuse of PII. See "Chart of Practices Useful to Certain Plan Administrators to Minimize Security Breaches" in section IV.A.2 below for a review of some of these practices suggested for adoption by plan administrators.

i. Data management

The Council learned that problems generally arise when data is not well protected and that control over the data must be maintained at all times. A system is no stronger than its weakest link. Testimony indicated that: (1) not all participants will deal with automated systems; (2) there can be conflicting objectives in the area of data privacy and security and other priorities – on one hand, it is best to keep only the data that is absolutely necessary, but on the other hand, if any entity wants to assist participants with broader planning, more data is needed; and (3) some of the problems related to data security include keeping more data than needed, keeping data that is no longer relevant, failing to keep controls over back-up copies, including electronic tapes, and not knowing the entire group of people having access to the data.

ii. Technology management

The Council learned that failure to execute and continually update effective management of technology can be a source of many problems, resulting in inadequate and out-of-date technology; outdated or poor technology design; weak system and process design; failure to promptly apply system updates; inadequate authentication; inadequate control over wireless and portable devices (including thumb drives and CDs); failure to use, or improper use of, encryption; and allowing cyber criminals the ability to infiltrate a system that is not adequately secured. The testimony noted that an area for focus in today's market is multi-factor authentication, which goes substantially beyond the use of a sign-in name and a password.

iii. Service provider management

Record keepers and other service providers play a major role in helping to protect information. The Council recommended that DOL provide information to plan sponsors to help them with executing due diligence about plan data security in the selection and monitoring of service providers (including TPAs). The testimony revealed that while many service providers have extensive security and privacy control systems in place and currently exercise a high level of diligence, some service providers may not have exercised much effort regarding data security and privacy. The testimony highlighted that one of the challenges faced by plan sponsors is to be sure that the service provider has appropriate security and privacy systems and that all groups who have access to plan information should consider the protection of plan data.

iv. People issues

Problems have been caused by hiring the wrong people, and by failure to properly train and manage personnel. Testimony indicated that employees of the plan sponsor or administrator can be a traditional source of fraud and that good employees can become problem employees when they are under pressure from family, health issues, substance abuse, gambling problems or other financial pressures. The testimony highlighted the ease by which employees who are not well trained can be socially engineered, e.g., tricked into giving crucial access information and/or PII to criminals who will commit fraud on the participants. Also, the testimony showed how poorly trained people may inadvertently fail to pay attention to red flags of fraud that would be obvious to trained personnel.

The Council also heard testimony that disconnects in the organizational structure of a company can often contribute to the problem of unsecured data in benefit plans, such as when the company's information technology specialist is the person responsible for handling the security of computer systems for the company, while the benefits and human resources personnel generally are responsible for maintaining the privacy and security of personal data for company's employees. The Council learned that more coordination in this area could help decrease the number of problems otherwise encountered in providing privacy and security to plan data, including PII.

v. Challenges for Small Business

While small businesses have not been the main historical targets of cyber-thieves, the Council heard testimony that indicates this is quickly changing. Alan Brill pointed out that cyber-thieves have started to target smaller businesses, particularly as larger organizations take steps to implement more sophisticated security measures. In these cases, small businesses believe that because they are small they are not vulnerable. This false sense of security has led to fertile ground for cyber-thieves. An article on the front page of the July 21, 2011 WALL STREET JOURNAL, entitled *Hackers Shift Attacks to Small Firms,* indicated that in 2009, 27 per cent of cyber-attacks (141 attacks) were made on businesses with 100 or fewer employees, with an increase to 63 per cent (763 attacks) in 2010.

Testimony presented stressed that small businesses may have limited resources to devote to privacy and security of plan data including lack of access to the specialists with expertise in managing these issues. The testimony stated that these small employers are more likely to be totally dependent on the TPA for providing security for the data of benefit plan participants and beneficiaries. According to the testimony, these plan sponsors are less likely to be sophisticated with respect to selecting and monitoring TPAs. The Council concluded that information to assist small employers to exercise greater due diligence in this process would be particularly helpful.

vi. Participants and Beneficiaries

The Council heard testimony confirming that is it important to educate participants and beneficiaries about their role in protecting data, SSNs and other PII because they inadvertently may become a weak link in the efforts to secure and protect PII.

2. Chart of Practices Useful to Certain Plan Administrators to Minimize Security Breaches

Practices	**For TPAs, Record keepers**	**For Employers and Plan Sponsors**
Computers and Systems		
A. Data		
1. Keep only data that is needed.	✓	✓
2. Use effective processes to discard unnecessary data, including back-up paper and electronic copies.	✓	✓
3. Know where PII is located in all of the organization's systems.	✓	✓
4. Understand cloud computing and/or remote data storage, including how data is stored or protected.	✓	✓
B. Systems		
1. Keep computer systems updated, including prompt installation of software patches.	✓	✓
2. Stay current on electronic threats and effective responses.	✓	✓
3. Follow National Institute of Security and Technology (NIST) guidelines on computer configuration.	✓	✓
4. Use full disk encryption on laptops and external data storage devices that might include PII or information on how to access it.	✓	✓
5. Maintain complete log-in for the network, firewalls, routers and key software applications.	✓	✓
6. Limit or define usage of portable devices.	✓	✓
People and Training		
1. Perform criminal background checks and drug screening for employees with access to PII.	✓	✓
2. Ensure all personnel who have access to PII are trained in properly safeguarding it. Include training in areas such as data retention/destruction, social networking, social engineering, and litigation holds.	✓	✓

Practices	**For TPAs, Record keepers**	**For Employers and Plan Sponsors**
3. Designate an individual to be in charge of privacy and security.	✓	✓
4. Educate all stakeholders regarding appropriate focus according to their roles.	✓	✓
5. Implement and test contingency plans for use in event of data breach.	✓	✓
Service Provider Management		
1. Consider privacy and security factors regarding the selection and performing of due diligence for providers.		✓
2. Make sure provider subcontractors are held to same standards as service provider.		✓
General Tips		
1. Make sure to know what partners have access to PII and that they are paying attention to these issues.	✓	✓
2. Perform periodic risk assessments (Generally Accepted Privacy Principles).	✓	✓
3. Maintain good controls and be careful about who can over-ride them.	✓	✓
4. Use a process to confirm compliance with policies.	✓	✓
5. Make sure policies are clear and communicated to all appropriate parties.	✓	✓
6. Adopt a privacy policy designed for the organization.	✓	✓
Special Concerns for Employees		
1. Educate employees about the importance of safe-guarding their data at all times.		✓
2. Focus on security measures in place for distributions. Ensure added security for participants at time of distribution.		✓

3. Outreach to Plan Sponsors

The DOL has at least one resource that addresses some of the issues discussed above, namely *Tips for Selecting and Monitoring Service Providers for Your Employee Benefit Plan,* http://www.dol.gov/ebsa /newsroom/fs052505.html. Rather than developing a completely new publication, this tip sheet could be updated to address issues related to privacy and security for pension plans. The tip sheet could include a questionnaire that would focus on key areas in the selection and monitoring of plan administrators or other service providers.

In addition, DOL should develop materials that highlight the need for plan sponsors to address privacy and security in plan administration. These materials could include factors to consider and adopt when developing and implementing privacy and security policy. The materials should highlight methods available for monitoring actions plan administrators take with respect to privacy and security, such as certifications plan administrators may obtain based on compliance with certain privacy and security standards, industry-used assessments on privacy and security, and remediation in the event of a security breach. Finally, the materials could discuss the need for, and methods of, additional layers of security at vulnerable decision and receipt points including plan loans, withdrawals, and distributions.

The Council's recommendations provide for expanding and producing companion educational resources. Information about updating and expanding these resources is included in Appendix A.

B. Issues facing participants and beneficiaries

1. Points of vulnerability

The testimony from witnesses confirmed that a significant source of vulnerability in protecting PII involves actions or inactions by participants and beneficiaries. Although plans and their service providers can do a lot to protect PII, participants and beneficiaries also need to be informed about their responsibilities and rights in protecting their PII held in retirement and welfare benefit plans.

The Council heard testimony regarding how individuals can contribute to the problems surrounding the security and privacy of PII, either by personal action, inattention or failure to act. The Council learned from testimony that individuals are particularly vulnerable when accessing plan funds. Some of the common things individuals do that contribute to the challenge of protecting PII include:

- Sharing passwords and log-in personal information with others;
- Failing to update passwords
- Using passwords rated low for security protection;
- Saving passwords to retirement plan data on various websites including portals;
- Failing to install software updates regularly;
- Being unaware of phishing and other electronic gambits which will leave their computers and PII at risk;
- Using computers, mobile and other electronic devices, and copy machines in unknown and/or unprotected places, such as wireless cafes;
- Failing to eliminate unnecessary information from personal computers;
- Sharing of, or failing to guard, personal information such as Social Security numbers, birthdates, mother's maiden name, etc.;
- Failing to monitor their accounts on a regular basis;
- Placing too much personal information on social networking sites;

- Sending personal information via e-mail or text message, which can be more vulnerable;
- Giving Powers of Attorney to people who do not have the elderly's best interests at heart; and
- Not recognizing scam artists and other attempts at social engineering to obtain PII and financial assets directly.

2. Elder abuse and challenges for those with little or no technology skills.

The Council learned from testimony that, in many respects, elder abuse is an important and growing subset of the social engineering problems as the United States population becomes increasingly older. See Administration on Aging, *A Profile of Older Americans: 2010*, http://www.aoa.gov/aoaroot/aging_statistics/Profile/2010/3.aspx. The Executive Director of the National Adult Protective Services Association indicated that the reported statistics concerning elder abuse are widely considered to be lower than the actual occurrences for two reasons: many people do not consider certain types of incidents to be elder abuse, and generally all occurrences are underreported. According to her testimony, seven to twelve percent of elders are subject to abuse, and many more elderly individuals may be subject to such abuse. The testimony noted that there are multiple contributors to such abuse including family members who often have alcohol, drug or gambling problems; caregivers; trusted individuals; and outsiders trying to scam the elderly. In addition, the testimony noted that trusted family members and individuals may misuse Powers of Attorney for their own purposes.

The Council learned that the reasons for elder abuse in these instances are simple. Older persons tend to have more assets than younger persons. They are also more vulnerable and are oftentimes less sophisticated about technology. For example, an older person may be retired and receiving retirement payments from a defined benefit and a defined contribution plan. In addition, they are generally receiving monthly Social Security checks. The testimony noted that retired individuals may be particularly vulnerable just after receiving a lump sum distribution upon retirement or termination of employment.

The testimony and submitted resources highlighted a related, but different, issue for other demographic groups that are less technologically savvy. For example, unbanked or under banked participants might be automatically enrolled in a retirement plan but not maintain any other accounts with a financial institution. This group has been found to be less familiar with the technology of online systems.

3. Outreach and educational efforts

The DOL already has resources that address some of the issues discussed above, e.g., *Ten Warning Signs That Your 401(k) Contributions Are Being Misused*, http://www.dol .gov/ebsa/Publications/10warningsigns.html; *Taking the Mystery Out of Retirement Planning*, http://www.dol.gov/ebsa/publications/nearretirement.html. In addition, the Federal Trade Commission has more general consumer information about identity theft, which would be helpful information for participants and beneficiaries. *See*, e.g., Federal

Trade Commission, *Fighting Back Against Identity Theft - Deter: Minimize Your Risk,* http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/deter.html.

The BITS (the Technology Policy Division of the Financial Services Roundtable) report entitled *Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation* sets forth numerous types of scams, as well as indications of when an individual may be a victim of financial elder abuse. See BITS Fraud Protection Toolkit, *Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation* (Feb. 2010), http://www.bits.org/downloads/Publications%20Page/ProtectingVulnerableAdults ToolkitApr2010.pdf.

The Council's recommendations provide for expanding and producing companion educational resources. Information about updating and expanding these resources is included in Appendix A.

VI. RATIONALE FOR RECOMMENDATIONS AND OBSERVATIONS

The Council's recommendations fall into three categories: clarification of plan fiduciaries' obligation under ERISA to protect PII; outreach and educational efforts to all stakeholders to help them address the issues affecting the protection of PII; and outreach and educational efforts to all stakeholders in order to increase awareness of issues affecting elder abuse. In addition, the Council had two major observations: (1) potential legislation on cyber security should be clear on its applicability to employee benefit plans, and (2) plan sponsors and administrators would benefit from a clearinghouse or other information resources to share information.

A. DOL Guidance on Fiduciary Obligation to Protect PII

It was generally noted that technology is constantly changing, along with the nature of cyber attacks and the responses to those attacks. Many of the entities providing services to employee benefit plans are regulated in some manner[2] and creating specific rules just for employee plans would neither be helpful nor cost-efficient. Instead, the witnesses made clear that security measures should be layered and tailored to a particular organization depending on their role in the benefits structure, their technological savvy, and the interface between them and the other stakeholders in the plan.

Witnesses and the Council agreed that protecting such data is important in order to protect plan funds. However, both the testimony and discussion among Council members demonstrated that there is a difference in opinion over whether there is any fiduciary responsibility to protect PII, and if so, the scope of that duty. Thus, clarification of this issue would be helpful to plan fiduciaries and service providers.

[2] Not every record keeper and similar party which touches PII for ERISA plan participants are captured by these alternative regulatory structures. The Council did not determine the number of entities outside these alternative regulatory structures or the rigor of their security measures.

B. DOL Education and Outreach to Stakeholders on Protection of PII

Although there is no reporting or regular data compiled on data breaches involving employee benefit plans, testimony noted that both private and public employee benefit plans had suffered data breaches involving the plans' PII. Witnesses discussed the current technological environment and the layered approach to protecting data. Several of them detailed practices that either they or their clients had found effective in preventing or lessening the possibility of data breaches. These suggested practices concerned computers and technology; people and training; general policies and procedures; and increased participant involvement in the benefit environment as defined contribution plans become even more prevalent.

The Council notes that varying levels of technological sophistication of participants and beneficiaries present some interesting issues to plans and service providers. More technologically savvy participants may want to use mobile devices to interface with their employee benefit accounts, which present a different set of issues than those who merely use computers. On the flip side, older and less technologically savvy participants cannot or may not wish to use computers at all.

The Council heard repeated requests for tools and information resources for plan sponsors and administrators to include, among others, a list of best practices; a sample model privacy policy; a checklist to use detailing security and privacy issues when issuing Requests for Proposals for selecting and monitoring administrators and other service providers; and education for participants. Consequently, the Council recommended that DOL develop educational materials and outreach efforts, and identified current publications that could be more easily updated to enable a quicker response to the Council's recommendation.

C. DOL Education and Outreach on Elder Abuse

With the United States population increasingly aging, employee benefit plans potentially holding a large amount of older persons' assets, with more participants electing lump sum distributions, and technology making potential financial abuse easier to hide, the Council recommends that DOL include in its outreach efforts and educational materials information regarding elder abuse to appropriate stakeholders to increase awareness of elder abuse issues related to benefit plans. The BITS Elder Fraud Prevention Toolkit, used by banks and other financial services, has proven successful in identifying potential elder abuse and can be used as a template by DOL.

D. Important Observations

As the Council heard testimony and performed its research, two related observations emerged as important on the issue of privacy and security of PII.

1. New Legislation

The Council heard that although there are numerous federal and state laws dealing with privacy and security, their applicability to employee benefit plans is unclear and their requirements may be inconsistent. The Council noted it would be helpful to stakeholders in the benefits community for legislators to be clear about the applicability and scope of new legislation on privacy and security to benefit plans.

The Council observed that:

> The current Administration's proposal on cyber security would attempt to unify and build on a complex and scattered State and Federal legislative structure. Plan sponsors are confronted with not knowing which legislation applies to them. The Council considers it important that groups working on cyber security or other legislative proposals relating to PII take into account issues related to the administration of retirement plans and be clear as to what does and does not apply.

2. Information Sharing

As work progressed on this issue, it became apparent that there are substantial resources and information on privacy and security issues, but they are not easily accessible if an individual is not already familiar with this topic. In an effort to make information on security and privacy more accessible and user-friendly to those in the benefits community, resources should be centralized and an information-sharing resource for benefit plans to exchange information, concerns and ideas should be established. Appendix B lists a number of resources.

The Council observed that:

> There are number of resources and information related to privacy and security of pension plans. The Council discussed the importance of helping plan sponsors and administrators have access to helpful or beneficial information and hopes that an appropriate party, or parties, will establish a clearinghouse and information resource.

VII. CONCLUSION

The Council's modest efforts here only highlight the importance of the protection of PII of participants and beneficiaries, and the difficulties in so doing. The protection of this information will only grow in importance as technology continues to quickly change and evolve, accompanying threats become more frequent and sophisticated, and the shift from defined benefit to defined contribution plans continues, requiring participants and beneficiaries to become even more responsible for their own retirement monies. Moreover, plans must deal with participants and beneficiaries who range from those who

are extremely tech savvy to those who do not use technology. The types of organizations dealing with PII are equally as varied, including small and large plans, service providers and plan sponsors. Consequently, as technology continues to advance, the Council suggests that the issue of security and privacy should be reviewed again by DOL in a few years to survey the state of the industry, the response of stakeholders in the benefits community, and current problems.

The Council again expresses its appreciation to DOL and all of the persons and entities whose time and effort contributed to this report. The Council respectfully commends its recommendations to the Secretary, which will bolster her efforts to promote and protect benefit plan security for participants and beneficiaries. Beyond the utility of the recommendations, the Council hopes that its exploration of the issues related to privacy and security of PII will be of interest and assistance to all stakeholders.

APPENDIX A

Information to Support Implementation of Outreach Recommendations

The Council's recommendations with regard to outreach and education focused both on updating and supplementing existing DOL outreach resources, as well as creating some additional resources. We provide suggestions here for possible content to assist DOL in implementing these recommendations.

APPENDIX A-1

Suggested Revisions to DOL Publications

DOL's current *Tips for Selecting and Monitoring Service Providers for Your Employee Benefit Plan*, available at its website under EBSA, provides a list of items to be considered in choosing a service provider, but should be updated to include factors relevant to security and privacy issues. Suggested topics for the list might include:

- What are the service provider's processes and systems for dealing with cyber-security threats and protection of PII?
- Does the company have a privacy and security policy, and does the policy apply to data held by benefit plans?
- Is the company's policy clear with respect to storing PII on laptops and portable storage devices? What is that policy?
- Is advanced authentication used by the company? Can the service provider explain the process? Can you explain it?
- Are technology systems regularly updated?
- Does the service provider have policies on storing PII including where it is stored, how long it is stored, and how it is eliminated?
- Are all personnel who come in contact with PII trained on adequate protection of the information?
- Does the company carry cyber-security insurance?
- Has the company experienced any security breaches?

APPENDIX A-2

Suggested Revisions to DOL Publications

DOL's current *Ten Warning Signs That Your 401(k) Contributions Are Being Misused*, available at its website under EBSA, is a reference tool that should be promoted as the information included could help individuals uncover some breaches of PII. In addition, the Council recommended that DOL produce and promote a companion piece to this publication that would focus on *Warning Signs* and tips for protecting an individual's retirement sources and PII. Suggested topics for consideration include the following information for individuals:

- Regularly check account balances;
- Look for unusual transactions when checking account balances;
- Promptly change address to reflect any change in residence;
- Safeguard passwords and update them regularly;
- Set up strong passwords that are less vulnerable;
- Avoid use of another's computer in hotel business centers; internet cafes, or other public places to conduct financial transactions without knowing the security of that computer;
- Exercise caution when using outside copy or FAX machines;
- Protect identity by not leaving documents with identifying information like Social Security numbers easily accessible to others;
- Exercise caution before actually authorizing another to act through a Power of Attorney even when family members are involved.

APPENDIX A-3

Suggested Revisions to DOL Publications

DOL's current *Taking the Mystery Out of Retirement Planning,* available at its website under EBSA, provides information to people who are nearing retirement. Chapter V of the publication includes a number of helpful resources regarding investment scams but does not include any discussion of identity theft, elder abuse, or Powers of Attorney. Suggested ideas for update of the publication might include the following:

- Information on pension scams and steps on how to avoid them;
- Steps describing how participants can ensure that plan transactions (such as obtaining plan loans, withdrawals and other plan distributions) are exercised securely;
- Items incorporated from Appendix A-3 on protecting pension information;
- Explain that participants should be wary of e-mails or telephone inquiries from unknown sources;
- Explain that individuals should not provide information in response to e-mails or telephone requesting personal information;
- Caution individuals against performing financial transactions in cyber-cafes and hotels using unknown computers to prevent the potential capture of their personal information;
- Note that pass codes should be changed immediately if there is any possibility that they have been lost or compromised.

DOL could also add a paragraph regarding elder abuse and the need to be careful about people you work with, including relatives and friends. Some ideas could include:

- Highlight that at least 10 per cent of the elderly are subject to financial abuse at some time, and it is often from family members or trusted individuals;
- The elderly should be very careful when selecting a person to give their power of attorney;
- The elderly should be very careful not to disclose their passwords, and, if they must, make sure it is to a trusted individual;
- If the elderly has a family member who helps them with financial matters, it is helpful to have another person check over everything.

Chapter VI of *Taking the Mystery Out of Retirement Planning* also includes references that can be helpful, including a link to the Financial Literacy & Education Commission's website available on the website of mymoney.gov. The Commission's website includes a section on frauds, scams and identity theft. A cross-reference between the *Taking the Mystery Out of Retirement Planning* webpage and the Commission's materials on scams and identity theft, also available at the mymoney.gov website, could be

beneficial to individuals who may be able to use this information in protecting their finances.

Other resources:

- A joint report highlighting elder financial abuse, commons signs, and ways to stop it, published by The Women's Institute for a Secure Retirement and The National Adult Protective Services Association. *See Issue Brief on Elder Financial Abuse*, available at the website for WISER.
- See The National Adult Protective Services (NAPSA) website providing further resources on elder abuse, including information for organizations that have information on elder abuse.
- The Technology Policy Division of the Financial Services Roundtable, provides materials on Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation from April 2010. See the BITS website (BITS.org) that includes a discussion of types of abuse and scams, and information to help financial institutions work with their customers to recognize and report scams. There are other links for more information on working with law enforcement agencies. The information included could be helpful to individuals, family members, plan sponsors and plan administrators. *See Protecting the Elderly and Vulnerable From Financial Fraud and Exploitation*, available at the BITS website.

APPENDIX A-4

Resources for Plan Sponsors

Sources of information on regulation, outside review and accreditation of certain service providers in the benefits area are helpful in determining appropriate methodology for due diligence when vetting providers, in understanding the extent to which others are probably looking at security systems and determining when obtaining cyber-security insurance is prudent.

Due Diligence

In performing due diligence, it is helpful to know whether an organization is subject to regulation regarding the security and protection of PII as well as whether another organization has conducted a review of its security processes. Some resources for this information are available as follows:

- The Center for Fiduciary Excellence (CEFEX), working with American Society for Pension Professionals and Actuaries (ASPPA), offers a Service Provider Certification Mark. See CEFEX's website. The certification program is based on best practices that include some review of the management of PII.
- The American Institute of Certified Public Accountants' standards known as the Statements on Standards for Attestation Engagements (SAE) 16 replaces Statement on Auditing Standards 70 and provides for independent review of an organizations privacy and security processes. This review is presented in a Service Organization Control Reports (SOC) 1, SOC 2 or a SOC 3 report. These reports can cover a range of issues, and some of them deal with the protection of PII and controls maintained by the service provider. *See* Appendix B and the witness summary for Ian McKay for more information on the nature and content of these reports and how they differ.
- Various technology standards exist. The Federal Finance Institutions Examination Council (FFEIC) (described in Appendix B) is a resource for technology standards as they apply in banking. The International Organization for Standards (ISO) is a source of international standards. See website for ISO.

Cyber-Security Insurance

Testimony from a few witnesses stated that cyber security insurance can be purchased to provide protection against the cost of remediation in the case of a security breach, with the insurance generally covering reporting requirements after a breach has occurred under applicable state legal requirements. The Council did not investigate how the insurance works or how common it is for businesses to purchase such insurance, but testimony indicated that it is a relatively new product and requires an extensive qualification process. The availability of this insurance may signal the growing importance of cyber security of PII and other financial data.

APPENDIX A-5

Resources for Plan Sponsors

The following SAMPLE CHECKLIST is not a Power Of Attorney, nor is it a comprehensive legal checklist. Instead, the sample checklist is intended to help employers review the treatment of major transactions normally executed by plan participants or beneficiaries in defined contribution retirement plans when a third party acts on their behalf. The sample checklist does not address nuances of whether the Power of Attorney is validly executed in a specific jurisdiction (e.g. how many witnesses are required, etc.) and is not intended as legal advice.

Sample Power of Attorney Checklist for Plan Sponsors and Administrators

The purpose of the Power of Attorney Checklist is to confirm whether the Plan will accept a Power of Attorney that is presented to the plan by an agent for the participant or beneficiary with respect to decisions on behalf of the named participant or beneficiary regarding transactions under the Defined Contribution Plan:

Name of Defined Contribution Retirement Plan
Name of Participant or Beneficiary

Indicate the purpose of the Power of Attorney. For example, Check all that apply:

_____ 1. Make investment elections.

_____ 2. Make distribution elections, including loans and withdrawals.

_____ 3. Change or name beneficiary.

_____ 4. Agent may name self as beneficiary.

Indicate that the Power of Attorney has been reviewed by the legal department and whether it is accepted as having complied with the state law in which it was executed.

Ensure signature of both the Plan Administrator and Participant/Beneficiary.

Indicate that the plan sponsor or fiduciary has accepted the Power of Attorney and state the purposes. For example:

Check all that apply

_____1. Make investment elections.

_____2. Make distribution elections, including loans and withdrawals.

_____3. Change or name beneficiary.

_____4. Agent may name self as beneficiary.

APPENDIX B

Resources and Sources of Information on Matters Studied for the Report

This section presents some ideas with regard to developing a resource center. A description of some of the organizations and their efforts are set forth below:

Obama Administration proposed cyber security legislation: This proposal would replace the laws in nearly all states with a unified approach to cyber security. It also would strengthen and unify applicable penalties for cyber crime. The proposals provide for government assistance to various groups and clarify the role of the Department of Homeland Security. A fact sheet was released on May 12, 2011, which can be found on the website for the White House..

AICPA Organization Control Reports: The accounting profession has recognized the importance of privacy and security in providing effective controls to protect data and funds. The AICPA in SSAE 16 provides three types of Service Organization Control Reports (SOC 1, SOC 2, and SOC 3). This guidance, which became effective in 2011, replaces and expands the SAS 70. SOC 2 reports are voluntary and may be structured to respond to different portions of organizational controls such as privacy, security, business continuity and anti-money laundering. SOC 2 reports are long and technical limited use reports, but deal specifically with privacy and security issues. SOC 3 reports are summarized reports designed for public use. The scope of examination in these reports depends on the engagement and is at the discretion of the organization requesting the review. Organizations wishing to conduct due diligence on matters where there is a SOC 1, SOC 2 and/or SOC 3 report will probably find that there is helpful information in these reports. A service organization logo linked to SOC reports is available, and it also may be helpful in due diligence. SSAE 16 became effective in mid-2011, and the importance and helpfulness of these reports will develop as it is implemented by more organizations. There are two types of assignments under these standards – those analyzing control structures and those also testing their operation. The new SSAE 16 standard goes significantly beyond the prior standard, the SAS 70, as it provides for review and auditing of controls that are not directly linked to the financial statement. Testimony was presented which stated that the marketplace demand will drive how widely used these reports become.

AICPA General Accepted Privacy Principles: The AICPA, jointly with the Chartered Accountants of Canada (CICA), promulgated Generally Accepted Privacy Principles (GAPP) which address a wide range of privacy and security issues. They include recommended mitigation strategies. This resource can offer information on what can and should be done in appropriate settings.

AARP is a nonprofit, nonpartisan organization with a membership that helps people age 50. In November 2011, AARP's Public Policy Institute released a new research report focusing on older investors with diminished capacity -- and how financial services professionals, regulators, and other stakeholders can best meet their needs. The report noted that increasingly, older people are responsible for their own retirement security in

an era of defined contribution plans and other forms of "do-it-yourself" retirement. According to the report, financial capacity is the first kind of decision-making capacity to decline with the onset of dementia and other causes of cognitive impairment. The report raises the questions whether financial services industries prepared for the age boom and increased incidence of diminished capacity. The report includes information on diminished financial capacity, the risk of financial exploitation, and the financial professionals who serve older clients. In addition, the report shares results of a national survey of financial professionals and an interdisciplinary roundtable about current practices, protocols and needs—and makes recommendations for federal and state policy-makers, industry, aging organizations and other stakeholders. The report by Naomi Karp & T. Ryan Wilson, *Protecting Older Investors: The Challenge of Diminished Capacity* (Nov. 2011), can be found at AARP's website.

ASPPA and CEFEX: ASPPA is a professional affiliation for smaller plan administrators, including those who are not affiliated with banks, mutual funds, and insurance companies. ASPPA offers education on some aspects of plan administration and has established a set of best practices for plan administration that include a focus on privacy and security. ASPPA has partnered with the Center for Fiduciary Excellence to provide a certification program for plan administrators that indicates adherence to best practices. The review in the certification process examines the control and organizational structure but does not test these controls. Organizations wishing to conduct due diligence on privacy and security in plan administration matters will probably find that the CEFEX/ASPPA certification is helpful. This could be valuable to smaller plan sponsors who do not have their own experts in IT to help in the evaluation of their controls and organizational structure. Organizations could use the ASPPA best practices to help them identify what issues to cover in due diligence. As with the SOC reports, this program is new to the market and is voluntary. Marketplace demand will probably drive how popular these programs become in benefits privacy and security.

Ontario Privacy Commission: Canada has national and provincial privacy offices and provides information available on its website. Privacy by Design, available at its website, focuses on how privacy is interwoven with business management.

BITS: BITS is a division of **The Financial Services Roundtable** and a not-for-profit industry consortium whose members are 100 of the largest financial institutions in the United States. Created in 1996 by the CEOs of these institutions, BITS states that its mission is to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. The organization works to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions, BITS provides intellectual capital and addresses emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry.

Federal Financial Institutions Examination Council (FFIEC): The FFIEC is the federal Agency that oversees authentication and issues guidance for the banking industry. The FFIEC guidance Supplement to Authentication in an Internet Banking Environment

is an important resource on multi-layered and advanced authentication. The FFIEC is an important resource on security in a banking environment. The examination handbooks are helpful resources in understanding preferred practices for all who touch this data and in setting forth requirements for the banking industry. Much of the information is available on FFIEC's website.

Financial Literacy and Education Commission (FLEC): FLEC is the federal government's financial literacy and education website. This website provides resources regarding scams and frauds from many different agencies. See mymoney.gov.

Private sector general resources: The Council located several sources of information related to this topic. These are examples, and there are probably many more. The Council investigation was strongly supported by witnesses from Kroll and RSA, who provided insight into the societal issues. The Kroll and RSA websites also include fact sheets, background papers and resources. These firms support businesses in their focus on privacy and security. It is likely that other firms in this business area also have similar resources on their websites.

Resources on legal structure: The Council learned that within the United States, there are many frequently changing laws that touch on these matters. The Council also learned that the U.S. legal structure is entirely different from that in the European Union and other countries that use a variety of approaches to cyber security. Resources that offer some insights about, and summarize the legal environment include:

- Data Privacy Compliance for Employers in the U.S., Baker & McKenzie, 2010, chapter in KLUWER INTERNATIONAL LABOR AND EMPLOYMENT HANDBOOK. This chapter reviews how state and federal privacy laws impact employers and includes a number of matters that apply to benefit plans.
- Data Protection and Privacy: EU as compared to the United States, resources from the Association of Corporate Counsel, available at their website.
- The Global Employer Volume XV, No. 3, DATA PRIVACY AND PROTECTION in the Workplace from Baker & McKenzie, available at the firm's website. The first chapter of this publication provides an overview of global privacy laws, and the remainder includes a discussion of issue in many countries.
- Kroll offers a summary of United States laws which can be found at the company's website.
- The Administration proposal on cyber security which can be found on the Whitehouse's website.

APPENDIX C: WITNESS SUMMARIES

Summary of Testimony to the ERISA Advisory Council on Privacy and Security Issues Affecting Employee Benefit Plans

Jeffrey Hinman, EBSA Office of Enforcement

Mr. Hinman is the Deputy Director of Criminal Enforcement of the Employee Benefits Security Administration (EBSA). Mr. Hinman gave an overview of criminal activity involving theft or embezzlement from pension and employee benefit plans that have been investigated by EBSA's Office of Enforcement. The Department of Labor (DOL) refers cases to the Department of Justice and cooperates with other law enforcement agencies such as the FBI or IRS in some of these investigations. In a typical year, investigations by EBSA result in about 100 to 120 indictments.

Many of the cases involve illegal uses of personal identifiable information (PII). Most cases are thefts from employee benefit plans because that is where the money is; health plans are less frequently affected. In addition, most cases involve embezzlement, that is, theft committed by a party that has some control over the plan assets; such as the fiduciary, investment advisors, the third party administrator (TPAs), or certified public accountants (CPAs).

Mr. Hinman described several examples. In one case, an international criminal gang infiltrated a major TPA by getting one of their gang members hired as an employee, resulting in the theft of PII and account funds. They, in particular, targeted accounts that had little recent activity.

In another case, the manager of a retirement plan at a construction company targeted accounts where the statements were returned as undeliverable. He revised the vesting schedule of these accounts and changed the address to those of a co-conspirator who then cashed checks issued from these accounts.

An example of a case involving an outsider was the co-worker of a retirement plan participant who stole PII, called the plan to initiate a withdrawal, intercepted the mailing of the check and deposited the money.

In response to questions, Mr. Hinman said that smaller plans were generally more likely to be affected by these crimes. Larger plans tend to have more independent oversight, for example, by accountants, that deters illegal activity. In many cases, the wrongdoers have criminal backgrounds. Mr. Hinman did not know whether TPAs are performing criminal checks before hires, as they are required to do.

Alan Brill, Kroll, Inc.

Mr. Alan Brill is the Senior Managing Director in the Computer Forensics and Information Security practice of Kroll. A dedicated area of their practice is in

understanding and helping clients cope with protecting sensitive personal, financial, and health information. Because the firm is called in when a breach is suspected or has occurred, they see the issues surrounding privacy and security of sensitive personal information as they evolve around the world.

In his testimony, Mr. Brill acknowledged that most businesses operate in an environment where resources are limited, thereby forcing information security to compete with other important business needs. Against this backdrop, Mr. Brill testified about some of the lessons learned and how to avoid preventable data breaches. Despite the many advantages that technology offers, Mr. Brill testified, it brings a number of risks. The technology-law gap accounts for a significant part of the problem, Brill noted. Because technology advances at the speed of light and the laws protecting and overseeing that technology advance at legislative speed, people who are up to no good will exploit this vulnerability.

Mr. Brill testified that the elderly represent the perfect storm of risk because there are large amounts of sensitive information about them, including financial information, but they represent a segment of the population less technologically knowledgeable. Medium to small businesses in both large and small cities are also being targeted because they are often less protected and offer the value of smaller amounts quickly adding up, to cyber-criminals who often operate from anywhere in the world. He explained that retirement plans require storage of enormous amounts of highly sensitive data for extended periods that could span an individual's working life and retirement years. The personal and financial data on participants, spouses, and possible beneficiaries must be addressed in the discussion of technology security measures.

Tom Condron, Executive Vice President, Client Relationships, Guided Choice, Inc.

Guided Choice provides investment advisory services to 78,000 retirement plans with more than four million participants. Mr. Condron testified regarding some of the important data security and privacy challenges in the current environment including cloud computing, smart phones, iPads, and other mobile devices. He indicated that Guided Choice provides important data privacy and security safeguards with detailed policies, including: ethics policy within security policy; policies governing data access levels and records of login and data access, separate audits of those records; acceptable use policy; risk assessment policy; security audit policy; password policy balancing usability versus security; router security policy (no wireless in certain areas); server security policy; remote access policy (any needs to have multipoint security); antivirus policy; application service provider policy; acceptable encryption policy; email retention policy; hardware purchasing and upgrades policy; technology policy; wireless or VPN policy; third party connection policy; network policy.

Mr. Condron discussed the importance of limiting the data collected to only that data needed to provide the advice, as well as the related importance of limiting data provided to other parties (e.g., employer and TPA) to exclude information not relevant to that

party's needs (including additional personal identifiable information provided by the participant regarding non-plan assets and other personal financial information).

Mr. Condron also discussed the importance to plan sponsors and participants of a "single sign-on," so that if they logged into another system, such as the plan sponsor's network, they do not want to be required to log in again when passed to the Guided Choice website. This, too, creates challenges for data security because it relies on the security protocols and protections of the system from which the hand-off is received. He also noted some unique challenges for unbanked participants, who might be automatically enrolled in the plan but not maintain any other accounts with financial organizations. He stated that such individuals may be less familiar with the technology inherent in the online systems.

He identified additional specific considerations and issues, including: (1) The desirability of using identifiers other than SSN. However, he recognized the reality that the SSN may be the only common data element across multiple parties with which Guided Choice will interact with respect to a particular plan and participant. (2) Additional challenges that may arise working with some smaller TPAs that may not have similar data safeguards in place. (3) The importance of data encryption, which is no longer reserved to transfers between networks and servers. It is also important for wireless access and generally for laptops. Wireless access points should be secured or avoided. Also, no client data should be stored on a laptop that would use wireless. (4) The absence of significant data security due diligence by some smaller employers, relying more on the selected TPA to provide such security. He agreed that development of privacy and security standards similar to what is used on the health side, such as agreement & notice requirements, could be very helpful. However he recognized that such standards should be commercially reasonable for the industry, and that implementing any such process will take time.

David L. Wray, President, Profit Sharing/401k Council of America

Mr. Wray presented testimony concerning the privacy and security of employer-sponsored defined-contribution plans by incorporating the results of a Profit Sharing/401k Council of America (PSCA) snapshot survey of 234 plan sponsors on the topic. (Subsequent to this testimony the Profit Sharing/401k Council of America changed its name to Plan Sponsor Council of America (PSCA).

When PSCA first collected data with respect to internet access in 1997, 60 per cent of the plans did not provide internet access, compared to 9 per cent without internet access today. Currently, retirement plans rely on a single level of authentication -- usernames and passwords -- because employers have not experienced significant problems in this area.

Mr. Wray spoke about three different issues: privacy, security and fraud. In defined contribution plans, a significant amount of personal data is attached to each account. This information resides in the databases of third party record keepers, because employers outsource this function. Both plan sponsors and participants access this data

through the internet. Record keepers have extensive protections in place, e.g., providers now use IP addresses to track someone attempting to gain illegal access.

However, Mr. Wray noted that it was important to differentiate "privacy" from "security," because protecting plan privacy is not a fiduciary obligation. Nevertheless, record keepers often have contractual obligations to secure the privacy of participant information. In addition, some record keepers are held to privacy practice standards by regulating agencies. However, there are no federal requirements for record keepers that are not financial institutions. When asked if the privacy requirements extend to record keepers that are affiliated with financial institutions, Mr. Wray replied record keepers generally had a single system, but that legal privacy protections would not necessarily extend to plan participants.

Mr. Wray commented that states are also taking action in the area of privacy. Both California and Massachusetts have broad laws affecting retirement plans and record keepers not covered by federal regulations.

Mr. Wray agreed that ERISA imposes a fiduciary obligation on plan sponsors to protect plan assets. This duty includes ensuring that plan distributions are made only to plan participants. Withdrawals, distributions and loans are requested via the internet, but distribution is normally a paper check. PSCA survey data shows that this is changing, with 41 per cent of employers permitting electronic transfer and 27 per cent having an extra level of security for distributions. Because participants do not need distributions from their retirement plan very often, 11 per cent of the employers allowed participants to "lock" their accounts, so that distributions cannot be made until the account is "unlocked" – thus blocking unauthorized access in the interim.

In the PSCA snapshot survey, about the half the respondents have privacy and security policies that apply to their retirement plans, but in most cases they are part of a broader policy regarding benefits. Another security concern is the payroll service that transmits data to the record keepers. Larger plan sponsors include questions about privacy and security in contracts and requests for proposal. In contrast, smaller companies often do not raise these issues and rely on service providers to automatically provide security and privacy protection.

Mr. Wray stated that a loss of plan assets is necessary before a privacy breach would be considered a fiduciary responsibility. When asked if a plan fiduciary involvement in the misuse of plan information would be self-dealing under ERISA, Mr. Wray responded that plan sponsors should not use participant data except for what is necessary for administering the plan, but that the amount of data needed for proper plan administration can be extensive.

Mr. Wray had the following recommendations: (1) Develop templates that plan sponsors could use in developing their own retirement plan internet privacy and security policies. (2) Develop a template of suggested questions that plan sponsors could use as part of a

request for proposal or ongoing monitoring process to determine if their record keepers have privacy and security protections in place.

Mr. Wray strongly opposed DOL regulation in this area, noting that federal and state laws are already requiring those managing individual information electronically to maintain high levels of privacy and security protection. Mr. Wray believes that holding plan sponsors accountable for a new set of regulations for a system over which they have no control could have a significant impact on the willingness of companies to sponsor plans.

Finally Mr. Wray noted that security risk is inherent in all we do. He suggested that plans mitigate the risk by choosing reliable vendors and being careful with data. More regulations are not going to change the risk. Big financial institutions are aware of these issues and have taken action, but there could be a gap in terms of independent TPAs that service smaller plans.

There is an independent look at internal control by TPAs by the accountants, but not all record keepers have a Statement of Auditing Standards (SAS) No. 70 (in-depth audit of an organization's control objectives and control activities, which often include controls over information technology and related processes). Mr. Wray recommended that providers have a SAS 70 to help plan sponsors make good choices. However, there is a cost involved. There is no oversight body for record keepers. There is a group of record keepers that are not subject to any of these rules. He did not know how many, but those record keepers are more likely to provide services for small to medium size plans.

Kathleen M. Quinn, Executive Director, National Adult Protective Services Association

Kathleen Quinn, the Executive Director of the National Adult Protective Services Association, described the dimensions and incidence of elder abuse, including financial exploitation, and noted a conservative estimate was that about 10 percent of older people experienced abuse within the past 12 months. One concern is the underreporting of elder abuse with a recent study in New York finding that only one in 44 cases of financial abuse was reported to an outside agency.

Most elder financial abuse is committed by family members, such as adult children and grandchildren, with common methods being theft, intimidation or transfer of assets. The misuse of powers of attorney is also common particularly for elders with dementia or cognitive decline who do not understand what they are signing. Ms. Quinn noted that states may require a witness to the power of attorney which mitigates some of the risk. Trusted advisors, including attorneys, financial planners and insurance agents, may also perpetrate financial abuse. Professional con artists using traditional schemes and ruses are also responsible for a significant amount of financial abuse.

Older people may be at risk of financial abuse due to their increased dependence on others, isolation and perceived obligations from family ties as well as the impact of the

aging process on decision-making.

State adult protective services (APS) programs are responsible for receiving and responding to reports of elder abuse, although there may be significant differences from state to state as there is no federal support or standard for these programs. Professionals, including doctors, nurses, law enforcement officers and social workers, are required to report suspected abuse in all but four states and banks must do so in eleven states. APS can intervene to protect victims.

To address elder financial abuse, Ms. Quinn suggested that everyone should be made aware that abuse can happen to them or someone they know and take steps to mitigate the risk especially by avoiding isolation and increasing social connections. She also noted that exercising care with respect to powers of attorney was important, including requiring regular accountings and updates of the authorizing document.

Ms. Quinn also suggested that increasing plan administrators' awareness of the risk of elder abuse could be helpful, as well as educating plan participants. She highlighted two initiatives that might serve as examples. The BITS Elder Fraud Prevention Toolkit, produced by a division of the Financial Services Roundtable, can be used by banks and provides training on different types of financial exploitation and warning signs. The other, the Investor Protection Trust Elder Investment Fraud and Financial Exploitation Program, trains physicians and other clinicians to be aware of elder financial abuse and the increased risk for abuse posed by cognitive impairment and offers a pocket guide with helpful information about warning signs and questions to ask.

Seth Geftic, RSA, Security Division of EMC

Mr. Geftic has worked extensively combating cyber crime and fraud at RSA. His firm protects over 8,000 organizations and 250 million online identities, and has secured over 20 billion online transactions across a wide range of industries.

Cyber attacks against employee benefit plans are no different than against the remainder of the financial services industry. As to the reason, the obvious answer is that is where the money is. However, besides money and financial data, cybercriminals target personal identifiable information (PII). The more data that exists about customers and employees, and the more that data is moved around, the more opportunities there are for PII to be stolen and used for other crimes.

There is an underground network of cyber criminals that has been growing in size and sophistication for more than five years. In this underground, one can learn about new methods of cyber attack as well as purchase malicious technology for such attacks. Moreover, people create and sell toolkits so that someone else can attack organizations such as financial institutions and government agencies. This underground also acts as a marketplace for the sale of information, PII and credit cards.

Generally, data is stolen through "social engineering" or the manipulation of people into performing actions or divulging confidential information.

Malware that gets installed onto a computer can steal usernames and passwords, steal information from online banking or other websites visited, or automate transactions without an individual's knowledge. Malware can be targeted at employee benefit accounts through the 401(k) provider.

Small and medium size businesses, non-profit organizations, and city and county governments are frequently attacked because they may be less protected and less sophisticated.

Because there is no "silver bullet" or single security technology that will protect a site, organizations must have a layered security strategy which is adaptable to new threats. That could include strong authentication, fraud protection services that block and shut down attacks, identity verification, and education of employees.

Mr. Geftic believes that the current security policy utilized in the financial services industry -- the Federal Financial Institution Examination Council – is the type of policy that would be beneficial to employee benefit plans, in that it requires increased account protection without mandating a specific technology to achieve that goal.

In response to a Council member's inquiry concerning the type of key questions to ask a service provider about their security strategy, Mr. Geftic suggested the following: what type of authentication is in place; what type of defenses are in place against common attacks such as phishing and Trojan attacks; do they have access and authentication controls; what are the guarantees for protection of the plan's data; what is the risk and liability of the plan; how much support would the provider give the plan should there be a breach in security; does the consumer have the responsibility to ensure that their own computers are safe; what advice are they providing to their customers in order to protect their site and the data.

In designing multi-factor authentication for retirees, various methodologies could be used subject to cost constraints and ease of use. These could include: offline tokens (but the physical device would need to be tracked); use of a mobile device (although attacks on these are becoming more frequent); use of a dedicated computer for only financial transactions which significantly lowers the risk of being compromised; a risk-based approach; or one-time authentication methods.

Ian MacKay, Director of Regulatory Affairs, American Institute of Certified Public Accountants (AICPA) and Director of the AICPA Employee Benefit Plan Audit Quality Center

Mr. Mackay began his testimony discussing the letter submitted by Jim Merklin regarding fraud. He indicated that the auditor is concerned about security and privacy issues as they relate to the misappropriation of assets which could be fraud. Stealing plan assets affects the financial statements.

Mr. Mackay's comments covered the background of Service Organization Reports on internal controls which are commonly referred to as SAS 70 reports. He indicated that these reports are used by plan sponsors and auditors to understand the controls at third party service providers and to help the auditor reduce testing in certain areas of the audit. Many plan sponsors outsource certain functions such as participant record keeping, asset custodial/trustee, and payroll processing. Each of these service providers processes information and transactions that affect the plan's financial statements. SAS 70 was issued in 1992 to alleviate duplication of efforts by outside auditors and it addresses the controls relevant to the Plan's internal control over financial reporting. These reports are voluntary on the part of the service provider but can reduce audit costs and help the plan sponsor in meeting fiduciary responsibilities. Controls typically covered are access controls, transactions controls, trust and investment controls. Controls over privacy and security issues such as firewall security and cloud computing are addressed only as they relate to financial reporting controls. There are two types of reports: the Type 1 report covers the design of the service organization's system and the Type 2 report covers the operating effectiveness of the controls. A Type 2 report is more beneficial to the plan sponsor and plan auditor. Mr. MacKay indicated that many times the plan sponsor does not read the report, but obtains it for their auditor's use.

Mr. MacKay then discussed the current changes to the SAS 70 reports, now called SSAE No. 16 reports effective June 15, 2011. These new reports are Service Organization Control Reports (SOC reports). There are three new reports: SOC 1, which is similar to the old SAS 70 report for financial statements, and SOC 2 and SOC 3 reports, which include controls relevant to user entities other than for controls over financial statements. The SOC 2 and SOC 3 reports can cover controls regarding security, availability, processing integrity, privacy and confidentiality. Mr. MacKay provided an exhibit that compared all three types of reports.

Mr. MacKay then discussed the process for preparing these reports and the process for auditors to issue their opinion on such reports. He indicated that if a control was not tested that the auditor would need to perform additional procedures to complete the audit. If a control was not tested the auditor might indicate that such controls were not part of the examination.

He provided some examples of where benefit plans have been "hacked" and plans have had security breaches related to lost computers. He concluded his comments indicating that because the SOC 2 and SOC 3 reports are new, he has not seen any issued yet. He

believed that the new reports were in response to a perceived need of corporations that outsource information requiring assurance regarding privacy and security controls. He also discussed the reports issued by a joint task force of the AICPA and the Chartered Accountants of Canada related to Generally Accepted Privacy Principles.

Panel of Chris Brecht, Carday Associates; John Barton, Health Services Benefit Administrators, Inc. (retired from Mercer); Richard Carpenter, ASPPA

John Barton: Health Services Benefit Administrators, Inc. (HSBAI) is a small third party administrator (TPA) with a revenue stream of $10-11 million per year, split 70 per cent/30 per cent health plans to retirement plans. Their primary clients are multiemployer Taft-Hartley plans as well as some single employer plans. Their primary geographic focus is northern California. On the subject of cyber and other security, Mr. Barton encouraged the council to think of HIPAA. All TPAs with health plan business have been coping with those extensive requirements because: (1) many workers know their rights concerning requirements for privacy of health information, and (2) the environment is complex, involving information sharing with many vendors and service providers. Citing two specific anecdotes, he observed that there are many ways to lose control of data. Key requirements include having the requisite security procedures in place to prevent loss and protect the data, and procedures to remediate when necessary. He noted that 98 per cent of incoming email to HSBAI is rejected on the first pass frequently due to large files from known senders. He also noted that many Taft-Hartley plan service providers have been approached with offers of cyber security insurance – coverage for privacy notification, crisis management, reward expense, e-business interruption, and other costs. This has raised questions of the proper party to be covered -- the trustee or the service provider. Mr. Barton provided two recommendations: (1) Do not permit data to be left on laptops except where needed, and even then only with encryption. He noted that this was an important point that extended beyond health plan clients. After HSBAI became compliant with HIPAA, the firm implemented the same safeguards for all plan clients. (2) The data security environment is constantly changing, with more demand for instant information, new developments such as state insurance exchanges, and overall intense and rapid distribution of information, and service providers should expect the standards to continue to rise. He also suggested that there could be a benefit to providing a clearinghouse of beneficial cyber security developments.

Chris Brecht: Carday Associates administers multi-employer plans exclusively, including 21 health and welfare plans, 14 defined benefit plans, and 5 defined contribution plans. Mr. Brecht's comment focused on pensions, discussing potential for fraud and key areas of concern. He noted that privacy is not as major an issue for multiemployer plans. For example, when individuals move between participating employers, little personal information needs to be moved, and when it does, an alternate ID is used rather than a Social Security number. In addition, the plans involve limited participant contact during working years. Initiation of pensions is a paper process, not an electronic one. There are concerns about privacy and security in call centers. He noted that service providers have significantly increased their procedural safeguards in verifying the caller's identity. HIPAA changes have migrated over to the pension side

with tightened access to information. Security procedures include: alternate ID, encryption, and site-to-site communication. In addition, no personal information is stored on laptops: it is stored on servers which require passwords and identifiers and utilize multi-level databases. While in-house software was once the norm, now service providers are generally using outside software at least for some functions, because it is almost impossible to maintain software in-house and keep up with developments. Mr. Barton also commented on how constant change is driving consolidation of service providers. This was illustrated by an anecdote about a small administrator in California that was acquired because their auditors were telling them their controls were inadequate. Mr. Brecht noted that his firm's five most recent client acquisitions were plans that had been self-administered and simply could not keep up with changing requirements. He also highlighted the importance of concerns regarding fraud in pension plans, beginning at the active participant level. He referenced the frequency with which individuals "rent" a Social Security number in order to work, with one result that sometimes multiple individuals use the same number over a particular period, sometimes requiring reviews and reconciliations at the time benefits are to be paid. To guard against fraud within the service provider shop, he noted the importance of separating duties or portions of duties; for example, having paperwork start with a processor, and then advancing to a supervisor, then to account executive, then to trustee. As for participant fraud, he noted a few examples: the participant does not disclose the existence of a spouse, or can claim common law marriage in order to get coverage under a health and welfare plan, and then deny it at retirement time. Another fraud is an intentional failure to notify when the retiree receiving an annuity dies.

Richard Carpenter: Mr. Carpenter has been involved with the American Society of Pension Professionals & Actuaries (ASPPA) for 30 years, including recently the Center for Fiduciary Excellence (CFEX). CFEX applies best practices for record keeping and compliance TPAs. He is passionate about this issue because his own company's computer was hacked to get access to data to and from other sources. He noted the ERISA plans have changed considerably since the first 401(k) was established in 1981. Today participants have daily access with instant website updates. He noted that most Third Party Administrators (TPAs) work with backrooms, and do not handle all of the data flow themselves. CFEX follows International Organization for Standardization (ISO) 9001 of quality control, including data security, privacy, but also hiring and other functions. He noted that when an auditor visits a TPA the analyst will go through a long list of criteria: privacy, data security, generally focusing on operational matters. Training is also important – what information to share, and with whom. He noted that when considering rules or requirements it is important to understand the demographics of the plans and also the people providing the information. He indicated that although most retirement plans are small with only 11 per cent having more than 100 participants, larger plans have 82 per cent of assets and 86 per cent of participants. Thus, the top 1,000 plans represent the majority of both assets and participants. He noted that 65 per cent of qualified plans have less than $1 million in assets, and that the TPA domain is small and midsized plans. He also noted that many small plans do not use a TPA; instead they work exclusively with an investment provider. He cited that there are generally two types of TPAs: record keeping TPA (approximately 300), and compliance TPA (Form

5500, nondiscrimination testing). He observed that almost all record keeping firms have or are seriously considering SAS 70 (or its successor). They are cognizant of privacy issues; however many are too small to maintain their own IT dept. The level of awareness, however, has risen in the past five years; some TPAs are working with an insurance company that has detailed processes and procedures, and secure portals. In response to the inquiry as to how many TPAs administer retirement plans exclusively, and thus do not maintain HIPAA procedures, he noted that there are over 3000 TPAs, not including law firms and accounting firms. This includes a very small population of TPAs also administering defined benefit plans. Mr. Barton responded to a question about the process for TPAs to acquire cyber security insurance, and noted that it is a fairly new phenomenon, although at least four carriers specialize in it. The information required to obtain the insurance can be difficult to provide: technology infrastructure, including safeguards, policies and procedures, training for staff, HIPAA compliance, and detailed questionnaires. It also includes questions about such areas as outsourcing payment processing; backups; controls on access; regulatory investigations; and the number of records on hand.

A question was posed regarding the type of procedures TPAs put in place focusing on terminated or retired employees. In particular, the questioner was interested in how these employees accessed information from outside the employer's workplace. Mr. Barton related an anecdote regarding fraud by retirees and their families. In one case a plan's actuary was concerned that retirees in the Philippines lived unusually long lives. The plan's trustees engaged private investigators, and learned that a decedent payee's thumbs were preserved in formaldehyde to provide thumb prints as required for validation for continued payment.

A question was posed to Mr. Barton regarding the cost of implementing HIPAA type requirements for a TPA not currently subject to such requirements. With appropriate disclaimers that this was not a formal estimate, he indicated that it might cost $200,000, including the cost of internal training, updates, review of procedures and redesign. Mr. Carpenter noted that, for a TPA already subject to HIPAA, it would be preferable to extend the same procedures to pensions rather than developing two sets of standards. However, he also did not think a blanket extension of HIPAA requirements to all TPAs was a good idea. He suggested that many TPAs would not incur the costs because they would rely on third parties to comply with security guidelines. Mr. Brecht concurred with Mr. Barton that there were difficulties in extrapolating HIPPAA requirements to retirement plans, highlighting the extent of training that might be required.

Investment Company Institute

The Investment Company Institute (ICI) is the national association of U.S. investment companies including mutual funds. ICI submitted written testimony making three key points. First, the regulatory framework under which funds design their security programs works well because it is not prescriptive and provides funds broad discretion to tailor their security programs to their business and the needs of their investors. Second, technology and the security threats that mutual funds face change rapidly, and regulators

must provide flexibility to allow financial institutions to adapt their policies and procedures to changing conditions. Third, the fund industry has developed strong procedures and safeguards that rely on layered defenses, robust auditing, and a commitment from senior management. While fund companies' procedures share common elements, there is no "one-size-fits-all" approach that is best for every fund company and its investors.

ICI discussed the SEC requirements under Regulation S-P, which are formulated as broad concepts, e.g., ensure security and confidentiality of customer records and information; protect against anticipated threats; and protect against unauthorized access. ICI then explained that mutual funds use a layered approach to meet these requirements, managing both the physical access to facilities and the authentication and authorization process for access to computer systems. Security risks include operational risks that arise due to viruses, phishing, distributed denial of service attacks (denial of computer access by "crashing" the system), website defacement and common fraud. Each organization employs a variety of techniques appropriate to its size, business model, type of clients, vulnerabilities and its analysis of which combination of practices it believes will best protect shareholders and systems from these risks.

Hiring of specialized IT staff is important in establishing and implementing various security policies and procedures. This may include policies for hiring and training of non-IT staff (including background checks). In addition, ICI set forth numerous layered defense tools including: firewalls, antivirus software, intrusion detection monitoring, shareholder validation for account access, verification procedures for identity of phone callers, system controls for employee access, procedures for determining inconsistent patterns of activity for shareholders and employees, procedures to confirm account changes, and physical protection of computer equipment and hardcopy shareholder information.

Finally, ICI stated that mutual funds must maintain written policies and procedures as part of their compliance programs; must test these policies and make changes to address material weaknesses. The policies may include areas such as privacy, computer usage, employee policies concerning the use of computer and mobile devices, use of social media and employee ethics. Testing of these procedures and programs include auditing by third party auditors, testing of new computer programs, and facility audits.